Segment ID	Segment status	Source segment	Target segment
1	Translated (0%)	<3/> <6>Acceptable Use Policy<10/><14/></6>	<3/> <6>6/></14></10>سياسة الاستخدام المقبول
2	Translated (100%)	Page <28><19/> of <27/></28>	28/></27> من </19><28>صفحة
3	Translated (100%)	Al Hammadi Holding	شركة الحمادي القابضة
4	Translated (0%)	<60/>MAMeAr	<60/>MAMeAr
5	Translated (100%)	Acceptable Use Policy	سياسة الاستخدام المقبول
6	Translated (100%)	CYBERSECURITY DEPARTMENT	إدارة الأمن السيبراني
7	Translated (100%)	Policy ID	معرّف السياسة
8	Translated (100%)	AHH-CS-ISMS-001	AHH-CS-ISMS-001
9	Translated (100%)	Class	الفئة
10	Translated (100%)	Internal Release	إصدار داخلي
11	Not Translated (0%)		
12	Translated (100%)	V 1.0	V 1.0
13	Translated (100%)	Published at	نُشرت في
14	Translated (100%)	June 2025	يونيو 2025
15	Translated (100%)	Document Owner	المسؤول عن المستند
16	Translated (100%)	Cybersecurity <89>Department</89>	إدارة<89/> الأمن السيبراني<89>
17	Translated (0%)	Alhammadi holding	شركة الحمادي القابضة
18	Translated (100%)	Disclaimer	تنويه

19	Translated (100%)	The information contained in this document is property of Al Hammadi Holding and must not be copied or communicated to a third party or used for any purpose other than that for which it is supplied, without the written consent of Al Hammadi Holding.	المعلومات الواردة في هذا المستند هي ملك لشركة الحمادي القابضة ولا يجوز نسخها أو إبلاغها إلى طرف ثالث أو استخدامها لأي غرض آخر غير الغرض الذي تم توفيرها من أجله، دون موافقة خطية من شركة الحمادي القابضة.
20	Translated (100%)	Contents	جدول المحتويات
21	Translated (100%)	Document Control	ضبط المستندات
22	Translated (100%)	Document Information	معلومات المستند
23	Translated (100%)	Synopsis	الملخص
24	Translated (100%)	Document Title:	عنوان المستند:
25	Translated (100%)	Acceptable Use Policy	سياسة الاستخدام المقبول
26	Translated (100%)	Document Status:	حالة المستند:
27	Translated (100%)	Approved	معتمد
28	Translated (100%)	Document Effective Date:	تاريخ سريان المستند:
29	Translated (0%)	June 202<206>5</206>	يونيو 202<206>5</206>
30	Translated (100%)	Document Issue Date:	تاريخ إصدار المستند:
31	Translated (100%)	June 202<221>5</221>	يونيو 202<221>5</221>
32	Translated (100%)	Document Next Revision Date:	تاريخ المراجعة التالية للمستند:
33	Translated (100%)	June 2026	يونيو 2026
34	Translated (100%)	Key contacts	جهات التواصل الرئيسية
35	Translated (100%)	Document Owner:	المسؤول عن المستند:
36	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
37	Translated	Approval Authority	جهة الاعتماد

	(100%)		
38	Translated (100%)	Document Created by:	:مُنشئ المستند
39	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
40	Translated (100%)	Document Reviewed by:	:راجع المستند
41	Translated (100%)	HR Manager	مدير الموارد البشرية
42	Translated (100%)	Document Approved by:	:اعتمد المستند
43	Translated (0%)	CS Manager	مدير الأمن السيبراني
44	Translated (100%)	Note:	:ملاحظة
45	Translated (100%)	Any additional approval will be added in the document annex	تُضاف أي اعتمادات إضافية في ملحق المستند
46	Translated (100%)	Classification	التصنيف
47	Translated (100%)	Company Internal – to be shared with 3rd parties after consent of CS Manager	داخلي لاستخدام للشركة – يُسمح بمشاركته مع جهات خارجية بعد موافقة مدير إدارة الأمن السيبراني
48	Translated (100%)	Version / Dates	الإصدار / التواريخ
49	Translated (100%)	Current Version:	:الإصدار الحالي
50	Translated (100%)	1.0	1.0
51	Translated (100%)	Date Published:	:تاريخ النشر
52	Translated (100%)	July 2025	يوليو 2025
53	Translated (100%)	Date of Next Review:	:تاريخ المراجعة التالية
54	Translated (100%)	July 2026	يوليو 2026
55	Translated (100%)	Prior Version:	:الإصدار السابق
56	Translated (99%)	N/A	لا ينطبق

57	Translated (100%)	Prior Published:	تاريخ النشر السابق:
58	Translated (100%)	N/A	لا ينطبق
59	Translated (100%)	Document Changes	التغييرات على المستند
60	Translated (100%)	Date	التاريخ
61	Translated (100%)	Version	الإصدار
62	Translated (0%)	Department Name	اسم الإدارة
63	Translated (100%)	Change Description	وصف التغيير
64	Translated (100%)	July 2025	يوليو 2025
65	Translated (100%)	1.0	1.0
66	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
67	Translated (100%)	V 1.0	V 1.0
68	Translated (100%)	Document Circulation	تعميم المستند
69	Translated (100%)	To	إلى
70	Translated (100%)	Date	التاريخ
71	Translated (100%)	Method	الطريقة
72	Translated (100%)	All Al Hammadi Staff	جميع موظفي شركة الحمادي
73	Translated (0%)	<404>July </404>2025	يوليو <404>2025<404/>
74	Translated (100%)	Intranet Portal	بوابة الإنترانت
75	Translated (100%)	Objectives	الأهداف
76	Translated	The objective of this Acceptable Use Policy (AUP) at Al Hammadi	الهدف من سياسة الاستخدام المقبول هذه في شركة الحمادي القابضة هو

	(0%)	Holding is to minimize the risk of misuse, unauthorized access, or damage to the organization's information systems and digital assets.	تقليل مخاطر سوء الاستخدام أو الوصول غير المصرح به أو تلف أنظمة معلومات المنظمة والأصول الرقمية.
77	Translated (0%)	This is achieved by clearly defining acceptable behaviors and responsibilities for all users who are granted access to Al Hammadi Holding’s technology resources.	ويتحقق ذلك من خلال التحديد الواضح للسلوكيات والمسؤوليات المقبولة لجميع المستخدمين الذين يتم منحهم حق الوصول إلى الموارد التكنولوجية لشركة الحمادي القابضة.
78	Translated (0%)	The policy also aims to ensure that all individuals including employees, temporary staff, trainees, and service providers fully understand their responsibilities in maintaining information security and are aware of the disciplinary actions that may result from violations of this policy.	تهدف السياسة أيضًا إلى التأكد من أن جميع الأفراد بما في ذلك الموظفين والموظفين المؤقتين والمتدربين ومقدمي الخدمات يفهمون تمامًا مسؤولياتهم في الحفاظ على أمن المعلومات ويدركون الإجراءات التأديبية التي قد تنجم عن انتهاكات هذه السياسة.
79	Translated (100%)	Scope	النطاق
80	Translated (100%)	This policy applies to all Al Hammadi Holding Cybersecurity Management operations, assets, and activities, including employees, trainees, service providers,<452> </452>and third parties under its control.	تنطبق هذه السياسة على جميع عمليات وأصول وأنشطة إدارة الأمن السيبراني لشركة الحمادي القابضة، بما في ذلك الموظفين والمتدربين ومقدمي الخدمات<452> <452/>والجهات الخارجية الخاضعة لسيطرتها.
81	Translated (100%)	Roles and Responsibilities	الأدوار والمسؤوليات
82	Translated (100%)	<464><462>Al Hammadi Holding </462></464><467>management is responsible for implementing, maintaining, and updating this policy with all its contents, in accordance with any changes in the Statement of Applicability, Al Hammadi Holding-SOA Document.</467>	تتحمل إدارة <464>شركة الحمادي القابضة <464/>مسؤولية تنفيذ هذه السياسة وحفظها وتحديثها بكامل محتوياتها، وذلك بما يتماشى مع أي تغييرات في بيان التطبيق الخاص بشركة الحمادي القابضة.
83	Translated (100%)	Principles	المبادئ
84	Translated (100%)	General Requirements	المتطلبات العامة
85	Translated (100%)	All users of Al Hammadi Holding's information and technology assets must sign and agree to the terms and conditions of their employment contract.	على جميع مستخدمي الأصول المعلوماتية والتكنولوجية لشركة الحمادي القابضة التوقيع والموافقة على شروط وأحكام عقد العمل الخاص بهم.
86	Translated (100%)	These terms and conditions outline the personnel's responsibilities regarding adhering to cybersecurity controls within the Al Hammadi Holding environment.	تحدد هذه الشروط والأحكام مسؤوليات الموظفين فيما يتعلق بالالتزام بضوابط الأمن السيبراني داخل بيئة شركة الحمادي القابضة.
87	Translated (0%)	All users must formally acknowledge this AUP annually, and violations may result in disciplinary action up to and including termination of employment or contract.	يجب على جميع المستخدمين الاعتراف رسميًا بسياسة الاستخدام المقبول هذه سنويًا، وقد تؤدي الانتهاكات إلى اتخاذ إجراءات تأديبية تصل إلى إنهاء العمل أو العقد.
88	Translated (100%)	All personnel at Al Hammadi Holding bear the primary responsibility for continuous compliance with cybersecurity policies.	يتحمل جميع الموظفين في شركة الحمادي القابضة المسؤولية الأساسية عن الامتثال المستمر لسياسات الأمن السيبراني.
89	Translated (100%)	Possess a level of awareness regarding data security relevant to their roles and responsibilities within Al Hammadi Holding.	امتلاك مستوى من الوعي فيما يتعلق بأمن البيانات ذات الصلة بأدوارهم ومسؤولياتهم داخل شركة الحمادي القابضة.
90	Translated	Commit to the terms and conditions of employment, encompassing	الالتزام بشروط وأحكام التوظيف، بما في ذلك سياسات الأمن السيبراني

	(100%)	cybersecurity policies within Al Hammadi Holding and the acceptable use policy for information and technology assets, as well as appropriate workplace practices within Al Hammadi Holding.	داخل شركة الحمادي القابضة وسياسة الاستخدام المقبول لأصول المعلومات والتكنولوجيا، وكذلك ممارسات مكان العمل المناسبة داخل شركة الحمادي القابضة.
91	Translated (0%)	Al Hammadi Holding reserves the right to monitor and log all activities on its information systems for operational, security, and compliance purposes.	تحتفظ شركة الحمادي القابضة بالحق في مراقبة وتسجيل جميع الأنشطة على أنظمة المعلومات الخاصة بها لأغراض التشغيل والأمن والامتثال.
92	Translated (100%)	Undergo periodic cybersecurity awareness assessments and take appropriate measures to address any identified gaps.	الخضوع لتقييمات دورية للتوعية بالأمن السيبراني واتخاذ التدابير المناسبة لمعالجة أي ثغرات محددة.
93	Translated (100%)	Each department or division manager must ensure the attendance of all their employees in the cybersecurity training and awareness sessions whenever these are conducted.	على كل مدير إدارة أو قسم التأكد من حضور جميع موظفيه في جلسات التدريب والتوعية بالأمن السيبراني كلما أجريت هذه الجلسات.
94	Translated (100%)	<557>All department or division managers within </557><563><561>Al Hammadi Holding </561></563><566>should ensure that personnel and external service providers who offer services to their respective departments are well-versed in and committed to the cybersecurity policies before being granted access to Al Hammadi Holding information and technology assets.</566>	<557>على <561><563><557/>جميع مديري الإدارات أو الأقسام داخل شركة الحمادي القابضة <566><563/><561/>التأكد من أن الموظفين ومقدمي الخدمات الخارجيين الذين يقدمون الخدمات لإداراتهم الخاصة على دراية جيدة بسياسات الأمن السيبراني والالتزام بها قبل منحهم حق الوصول إلى أصول المعلومات والتكنولوجيا الخاصة بشركة الحمادي القابضة.<566/>
95	Translated (0%)	Use of Al Hammadi Holding's technology assets including computers, mobile devices, Healthcare Systems, email systems, and internet access must be for authorized business purposes only.	يجب أن يكون استخدام الأصول التقنية لشركة الحمادي القابضة بما في ذلك أجهزة الكمبيوتر والأجهزة المحمولة وأنظمة الرعاية الصحية وأنظمة البريد الإلكتروني والوصول إلى الإنترنت لأغراض تجارية مصرح بها فقط.
96	Translated (0%)	Any personal use must be minimal and not interfere with work responsibilities or security requirements.	يجب أن يكون أي استخدام شخصي في الحد الأدنى ولا يتعارض مع مسؤوليات العمل أو متطلبات الأمان.
97	Translated (0%)	Users are strictly prohibited from engaging in the following activities:	يُمنع المستخدمون منعًا باتًا من المشاركة في الأنشطة التالية:
98	Translated (0%)	Unauthorized access, modification, or deletion of data or systems	الوصول غير المصرح به أو تعديل أو حذف البيانات أو الأنظمة
99	Translated (0%)	Sharing login credentials or access tokens	مشاركة بيانات اعتماد تسجيل الدخول أو رموز الوصول
100	Translated (0%)	Installing unauthorized software or hardware	تثبيت برامج أو أجهزة غير مصرح بها
101	Translated (0%)	Using Al Hammadi resources and assets to access or distribute offensive, illegal, or malicious content	استخدام موارد وأصول الحمادي للوصول إلى أو توزيع محتوى مسيء أو غير قانوني أو ضار
102	Translated (0%)	Attempting to bypass physical and security controls, or monitoring tools	محاولة تجاوز الضوابط المادية والأمنية، أو أدوات المراقبة
103	Translated (0%)	Any known or suspected cybersecurity incidents, violations of this policy, or potential threats must be immediately reported to the designated cybersecurity team at cybersecurity@alhammadi.com	يجب الإبلاغ على الفور عن أي حوادث معروفة أو مشتبه فيها تتعلق بالأمن السيبراني أو انتهاكات لهذه السياسة أو التهديدات المحتملة إلى فريق الأمن السيبراني المعين على cybersecurity@alhammadi.com
104	Translated (0%)	Users must lock or log off their devices when unattended and avoid leaving sensitive information visible on screens or desks.	يجب على المستخدمين قفل أجهزتهم أو تسجيل الخروج منها عند عدم مراقبتها وتجنب ترك المعلومات الحساسة مرئية على الشاشات أو المكاتب.

105	Translated (100%)	Maintaining Information Confidentiality	الحفاظ على سرية المعلومات
106	Translated (100%)	All temporary associates at Al Hammadi Holding must sign a confidentiality agreement as an indication of their commitment to safeguarding confidential and sensitive information within the organization.	على جميع الشركاء المؤقتين في شركة الحمادي القابضة التوقيع على اتفاقية سرية كدليل على التزامهم بحماية المعلومات السرية والحساسة داخل المنظمة.
107	Translated (0%)	This should be done before granting them access to critical and sensitive facilities or data.	يجب أن يتم ذلك قبل منحهم حق الوصول إلى المرافق أو البيانات الهامة والحساسة.
108	Translated (0%)	Confidential information must only be shared through secure communication channels approved by Al Hammadi Holding.	يجب مشاركة المعلومات السرية فقط من خلال قنوات اتصال آمنة معتمدة من قبل شركة الحمادي القابضة.
109	Translated (0%)	Use of external storage devices such as USBs is restricted and requires prior approval from the Cybersecurity Department.	مقيد ويتطلب موافقة مسبقة USBs استخدام أجهزة التخزين الخارجية مثل من إدارة الأمن السيبراني.
110	Translated (0%)	Personnel must not store or transmit Al Hammadi Holding's confidential or sensitive data using unauthorized cloud storage services, removable media, or personal devices.	يجب على الموظفين عدم تخزين أو نقل البيانات السرية أو الحساسة لشركة الحمادي القابضة باستخدام خدمات التخزين السحابي غير المصرح بها أو الوسائط القابلة للإزالة أو الأجهزة الشخصية.
111	Translated (100%)	Awareness, Education, and Training Programs	برامج التوعية والتثقيف والتدريب
112	Translated (100%)	All suppliers or external parties who may have access to Al Hammadi Holding information assets and technology must be educated about the cybersecurity practices followed within the organization before being granted access privileges.	يجب توعية جميع الموردين أو الجهات الخارجية الذين قد يكون لديهم حق الوصول إلى أصول وتكنولوجيا معلومات شركة الحمادي القابضة حول ممارسات الأمن السيبراني المتبعة داخل المؤسسة قبل منحهم امتيازات الوصول.
113	Translated (0%)	All employees are required to attend the cybersecurity awareness workshops organized by the organization to enhance their understanding of cyber risks and reinforce their commitment to the approved cybersecurity policies and procedures.	يُطلب من جميع الموظفين حضور ورش العمل التوعوية بالأمن السيبراني التي تنظمها المنظمة لتعزيز فهمهم للمخاطر السيبرانية وتعزيز التزامهم بسياسات وإجراءات الأمن السيبراني المعتمدة.
114	Translated (0%)	Refresher cybersecurity training must be conducted annually, with tracked attendance and completion records maintained by HR and the Cybersecurity Department.	يجب إجراء تدريب تنشيطي على الأمن السيبراني سنويًا، مع تتبع سجلات الحضور والإنجاز التي تحتفظ بها الموارد البشرية وإدارة الأمن السيبراني.
115	Translated (0%)	All new hires must complete cybersecurity onboarding training before being granted system access.	يجب على جميع الموظفين الجدد إكمال التدريب على الأمن السيبراني قبل منحهم حق الوصول إلى النظام.
116	Translated (100%)	Compliance and Adherence	الامتثال والالتزام
117	Translated (100%)	Al Hammadi Holding CEO shall ensure compliance with the cybersecurity policies and standards.	يضمن الرئيس التنفيذي لشركة الحمادي القابضة الامتثال لسياسات ومعايير الأمن السيبراني.
118	Translated (100%)	To ensure compliance, the Cybersecurity department will establish regular reporting by the Cybersecurity Manager, conduct periodic audits, or form a Cybersecurity Steering Committee for oversight.	لضمان الامتثال، سينشئ قسم الأمن السيبراني نظامًا لتقديم تقارير منتظمة يُعدّها مدير الأمن السيبراني، ويجري عمليات تدقيق دورية، أو يشكل لجنة توجيهية للأمن السيبراني للإشراف.
119	Translated (100%)	The CS manager shall ensure adherence to this policy.	يتعين على مدير الأمن السيبراني ضمان الالتزام بهذه السياسة.

120	Translated (100%)	All employees of Al Hammadi Holding must adhere to this policy.	.على جميع موظفي شركة الحمادي القابضة الالتزام بهذه السياسة
121	Translated (100%)	Violations of this policy may result in legal action in any jurisdiction or other measures as deemed appropriate by the Al Hammadi Holding.	قد تؤدي انتهاكات هذه السياسة إلى اتخاذ إجراءات قانونية في أي ولاية قضائية أو غيرها من التدابير التي تراها شركة الحمادي القابضة مناسبة.
122	Translated (100%)	Exceptions	الاستثناءات
123	Translated (100%)	Violation of cybersecurity policies and standards is prohibited unless a prior justified exception is obtained from the Cybersecurity Department or the Cybersecurity Steering Committee.	يُحظر انتهاك سياسات ومعايير الأمن السيبراني ما لم يتم الحصول على استثناء مبرر مسبق من إدارة الأمن السيبراني أو اللجنة التوجيهية للأمن السيبراني.
124	Translated (100%)	In case of a conflict, applicable legislative and regulatory requirements overrule Al Hammadi Holding policies and standards.	في حالة وجود تعارض، فإن المتطلبات التشريعية والتنظيمية المعمول بها تسود على سياسات ومعايير شركة الحمادي القابضة.
125	Translated (100%)	Revision	المراجعة
126	Translated (100%)	This policy is reviewed annually, after major changes in Al Hammadi Holding's organizational chart or infrastructure, and more frequently whenever required, to ensure it remains appropriate and current for Al Hammadi Holding, ISO 27001, and NCA requirements	تخضع هذه السياسة لمراجعة سنوية، ولإعادة التقييم بعد أي تغييرات جوهرية في الهيكل التنظيمي أو البنية التحتية لشركة الحمادي القابضة، إضافة إلى مراجعات دورية إضافية عند الضرورة، وذلك لضمان توافقها المستمر مع متطلبات شركة الحمادي القابضة، ومعيار آيزو ISO 27001:2022، وإرشادات الهيئة الوطنية للأمن السيبراني
127	Translated (100%)	Approval Section	قسم الاعتماد
128	Translated (100%)	Prepared by:	إعداد:
129	Translated (100%)	Mr. Mohammed Alamer	السيد/ محمد العامر
130	Translated (100%)	GRC Cybersecurity Specialist	أخصائي حوكمة ومخاطر وامتثال في الأمن السيبراني
131	Translated (100%)	Name	الاسم
132	Translated (100%)	Designation	المسمى الوظيفي
133	Translated (100%)	Signature	التوقيع
134	Translated (100%)	Date	التاريخ
135	Translated (100%)	Reviewed by:	راجعها:
136	Translated (100%)	Mr. Majid Al Nahdi	السيد/ ماجد النهدي
137	Translated	Manager, Human Resources	مدير الموارد البشرية

	(0%)		
138	Translated (100%)	Name	الاسم
139	Translated (100%)	Designation	المسمى الوظيفي
140	Translated (100%)	Signature	التوقيع
141	Translated (100%)	Date	التاريخ
142	Translated (100%)	Reviewed by:	راجعها:
143	Translated (100%)	Ms. Mashael Alotaibi	السيدة/ مشاعل العتيبي
144	Translated (0%)	Manager, Cybersecurity	مدير الأمن السيبراني
145	Translated (100%)	Name	الاسم
146	Translated (100%)	Designation	المسمى الوظيفي
147	Translated (100%)	Signature	التوقيع
148	Translated (100%)	Date	التاريخ
149	Translated (100%)	Approved by:	اعتمدها:
150	Translated (100%)	Dr. Abdulaziz Al Hammadi	الحمادي<Bold><Bold></Bold></Bold> د./ عبد العزيز<Bold><Bold></Bold></Bold>
151	Translated (100%)	Chief Operating Officer	الرئيس التنفيذي للعمليات
152	Translated (100%)	Name	الاسم
153	Translated (100%)	Designation	المسمى الوظيفي
154	Translated (100%)	Signature	التوقيع
155	Translated (100%)	Date	التاريخ
156	Translated (100%)	Approved by:	اعتمدها:

157	Translated (100%)	Mr. Mohammad Al Hammadi	السيد/ محمد الحمادي
158	Translated (100%)	Chief Executive Officer	الرئيس التنفيذي
159	Translated (100%)	Name	الاسم
160	Translated (100%)	Designation	المسمى الوظيفي
161	Translated (100%)	Signature	التوقيع
162	Translated (100%)	Date	التاريخ

Segment ID	Segment status	Source segment	Target segment
1	Translated (0%)	<3/> <26><6>Risk Management<10/><14/> Policy </6></26>	<3/> <26><6><10/><14/> 26/><6/> <سياسة إدارة المخاطر
2	Translated (100%)	Page <37><28/> of <36/></37>	<صفحة </28><37> من <37/></36>
3	Translated (100%)	Al Hammadi Holding	شركة الحمادي القابضة
4	Translated (0%)	Cybersecurity Risk Management Policy	سياسة إدارة مخاطر الأمن السيبراني
5	Translated (100%)	CYBERSECURITY DEPARTMENT	إدارة الأمن السيبراني
6	Translated (100%)	Policy ID	معرّف السياسة
7	Translated (100%)	AHH-CS-ISMS-002	AHH-CS-ISMS-002
8	Translated (100%)	Class	الفئة
9	Translated (100%)	Internal Release	إصدار داخلي
10	Not Translated (0%)		
11	Translated (100%)	V0.1	V0.1
12	Translated (100%)	Published at	نُشرت في
13	Translated (100%)	April 2025	أبريل 2025
14	Translated (100%)	Document Owner	المسؤول عن المستند
15	Translated (0%)	Cybersecurity <131>Department</131>	إدارة<131/> الأمن السيبراني<131>
16	Translated (100%)	Disclaimer	تنويه
17	Translated (100%)	The information contained in this document is property of Al Hammadi Holding and must not be copied or communicated to a third party or used for any purpose other than that for which it is supplied, without the written consent of Al Hammadi Holding.	المعلومات الواردة في هذا المستند هي ملك لشركة الحمادي القابضة ولا يجوز نسخها أو إبلاغها إلى طرف ثالث أو استخدامها لأي غرض آخر غير الغرض الذي تم توفيرها من أجله، دون موافقة خطية من شركة الحمادي القابضة.

18	Translated (100%)	Contents	جدول المحتويات
19	Translated (100%)	Document Control	ضبط المستندات
20	Translated (100%)	Document Information	معلومات المستند
21	Translated (100%)	Synopsis	الملخص
22	Translated (100%)	Document Title:	:عنوان المستند
23	Translated (0%)	Risk Management Internal Organization	التنظيم الداخلي لإدارة المخاطر
24	Translated (100%)	Document Status:	:حالة المستند
25	Translated (100%)	Approved	معتمد
26	Translated (100%)	Document Effective Date:	:تاريخ سريان المستند
27	Translated (100%)	April 2025	أبريل 2025
28	Translated (100%)	Document Issue Date:	:تاريخ إصدار المستند
29	Translated (100%)	April 2025	أبريل 2025
30	Translated (100%)	Document Next Revision Date:	:تاريخ المراجعة التالية للمستند
31	Translated (100%)	December 2025	ديسمبر 2025
32	Translated (100%)	Key contacts	جهات التواصل الرئيسية
33	Translated (100%)	Document Owner:	:المسؤول عن المستند
34	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
35	Translated (100%)	Approval Authority	جهة الاعتماد
36	Translated (100%)	Document Created by:	:مُنشئ المستند
37	Translated	Cybersecurity Department	إدارة الأمن السيبراني

	(100%)		
38	Translated (100%)	Document Reviewed by:	:راجع المستند
39	Translated (0%)	Al Hammadi Holding CS Manager	مدير الأمن السيبراني في شركة الحمادي القابضة
40	Translated (100%)	Document Approved by:	:اعتمد المستند
41	Translated (100%)	Al Hammadi Holding COO & CEO	الرئيس التنفيذي للعمليات والرئيس التنفيذي في شركة الحمادي القابضة
42	Translated (100%)	Note:	:ملاحظة
43	Translated (100%)	Any additional approval will be added in the document annex	تُضاف أي اعتمادات إضافية في ملحق المستند
44	Translated (100%)	Classification	التصنيف
45	Translated (100%)	Company Internal – to be shared with 3rd parties after consent of CS Manager	داخلي لاستخدام للشركة – يُسمح بمشاركته مع جهات خارجية بعد موافقة مدير إدارة الأمن السيبراني
46	Translated (100%)	Version / Dates	الإصدار / التواريخ
47	Translated (100%)	Current Version:	:الإصدار الحالي
48	Translated (100%)	V 1.0	V 1.0
49	Translated (100%)	Date Published:	:تاريخ النشر
50	Translated (100%)	April 2025	أبريل 2025
51	Translated (100%)	Date of Next Review:	:تاريخ المراجعة التالية
52	Translated (100%)	April 2026	أبريل 2026
53	Translated (100%)	Document Changes	التغييرات على المستند
54	Translated (100%)	Date	التاريخ
55	Translated (100%)	Version	الإصدار
56	Translated (100%)	Document Owner	المسؤول عن المستند

57	Translated (100%)	Change Description	وصف التغيير
58	Translated (100%)	April 2025	أبريل 2025
59	Translated (100%)	1.0	1.0
60	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
61	Translated (0%)	Document Established	تم إنشاء المستند
62	Translated (100%)	Document Circulation	تعميم المستند
63	Translated (100%)	To	إلى
64	Translated (100%)	Date	التاريخ
65	Translated (100%)	Method	الطريقة
66	Translated (100%)	IT Staff	موظفو تكنولوجيا المعلومات
67	Translated (100%)	April 2025	أبريل 2025
68	Translated (100%)	Intranet Portal	بوابة الإنترانت
69	Translated (100%)	All Al Hammadi Staff	جميع موظفي شركة الحمادي
70	Translated (100%)	April 2025	أبريل 2025
71	Translated (100%)	Intranet Portal	بوابة الإنترانت
72	Translated (100%)	Objectives	الأهداف
73	Translated (0%)	The purpose of this policy is to establish principles and procedural implementation guidelines through which Al Hammadi Holding identifies and manages risks effectively.	الغرض من هذه السياسة هو وضع مبادئ وإرشادات تنفيذ إجرائية تحدد من خلالها شركة الحمادي القابضة المخاطر وتديرها بفعالية.
74	Translated (0%)	This ensures management's direction and support for risk management in alignment with business requirements, relevant laws and regulations, and compliance with the requirements such as:	وهذا يضمن توجيه الإدارة ودعمها لإدارة المخاطر بما يتماشى مع متطلبات العمل والقوانين واللوائح ذات الصلة والامتثال للمتطلبات مثل:
75	Translated	(NCA, NIST, ISO27005, and ISO31000)	(NCA وNIST وISO 27005 وISO 31000)

	(0%)		
76	Translated (0%)	Key Outcomes of Implementing the Principles and Procedural	النتائج الرئيسية لتنفيذ المبادئ والإجراءات
77	Translated (0%)	This Policy adheres to the national legislative and regulatory requirements and is a legislative requirement as stated in Control No. (ECC 1-5-1) of the Essential Cybersecurity Controls (ECC-1:2018) issued by the National Cybersecurity Authority.	تلتزم هذه السياسة بالمتطلبات التشريعية والتنظيمية الوطنية وهي من (ECC 1-5-1) .مطلب تشريعي كما هو مذكور في الضابط رقم الصادرة عن الهيئة (ECC -1:2018) ضوابط الأمن السيبراني الأساسية .الوطنية للأمن السيبراني
78	Translated (0%)	Protecting Al Hammadi 's digital data and assets from cybersecurity risks.	.حماية بيانات وأصول شركة الحمادي الرقمية من مخاطر الأمن السيبراني
79	Translated (100%)	Scope	النطاق
80	Translated (0%)	This policy applies to all Al Hammadi Holding Cybersecurity Management operations, assets, and activities, including employees, contractors, suppliers, and third parties under its control.	تنطبق هذه السياسة على جميع عمليات وأصول وأنشطة إدارة الأمن السيبراني لشركة الحمادي القابضة، بما في ذلك الموظفين والمتعاقدين .والموردين والجهات الخارجية الخاضعة لسيطرتها
81	Translated (0%)	It covers all IT systems, Healthcare Systems, information assets, and operational risks relevant to ensuring patient safety, employee well-being, compliance with legal standards, and operational continuity.	وهو يغطي جميع أنظمة تكنولوجيا المعلومات وأنظمة الرعاية الصحية وأصول المعلومات والمخاطر التشغيلية ذات الصلة بضمان سلامة المرضى ورفاهية الموظفين والامتثال للمعايير القانونية واستمرارية .التشغيل
82	Translated (100%)	Roles and Responsibilities	الأدوار والمسؤوليات
83	Translated (0%)	Al Hammadi Holding management is responsible for implementing, maintaining, and updating this policy with all its contents, in accordance with any changes in the Statement of Applicability, Al Hammadi Holding-SOA Document.	تتحمل إدارة شركة الحمادي القابضة مسؤولية تنفيذ هذه السياسة وحفظها وتحديثها بكامل محتوياتها، وذلك بما يتماشى مع أي تغييرات في .بيان التطبيق الخاص بشركة الحمادي القابضة
84	Translated (100%)	Principles	المبادئ
85	Translated (0%)	Controls for Risk Management	ضوابط إدارة المخاطر
86	Translated (0%)	<567>Al Hammadi Holding's Cybersecurity management</567> <576>will establish a set of Cybersecurity Risk Management policies, which must be approved by the cybersecurity department, published, and communicated to employees and relevant external parties.</576>	<567>ستضع <567>إدارة الأمن السيبراني في شركة الحمادي القابضة</567/> مجموعة من سياسات إدارة مخاطر الأمن السيبراني، والتي يجب<576> أن تتم الموافقة عليها من قبل إدارة الأمن السيبراني ونشرها وإبلاغها <للموظفين والأطراف الخارجية ذات الصلة.</576/>
87	Translated (0%)	These controls are designed to identify, assess, monitor, and mitigate risks to ensure patient safety, employee well-being, compliance with legal standards, and operational continuity.	تم تصميم هذه الضوابط لتحديد المخاطر وتقييمها ومراقبتها والتخفيف من حدتها لضمان سلامة المرضى ورفاهية الموظفين والامتثال للمعايير .القانونية واستمرارية التشغيل
88	Translated (0%)	Regular communication about this policy should be ensured, with updates being regularly reviewed and effectively communicated to all concerned parties.	يجب ضمان التواصل المنتظم حول هذه السياسة، مع مراجعة التحديثات .بانتظام وإبلاغها بشكل فعال إلى جميع الأطراف المعنية
89	Translated	General Requirements	المتطلبات العامة

	(0%)		
90	Translated (0%)	The Cybersecurity Department must develop, document, and approve the Cybersecurity Risk Management Methodology and procedures for managing cybersecurity risks in Al Hammadi, using the standard of the National Cybersecurity Authority.	يجب على إدارة الأمن السيبراني تطوير وتوثيق واعتماد منهجية وإجراءات إدارة مخاطر الأمن السيبراني في الحمادي، باستخدام معيار الهيئة الوطنية للأمن السيبراني.
91	Translated (0%)	Internationally approved guiding standards may be used, such as:	يمكن استخدام المعايير التوجيهية المعتمدة دوليًا، مثل:
92	Translated (0%)	(NIST, ISO27005, and ISO31000) in developing a methodology for managing cybersecurity risks.	في (ISO31000، ISO27005، المعهد الوطني للمعايير والتكنولوجيا) تطوير منهجية لإدارة مخاطر الأمن السيبراني.
93	Translated (0%)	The Cybersecurity Risk Management methodology shall cover the following, as a minimum:	يجب أن تغطي منهجية إدارة مخاطر الأمن السيبراني ما يلي، كحد أدنى:
94	Translated (0%)	Identifying technical and digital assets and the degree of their importance and criticality.	تحديد الأصول التقنية والرقمية ودرجة أهميتها وأهميتها.
95	Translated (0%)	Identifying and assessing cyber risks affecting the business, assets, data, or employees of Al Hammadi.	تحديد وتقييم المخاطر السيبرانية التي تؤثر على الأعمال أو الأصول أو البيانات أو موظفي الحمادي.
96	Translated (0%)	Identifying and evaluating cybersecurity threats and vulnerabilities that may affect technical and digital assets.	تحديد وتقييم تهديدات الأمن السيبراني ونقاط الضعف التي قد تؤثر على الأصول التقنية والرقمية.
97	Translated (0%)	Determining options for addressing cyber risks.	تحديد خيارات معالجة المخاطر السيبرانية.
98	Translated (0%)	Determining remediation plans for cyber risks on Al Hammadi 's assets.	تحديد خطط معالجة المخاطر السيبرانية على أصول الحمادي.
99	Translated (0%)	Categorizing and defining cyber risk levels based on the level of impact and likelihood of the threat occurring to Al Hammadi.	تصنيف وتحديد مستويات المخاطر السيبرانية بناءً على مستوى التأثير واحتمال حدوث تهديد للحمادي.
100	Translated (0%)	Creating a Cybersecurity Risk Register to document and follow up on cyber risks.	إنشاء سجل مخاطر الأمن السيبراني لتوثيق ومتابعة المخاطر السيبرانية.
101	Translated (0%)	Defining roles and responsibilities for managing cybersecurity risks.	تحديد الأدوار والمسؤوليات لإدارة مخاطر الأمن السيبراني.
102	Translated (0%)	The Cybersecurity Department must identify events or circumstances that may violate the confidentiality, integrity and availability of information and technical assets, including identifying information and technical assets, potential threats and related vulnerabilities, approved controls, and then determine the effects resulting from the loss of confidentiality, integrity and availability of these assets.	يجب على إدارة الأمن السيبراني تحديد الأحداث أو الظروف التي قد تنتهك سرية وسلامة وتوافر المعلومات والأصول الفنية، بما في ذلك تحديد المعلومات والأصول الفنية والتهديدات المحتملة ونقاط الضعف ذات الصلة والضوابط المعتمدة، ومن ثم تحديد الآثار الناتجة عن فقدان سرية وسلامة وتوافر هذه الأصول.
103	Translated (0%)	The Cybersecurity Department must conduct a risk assessment periodically (at least quarterly) to ensure the protection of information and technical assets, and to deal with risks according to priority.	يجب على إدارة الأمن السيبراني إجراء تقييم للمخاطر بشكل دوري (ربع سنوي على الأقل) لضمان حماية المعلومات والأصول الفنية، والتعامل مع المخاطر حسب الأولوية.
104	Translated (0%)	The Cybersecurity Department shall implement, at a minimum, cybersecurity risk assessment procedures in the following cases:	يجب على إدارة الأمن السيبراني، كحد أدنى، تنفيذ إجراءات تقييم مخاطر الأمن السيبراني في الحالات التالية:
105	Translated	In the early stages of technical projects and industrial control operating	في المراحل الأولى من المشاريع الفنية ومشاريع نظام تشغيل التحكم

	(0%)	system projects.	.الصناعي
106	Translated (0%)	Before making a fundamental change in the technical architecture and operating systems of industrial control and its components.	قبل إجراء تغيير جوهري في البنية الفنية وأنظمة تشغيل التحكم الصناعي .ومكوناته
107	Translated (0%)	When planning to obtain services from a third party.	.عند التخطيط للحصول على خدمات من طرف ثالث
108	Translated (0%)	When planning and prior to launching new services.	.عند التخطيط وقبل إطلاق خدمات جديدة
109	Translated (0%)	The Cybersecurity Department shall reassess and update the risks as follows:	تقوم إدارة الأمن السيبراني بإعادة تقييم المخاطر وتحديثها على النحو :التالي
110	Translated (0%)	After a cyber incident has occurred and caused damage to the availability, confidentiality, and integrity of Al Hammadi 's data.	بعد وقوع حادث إلكتروني وتسبب في الإضرار بتوافر بيانات الحمادي .وسريتها وسلامتها
111	Translated (0%)	After obtaining audit results or proactive information.	.بعد الحصول على نتائج التدقيق أو المعلومات الاستباقية
112	Translated (0%)	In the event of a change to information and technical assets, and operating systems.	.في حالة حدوث تغيير في المعلومات والأصول التقنية وأنظمة التشغيل
113	Translated (0%)	The Cybersecurity Department shall assess the likelihood of threats and potential impacts on Al Hammadi 's assets, as follows:	تقوم إدارة الأمن السيبراني بتقييم احتمالية التهديدات والآثار المحتملة :على أصول الحمادي، على النحو التالي
114	Translated (0%)	The results of this assessment shall be used to determine the overall level of cyber risks and risk appetite.	يجب استخدام نتائج هذا التقييم لتحديد المستوى العام للمخاطر .السيبرانية ومدى تقبلها للمخاطر
115	Translated (0%)	Measuring the inherent risks faced by Al Hammadi for each identified cyber risk, including probability, impact, and correct classification of the risk.	،قياس المخاطر الكامنة التي يواجهها الحمادي لكل خطر إلكتروني محدد .بما في ذلك الاحتمال والتأثير والتصنيف الصحيح للمخاطر
116	Translated (0%)	Consultation with risk owners during the evaluation process.	.التشاور مع المسؤولين عن المخاطر أثناء عملية التقييم
117	Translated (0%)	The Cybersecurity Department shall identify, document and evaluate the controls in place which have been implemented to reduce the impact or likelihood of cyber risks occurring in Al Hammadi.	يجب على إدارة الأمن السيبراني تحديد وتوثيق وتقييم الضوابط المعمول بها والتي تم تنفيذها للحد من تأثير أو احتمال حدوث المخاطر السيبرانية .في الحمادي
118	Translated (0%)	The Cybersecurity Department uses the Key Performance Indicator (KPI) to ensure the effectiveness of Cybersecurity Risk Management.	لضمان فعالية (KPI) تستخدم إدارة الأمن السيبراني مؤشر الأداء الرئيسي .إدارة مخاطر الأمن السيبراني
119	Translated (0%)	The Cybersecurity Department shall define and document risk appetite criteria, according to the level of risk and the cost of addressing the risk against its impact.	،يجب على إدارة الأمن السيبراني تحديد وتوثيق معايير تقبل المخاطر .وفقًا لمستوى المخاطر وتكلفة معالجة المخاطر مقابل تأثيرها
120	Translated (0%)	The Cybersecurity Department shall ensure that appropriate remediation plans are implemented in order to reduce the risk to an acceptable level in case the remaining risk does not meet the risk appetite criteria.	يجب على إدارة الأمن السيبراني التأكد من تنفيذ خطط الإصلاح المناسبة من أجل تقليل المخاطر إلى مستوى مقبول في حالة عدم استيفاء .المخاطر المتبقية لمعايير الرغبة في المخاطرة
121	Translated (0%)	The Cybersecurity Department shall review and update the methodology and procedures for managing cybersecurity risks at planned intervals (or in the event of changes in legislative and regulatory requirements and related standards), and the changes shall be documented and approved.	تقوم إدارة الأمن السيبراني بمراجعة وتحديث منهجية وإجراءات إدارة مخاطر الأمن السيبراني على فترات مخططة (أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية والمعايير ذات الصلة)، ويجب توثيق .التغييرات واعتمادها

122	Translated (0%)	The Cybersecurity Department shall annually review the Cybersecurity Risk Management Policy, and document and approve changes.	يجب على إدارة الأمن السيبراني مراجعة سياسة إدارة مخاطر الأمن السيبراني سنويًا، وتوثيق التغييرات والموافقة عليها.
123	Translated (0%)	Cyber Risk Assessment	تقييم المخاطر السيبرانية
124	Translated (0%)	The Cybersecurity Department must ensure that the following provisions are applied:	يجب على إدارة الأمن السيبراني التأكد من تطبيق الأحكام التالية:
125	Translated (0%)	Reviewing and approving the risk identification results in accordance with the Risk Assessment Methodology.	مراجعة واعتماد نتائج تحديد المخاطر وفقًا لمنهجية تقييم المخاطر.
126	Translated (0%)	Evaluating the effectiveness of existing controls.	تقييم فعالية الضوابط القائمة.
127	Translated (0%)	Evaluating the residual risks faced by Al Hammadi for each identified risk.	تقييم المخاطر المتبقية التي يواجهها الحمادي لكل خطر محدد.
128	Translated (0%)	Determining whether the risks are within the limits of risk tolerance or risk appetite.	تحديد ما إذا كانت المخاطر ضمن حدود تحمل المخاطر أو الرغبة في المخاطرة.
129	Translated (0%)	Determining the cyber risk response strategy.	تحديد استراتيجية الاستجابة للمخاطر السيبرانية.
130	Translated (0%)	The degree of risk must be addressed or reduced by applying the necessary controls to reduce the likelihood of occurrence, impact, or both.	يجب معالجة درجة المخاطر أو تقليلها من خلال تطبيق الضوابط اللازمة لتقليل احتمالية الحدوث أو التأثير أو كليهما.
131	Translated (0%)	Determining and documenting risk treatment options based on the results of risk assessment, implementation cost and expected benefits.	تحديد وتوثيق خيارات معالجة المخاطر بناءً على نتائج تقييم المخاطر وتكلفة التنفيذ والفوائد المتوقعة.
132	Translated (0%)	Following up on Cybersecurity Risks	متابعة مخاطر الأمن السيبراني
133	Translated (0%)	The Cybersecurity Department must prepare and document a Cybersecurity Risk Register that contains the following data:	يجب على إدارة الأمن السيبراني إعداد وتوثيق سجل مخاطر الأمن السيبراني الذي يحتوي على البيانات التالية:
134	Translated (0%)	Scope of cyber risk.	نطاق المخاطر السيبرانية.
135	Translated (0%)	Administrator or risk owner.	المسؤول أو المسؤول عن المخاطر.
136	Translated (0%)	A description of the cyber risks, including their causes and effects.	وصف للمخاطر السيبرانية، بما في ذلك أسبابها وآثارها.
137	Translated (0%)	An analysis of cyber risks, showing the effects resulting from the risks.	تحليل للمخاطر السيبرانية، يوضح الآثار الناتجة عن المخاطر.
138	Translated (0%)	Assessment and classification of risks, including the probability of the risk, its size and the overall rating if it occurs.	تقييم المخاطر وتصنيفها، بما في ذلك احتمالية المخاطر وحجمها والتصنيف العام في حالة حدوثها.
139	Translated (0%)	The risk handling plan, including the procedure for dealing with it and the person responsible for it.	خطة التعامل مع المخاطر، بما في ذلك إجراءات التعامل معها والشخص المسؤول عنها.
140	Translated (0%)	Controls effectiveness	يتحكم في الفعالية

141	Translated (0%)	Description of residual risk and residual risk score	وصف المخاطر المتبقية ودرجة المخاطر المتبقية
142	Translated (0%)	Any other attributes that can support in evaluating and monitoring the cybersecurity risks status.	أي سمات أخرى يمكن أن تدعم في تقييم ومراقبة حالة مخاطر الأمن السيبراني.
143	Translated (0%)	<933><931>Cybersecurity Risk Management Controls for Critical Systems</931></933><936> and Data</936>	ضوابط إدارة مخاطر الأمن السيبراني للأنظمة<933><931> والبيانات</936> الحرجة <936><933></931>
144	Translated (0%)	The Cybersecurity Department shall establish and monitor a Cybersecurity Risk Register for critical systems and data at least once a month and include this in the Cybersecurity Risk Management methodology.	يجب على إدارة الأمن السيبراني إنشاء ومراقبة سجل مخاطر الأمن السيبراني للأنظمة والبيانات الهامة مرة واحدة على الأقل شهريًا وإدراجه في منهجية إدارة مخاطر الأمن السيبراني.
145	Translated (0%)	The Cybersecurity Department shall implement a cybersecurity risk assessment procedure on critical systems and critical data, at least once every three months.	يجب على إدارة الأمن السيبراني تنفيذ إجراء تقييم مخاطر الأمن السيبراني على الأنظمة الهامة والبيانات الهامة، مرة واحدة على الأقل كل ثلاثة أشهر.
146	Translated (0%)	Cybersecurity Risk Management Controls for Industrial Control Systems	ضوابط إدارة مخاطر الأمن السيبراني لأنظمة التحكم الصناعية
147	Translated (0%)	The Cybersecurity Department shall establish an Industrial Control Systems (OT/ICS) Cybersecurity Risk Management Methodology within Al Hammadi 's Risk Management and Safety Risk Management Methodology and Procedures.	يجب على إدارة الأمن السيبراني إنشاء منهجية لإدارة مخاطر الأمن السيبراني لأنظمة التحكم الصناعي (OT/ICS) ضمن منهجية وإجراءات إدارة المخاطر والسلامة في الحمادي.
148	Translated (0%)	The Cybersecurity Department must annually assess the cybersecurity risks of Industrial Control Systems, making sure to include the risks of signing contracts and agreements with third parties related to Industrial Control Systems, or when changes occur in relevant legislative and regulatory requirements as part of the assessment.	يجب على إدارة الأمن السيبراني تقييم مخاطر الأمن السيبراني لأنظمة التحكم الصناعي سنويًا، مع التأكد من تضمين مخاطر توقيع العقود والاتفاقيات مع أطراف ثالثة تتعلق بأنظمة التحكم الصناعي، أو عند حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات الصلة كجزء من التقييم.
149	Translated (0%)	The Cybersecurity Department shall establish a register of cybersecurity risks related to Industrial Control Systems.	تقوم إدارة الأمن السيبراني بإنشاء سجل لمخاطر الأمن السيبراني المتعلقة بأنظمة التحكم الصناعي.
150	Translated (0%)	In the event that it is not possible to meet the cybersecurity requirements within the environment of Industrial Control Systems, the concerned department or division must clarify the necessary justifications, with documentation and approval by the Cybersecurity Department, and the approval of the Cybersecurity Supervisory Committee and the Authorized Person.	في حالة تعذر تلبية متطلبات الأمن السيبراني ضمن بيئة أنظمة التحكم الصناعي، يجب على الإدارة أو القسم المعني توضيح المبررات اللازمة، مع التوثيق والموافقة من قبل إدارة الأمن السيبراني، وموافقة لجنة الإشراف على الأمن السيبراني والشخص المفوض.
151	Translated (0%)	In the event that it is approved to accept cyber risks, alternative/compensation controls must be identified, documented and approved by the Cybersecurity Supervisory Committee and the Authorized Person.	في حالة الموافقة على قبول المخاطر السيبرانية، يجب تحديد ضوابط بديلة/تعويض وتوثيقها والموافقة عليها من قبل لجنة الإشراف على الأمن السيبراني والشخص المفوض.
152	Translated (0%)	The Cybersecurity Department shall ensure that alternative/compensation controls are applied effectively at a specified time while continuing to assess and review those risks on an ongoing	يجب على إدارة الأمن السيبراني التأكد من تطبيق الضوابط البديلة/التعويضات بشكل فعال في وقت محدد مع الاستمرار في تقييم ومراجعة تلك المخاطر على أساس مستمر.

		basis.	
153	Translated (0%)	Cybersecurity Risk Management Controls for Remote Work	ضوابط إدارة مخاطر الأمن السيبراني للعمل عن بعد
154	Translated (0%)	The Cybersecurity Department shall assess the cybersecurity risks of remote work systems at least once a year.	يجب على إدارة الأمن السيبراني تقييم مخاطر الأمن السيبراني لأنظمة العمل عن بعد مرة واحدة على الأقل في السنة.
155	Translated (0%)	The Cybersecurity Department shall assess the cybersecurity risks when planning and before approving the remote work of any service or system.	تقوم إدارة الأمن السيبراني بتقييم مخاطر الأمن السيبراني عند التخطيط وقبل الموافقة على العمل عن بعد لأي خدمة أو نظام.
156	Translated (0%)	The Cybersecurity Department shall include cyber risks in relation to systems and remote work services in Al Hammadi 's Cybersecurity Risk Register and follow it up at least once a year.	يجب على إدارة الأمن السيبراني تضمين المخاطر السيبرانية فيما يتعلق بالأنظمة وخدمات العمل عن بعد في سجل مخاطر الأمن السيبراني في الحمادي ومتابعته مرة واحدة على الأقل في السنة.
157	Translated (0%)	Procedural Guidelines	المبادئ التوجيهية الإجرائية
158	Translated (0%)	Cybersecurity procedures for risk management	إجراءات الأمن السيبراني لإدارة المخاطر
159	Translated (0%)	The Cybersecurity Department shall adhere to the following procedures:	تلتزم إدارة الأمن السيبراني بالإجراءات التالية:
160	Translated (0%)	<1035>Determine the businesses, technological, and digital assets, industrial control systems, or employees in Al Hammadi on which cybersecurity risk assessments must be conducted based on their classification, document the scope of risk assessment work, develop an annual plan for risk assessment, obtain the approval of the Head of the Cybersecurity Department on the plan, and share it with the Cybersecurity </1035>Steering <1056>Committee and relevant parties.</1056>	تحديد الأعمال أو الأصول التكنولوجية والرقمية أو أنظمة<1035> التحكم الصناعي أو الموظفين في الحمادي التي يجب إجراء تقييمات مخاطر الأمن السيبراني بناءً على تصنيفها، وتوثيق نطاق عمل تقييم المخاطر، ووضع خطة سنوية لتقييم المخاطر، والحصول على موافقة رئيس إدارة الأمن السيبراني على الخطة، ومشاركتها مع </1035> اللجنة التوجيهية للأمن السيبراني والجهات ذات الصلة<1056>. </1056>
161	Translated (0%)	Assess cybersecurity risks to all of the Corporation's digital and technological business and assets, networks, and industrial control systems based on cybersecurity requirements.	تقييم مخاطر الأمن السيبراني على جميع الأعمال الرقمية والتكنولوجية للمؤسسة وأصولها وشبكاتها وأنظمة التحكم الصناعي بناءً على متطلبات الأمن السيبراني.
162	Translated (0%)	Share Cybersecurity Requirements with third parties who will collaborate with Al Hammadi before starting the project.	مشاركة متطلبات الأمن السيبراني مع أطراف ثالثة ستتعاون مع الحمادي قبل بدء المشروع.
163	Translated (0%)	Conduct a cybersecurity risk assessment before starting any project with third party.	إجراء تقييم لمخاطر الأمن السيبراني قبل بدء أي مشروع مع طرف ثالث.
164	Translated (0%)	Cybersecurity risk assessment procedures	إجراءات تقييم مخاطر الأمن السيبراني
165	Translated (0%)	Identify events or circumstances that may violate the confidentiality, integrity, and availability of information and technological assets, including identifying digital and technological assets and industrial control systems, potential threats and related vulnerabilities, and approved controls, and then determining the effects resulting from the loss of confidentiality, integrity, and availability of these assets.	تحديد الأحداث أو الظروف التي قد تنتهك سرية وسلامة وتوافر المعلومات والأصول التكنولوجية، بما في ذلك تحديد الأصول الرقمية والتكنولوجية وأنظمة التحكم الصناعي والتهديدات المحتملة ونقاط الضعف ذات الصلة والضوابط المعتمدة، ومن ثم تحديد الآثار الناتجة عن فقدان سرية وسلامة وتوافر هذه الأصول.

166	Translated (0%)	Identify the cyber risk response strategy and the controls that will be implemented to reduce the impact or likelihood of the cyber risk occurring in Al Hammadi, document them in the cybersecurity risk register based on the classification of Al Hammadi's business and assets and based on the cybersecurity requirements, share it with the Cybersecurity Supervisory Committee for approval, and with the relevant parties for implementation and application.	تحديد استراتيجية الاستجابة للمخاطر السيبرانية والضوابط التي سيتم تنفيذها للحد من تأثير أو احتمالية حدوث المخاطر السيبرانية في الحمادي، وتوثيقها في سجل مخاطر الأمن السيبراني بناءً على تصنيف أعمال وأصول الحمادي وبناءً على متطلبات الأمن السيبراني، ومشاركتها مع لجنة الإشراف على الأمن السيبراني للموافقة عليها، ومع الأطراف ذات الصلة للتنفيذ والتطبيق.
167	Translated (0%)	Monitor cybersecurity risks	مراقبة مخاطر الأمن السيبراني
168	Translated (0%)	Review the cybersecurity risk register every Three months and ensure that it is followed up based on cybersecurity requirements and according to business and asset classification.	مراجعة سجل مخاطر الأمن السيبراني كل ثلاثة أشهر والتأكد من متابعته بناءً على متطلبات الأمن السيبراني ووفقًا لتصنيف الأعمال والأصول.
169	Translated (0%)	Test and evaluate remediation plans and applied controls every three months and share reports with the Cybersecurity Supervisory Committee and relevant parties.	اختبار وتقييم خطط الإصلاح والضوابط المطبقة كل ثلاثة أشهر ومشاركة التقارير مع لجنة الإشراف على الأمن السيبراني والأطراف ذات الصلة.
170	Translated (0%)	Evaluate the residual risks faced by Al Hammadi for each specific risk every six months, determine whether the risks are within the boundaries of tolerance or acceptability, and share the reports with the Cybersecurity Supervisory Committee and relevant parties.	تقييم المخاطر المتبقية التي يواجهها الحمادي لكل خطر محدد كل ستة أشهر، وتحديد ما إذا كانت المخاطر ضمن حدود التسامح أو القبول، ومشاركة التقارير مع لجنة الإشراف على الأمن السيبراني والأطراف ذات الصلة.
171	Translated (100%)	Compliance and Adherence	الامتثال والالتزام
172	Translated (100%)	Al Hammadi Holding CEO shall ensure compliance with the cybersecurity policies and standards.	يضمن الرئيس التنفيذي لشركة الحمادي القابضة الامتثال لسياسات ومعايير الأمن السيبراني.
173	Translated (100%)	To ensure compliance, the Cybersecurity department will establish regular reporting by the Cybersecurity Manager, conduct periodic audits, or form a Cybersecurity Steering Committee for oversight.	لضمان الامتثال، سينشئ قسم الأمن السيبراني نظامًا لتقديم تقارير منتظمة يُعدّها مدير الأمن السيبراني، ويجري عمليات تدقيق دورية، أو يشكل لجنة توجيهية للأمن السيبراني للإشراف.
174	Translated (100%)	The CS manager shall ensure adherence to this policy.	يتعين على مدير الأمن السيبراني ضمان الالتزام بهذه السياسة.
175	Translated (100%)	All employees of Al Hammadi Holding must adhere to this policy.	على جميع موظفي شركة الحمادي القابضة الالتزام بهذه السياسة.
176	Translated (100%)	Violations of this policy may result in legal action in any jurisdiction or other measures as deemed appropriate by the Al Hammadi Holding.	قد تؤدي انتهاكات هذه السياسة إلى اتخاذ إجراءات قانونية في أي ولاية قضائية أو غيرها من التدابير التي تراها شركة الحمادي القابضة مناسبة.
177	Translated (100%)	Exceptions	الاستثناءات
178	Translated (100%)	Violation of cybersecurity policies and standards is prohibited unless a prior justified exception is obtained from the Cybersecurity Department or the Cybersecurity Steering Committee.	يُحظر انتهاك سياسات ومعايير الأمن السيبراني ما لم يتم الحصول على استثناء مبرر مسبق من إدارة الأمن السيبراني أو اللجنة التوجيهية للأمن السيبراني.
179	Translated (100%)	In case of a conflict, applicable legislative and regulatory requirements overrule Al Hammadi Holding policies and standards.	في حالة وجود تعارض، فإن المتطلبات التشريعية والتنظيمية المعمول بها تسود على سياسات ومعايير شركة الحمادي القابضة.

180	Translated (100%)	Revision	المراجعة
181	Translated (100%)	This policy is reviewed annually, after major changes in Al Hammadi Holding’s organizational chart or infrastructure, and more frequently whenever required, to ensure it remains appropriate and current for Al Hammadi Holding, ISO 27001, and NCA requirements	تخضع هذه السياسة لمراجعة سنوية، ولإعادة التقييم بعد أي تغييرات جوهرية في الهيكل التنظيمي أو البنية التحتية لشركة الحمادي القابضة، إضافة إلى مراجعات دورية إضافية عند الضرورة، وذلك لضمان توافقها المستمر مع متطلبات شركة الحمادي القابضة، ومعيار آيزو ISO 27001:2022، وإرشادات الهيئة الوطنية للأمن السيبراني
182	Translated (100%)	Approval Section	قسم الاعتماد
183	Translated (100%)	Prepared by:	إعداد:
184	Translated (100%)	Mr. Mohammed Alamer	السيد/ محمد العامر
185	Translated (100%)	GRC Cybersecurity Specialist	أخصائي حوكمة ومخاطر وامتثال في الأمن السيبراني
186	Translated (100%)	Name	الاسم
187	Translated (100%)	Designation	المسمى الوظيفي
188	Translated (100%)	Signature	التوقيع
189	Translated (100%)	Date	التاريخ
190	Translated (100%)	Reviewed by:	راجعها:
191	Translated (100%)	Ms. Mashael Alotaibi	السيدة/ مشاعل العتيبي
192	Translated (100%)	Cybersecurity Manager	مدير الأمن السيبراني
193	Translated (100%)	Name	الاسم
194	Translated (100%)	Designation	المسمى الوظيفي
195	Translated (100%)	Signature	التوقيع
196	Translated (100%)	Date	التاريخ
197	Translated (100%)	Reviewed by:	راجعها:

198	Translated (100%)	Mr. Wahid Raafat	السيد/ وحيد رأفت
199	Translated (100%)	Chief Audit Executive	المدير التنفيذي لعمليات التدقيق
200	Translated (100%)	Name	الاسم
201	Translated (100%)	Designation	المسمى الوظيفي
202	Translated (100%)	Signature	التوقيع
203	Translated (100%)	Date	التاريخ
204	Translated (100%)	Reviewed by:	راجعها:
205	Translated (100%)	Mr. Deepak Dasan	السيد/ ديباك داسان
206	Translated (100%)	IT Manager	مدير تكنولوجيا المعلومات
207	Translated (100%)	Name	الاسم
208	Translated (100%)	Designation	المسمى الوظيفي
209	Translated (100%)	Signature	التوقيع
210	Translated (100%)	Date	التاريخ
211	Translated (100%)	Approved by:	اعتمدها:
212	Translated (100%)	Dr. Abdulaziz Al Hammadi	الحمادي<Bold><Bold></Bold></Bold> د./ عبد العزيز<Bold><Bold></Bold></Bold>
213	Translated (100%)	Chief Operating Officer	الرئيس التنفيذي للعمليات
214	Translated (100%)	Name	الاسم
215	Translated (100%)	Designation	المسمى الوظيفي
216	Translated (100%)	Signature	التوقيع
217	Translated	Date	التاريخ

	(100%)		
218	Translated (100%)	Approved by:	:اعتمدها
219	Translated (100%)	Mr. Mohammad AlHammadi	السيد/ محمد الحمادي
220	Translated (100%)	Chief Executive Officer	الرئيس التنفيذي
221	Translated (100%)	Name	الاسم
222	Translated (100%)	Designation	المسمى الوظيفي
223	Translated (100%)	Signature	التوقيع
224	Translated (100%)	Date	التاريخ

Segment ID	Segment status	Source segment	Target segment
1	Translated (0%)	<3/><29><6>Information Security Risk Management Methodology Policy <19/><23/> </6></29>	سياسة منهجية إدارة مخاطر أمن المعلومات<6><3/><29> <19/><23/> </6></29>
2	Translated (100%)	Page <40><31/> of <39/></40>	صفحة <40><31/> من <39/></40>
3	Translated (100%)	Al Hammadi Holding	شركة الحمادي القابضة
4	Translated (0%)	Information Security Risk Management Methodology	منهجية إدارة مخاطر أمن المعلومات
5	Translated (100%)	CYBERSECURITY DEPARTMENT	إدارة الأمن السيبراني
6	Translated (100%)	Policy ID	معرّف السياسة
7	Translated (100%)	AHH-CS-ISMS-003	AHH-CS-ISMS-003
8	Translated (100%)	Class	الفئة
9	Translated (100%)	Internal Release	إصدار داخلي
10	Not Translated (0%)		
11	Translated (100%)	V3.0	V3.0
12	Translated (100%)	Published at	نُشرت في
13	Translated (100%)	April 2025	أبريل 2025
14	Translated (100%)	Document Owner	المسؤول عن المستند
15	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
16	Translated (100%)	Disclaimer	تنويه
17	Translated (100%)	The information contained in this document is the property of Hammadi Holding and must not be copied or communicated to a third party or used for any purpose other than that for which it is supplied, without the written consent of Al Hammadi Holding.	المعلومات الواردة في هذا المستند هي ملك لشركة الحمادي القابضة ولا يجوز نسخها أو إبلاغها إلى طرف ثالث أو استخدامها لأي غرض آخر غير الغرض الذي تم توفيرها من أجله، دون موافقة خطية من شركة الحمادي القابضة.

18	Translated (100%)	Contents	جدول المحتويات
19	Translated (100%)	Document Control	ضبط المستندات
20	Translated (100%)	Document Information	معلومات المستند
21	Translated (100%)	Synopsis	الملخص
22	Translated (100%)	Document Title:	:عنوان المستند
23	Translated (0%)	Information Security Risk Management Methodology Policy	سياسة منهجية إدارة مخاطر أمن المعلومات
24	Translated (100%)	Document Status:	:حالة المستند
25	Translated (100%)	Approved	معتمد
26	Translated (100%)	Document Effective Date:	:تاريخ سريان المستند
27	Translated (100%)	December 2024	ديسمبر 2024
28	Translated (100%)	Document Issue Date:	:تاريخ إصدار المستند
29	Translated (100%)	December 2024	ديسمبر 2024
30	Translated (100%)	Document Next Revision Date:	:تاريخ المراجعة التالية للمستند
31	Translated (100%)	December 2025	ديسمبر 2025
32	Translated (100%)	Key contacts	جهات التواصل الرئيسية
33	Translated (100%)	Document Owner:	:المسؤول عن المستند
34	Translated (100%)	CS Management	(CS) إدارة كائنات نهج المجموعة
35	Translated (100%)	Approval Authority	جهة الاعتماد
36	Translated (100%)	Document Created by:	:مُنشئ المستند
37	Translated	IT Management	إدارة تكنولوجيا المعلومات

	(100%)		
38	Translated (100%)	Document Reviewed by:	:راجع المستند
39	Translated (100%)	Al Hammadi Holding CS &IT Managers	مديرو الأمن السيبراني وتكنولوجيا المعلومات في شركة الحمادي القابضة
40	Translated (100%)	Document Approved by:	:اعتمد المستند
41	Translated (100%)	Al Hammadi Holding COO & CEO	الرئيس التنفيذي للعمليات والرئيس التنفيذي في شركة الحمادي القابضة
42	Translated (100%)	Note:	:ملاحظة
43	Translated (100%)	Any additional approval will be added in the document annex	تُضاف أي اعتمادات إضافية في ملحق المستند
44	Translated (100%)	Classification	التصنيف
45	Translated (99%)	<335>Company Internal</335> – to be shared with 3rd parties after consent of CS Manager	داخلي لاستخدام للشركة – <335/>يُسمح بمشاركته مع<335> جهات خارجية بعد موافقة مدير إدارة الأمن السيبراني
46	Translated (100%)	Version / Dates	الإصدار / التواريخ
47	Translated (100%)	Current Version:	:الإصدار الحالي
48	Translated (100%)	V 3.0	V 3.0
49	Translated (100%)	Date Published:	:تاريخ النشر
50	Translated (100%)	December 2024	ديسمبر 2024
51	Translated (100%)	Date of Next Review:	:تاريخ المراجعة التالية
52	Translated (100%)	April 2025	أبريل 2025
53	Translated (100%)	Prior Version:	:الإصدار السابق
54	Translated (100%)	V 2.0	V 2.0
55	Translated (100%)	Prior Published:	:تاريخ النشر السابق
56	Translated (100%)	December 2023	ديسمبر 2023

57	Translated (100%)	Document Changes	التغييرات على المستند
58	Translated (100%)	Date	التاريخ
59	Translated (100%)	Version	الإصدار
60	Translated (100%)	Document Owner	المسؤول عن المستند
61	Translated (100%)	Change Description	وصف التغيير
62	Translated (100%)	December 2024	ديسمبر 2024
63	Translated (100%)	2.0	2.0
64	Translated (100%)	IT Management	إدارة تكنولوجيا المعلومات
65	Translated (0%)	Updated the policy number to AHH-IT-ISMS-001	AHH - IT - ISMS -001 تم تحديث رقم السياسة إلى
66	Translated (100%)	April 2025	أبريل 2025
67	Translated (100%)	3.0	3.0
68	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
69	Translated (100%)	Document reviewed and updated based on NCA ECC-2:2024 and ISO27001:2022 requirements	تمت مراجعة المستند وتحديثه استنادًا إلى متطلبات الهيئة الوطنية للأمن السيبراني (NCA) المعيار ECC-2:2024 ومعيار آيزو ISO 27001:2022.
70	Translated (100%)	Document Circulation	تعميم المستند
71	Translated (100%)	To	إلى
72	Translated (100%)	Date	التاريخ
73	Translated (100%)	Method	الطريقة
74	Translated (0%)	*<506>*IT Staff*</506>*	*<506>506/>*موظفو تكنولوجيا المعلومات>
75	Translated (100%)	December 2024	ديسمبر 2024

76	Translated (100%)	Intranet Portal	بوابة الإنترانت
77	Translated (100%)	All Al Hammadi Staff	جميع موظفي شركة الحمادي
78	Translated (100%)	December 2024	ديسمبر 2024
79	Translated (100%)	Intranet Portal	بوابة الإنترانت
80	Translated (99%)	Introduction	المُقدمة
81	Translated (0%)	Al Hammadi holding adopts a proactive approach to cybersecurity risk management to minimize uncertainty and facilitate the assessment and mitigation of cyber risks in an ever-evolving threat landscape.	تتبنى شركة الحمادي القابضة نهجًا استباقيًا لإدارة مخاطر الأمن السيبراني لتقليل عدم اليقين وتسهيل تقييم وتخفيف المخاطر السيبرانية في مشهد التهديد المتطور باستمرار.
82	Translated (0%)	The healthcare faces significant challenges in keeping pace with the scale and diversity of cyber threats that may impact its strategic goals and operational processes.	تواجه الرعاية الصحية تحديات كبيرة في مواكبة حجم وتنوع التهديدات السيبرانية التي قد تؤثر على أهدافها الاستراتيجية وعملياتها التشغيلية.
83	Translated (0%)	To address the risks associated with its digital and technical assets, the hospital emphasizes the importance of establishing methodologies and controls to identify vulnerabilities and implement appropriate mitigation measures, ensuring the protection of its IT infrastructure, medical systems, and sensitive data from exploitation that could harm its reputation or operations.	ولمعالجة المخاطر المرتبطة بأصوله الرقمية والتقنية، يؤكد المستشفى على أهمية وضع منهجيات وضوابط لتحديد نقاط الضعف وتنفيذ تدابير التخفيف المناسبة، وضمان حماية البنية التحتية لتكنولوجيا المعلومات والأنظمة الطبية والبيانات الحساسة من الاستغلال الذي يمكن أن يضر بسمعته أو عملياته.
84	Translated (99%)	Executive Summary	الملخص التنفيذي
85	Translated (0%)	The Cybersecurity Risk Management Framework has been developed to ensure the confidentiality, integrity, and availability of Al Hammadi holding’s digital assets while protecting its operations from potential cyber threats.	تم تطوير إطار إدارة مخاطر الأمن السيبراني لضمان سرية وسلامة وتوافر الأصول الرقمية لشركة الحمادي القابضة مع حماية عملياتها من التهديدات السيبرانية المحتملة.
86	Translated (0%)	The framework serves as a reference for implementing, monitoring, and continuously improving risk management practices in alignment with national standards and international best practices.	يعمل الإطار كمرجع لتنفيذ ممارسات إدارة المخاطر ومراقبتها وتحسينها باستمرار بما يتماشى مع المعايير الوطنية وأفضل الممارسات الدولية.
87	Translated (0%)	The framework defines methodologies to identify, evaluate, and mitigate cybersecurity risks to an acceptable level.	يحدد إطار العمل منهجيات لتحديد وتقييم وتخفيف مخاطر الأمن السيبراني إلى مستوى مقبول.
88	Translated (0%)	It also supports the implementation and monitoring of cybersecurity controls to protect sensitive information and systems created, managed, stored, or transmitted by the hospital.	كما يدعم تنفيذ ومراقبة ضوابط الأمن السيبراني لحماية المعلومات والأنظمة الحساسة التي يتم إنشاؤها أو إدارتها أو تخزينها أو نقلها من قبل المستشفى.
89	Translated (0%)	By applying this framework, Al Hammadi holding ensures the resilience of its digital environment and readiness to address future threats effectively.	ومن خلال تطبيق هذا الإطار، تضمن شركة الحمادي القابضة مرونة بيئتها الرقمية واستعدادها لمواجهة التهديدات المستقبلية بفعالية.
90	Translated (0%)	Purpose of the Cybersecurity Risk Management Framework	الغرض من إطار إدارة مخاطر الأمن السيبراني

91	Translated (0%)	The Cybersecurity Risk Management Framework aims to document knowledge for those responsible for executing procedures, operations, and activities related to cybersecurity risk management at Al Hammadi holding.	يهدف إطار إدارة مخاطر الأمن السيبراني إلى توثيق المعرفة للمسؤولين عن تنفيذ الإجراءات والعمليات والأنشطة المتعلقة بإدارة مخاطر الأمن السيبراني في شركة الحمادي القابضة.
92	Translated (0%)	It ensures that the cybersecurity team and relevant stakeholders carry out their responsibilities effectively to achieve the following objectives:	يضمن قيام فريق الأمن السيبراني وأصحاب المصلحة المعنيين بمسؤولياتهم بفعالية لتحقيق الأهداف التالية:
93	Translated (0%)	Implementing the directives of stakeholders and the cybersecurity oversight committee regarding risk management across all hospital locations within and outside the Kingdom.	تنفيذ توجيهات أصحاب المصلحة ولجنة الإشراف على الأمن السيبراني فيما يتعلق بإدارة المخاطر في جميع مواقع المستشفيات داخل المملكة وخارجها.
94	Translated (0%)	Proactively addressing security and cyber threats to the hospital's digital assets, technical systems, and medical control devices.	التصدي بشكل استباقي للتهديدات الأمنية والإلكترونية للأصول الرقمية للمستشفى والأنظمة التقنية وأجهزة التحكم الطبية.
95	Translated (0%)	Ensuring the confidentiality, integrity, and availability of sensitive systems and data, including industrial control systems critical to hospital operations.	ضمان سرية وسلامة وتوافر الأنظمة والبيانات الحساسة، بما في ذلك أنظمة التحكم الصناعية الحيوية لعمليات المستشفى.
96	Translated (0%)	Scope of the Cybersecurity Risk Management Framework	نطاق إطار إدارة مخاطر الأمن السيبراني
97	Translated (0%)	The framework applies to all personnel (civilian and military), users, contractors, service providers, and consultants employed directly or indirectly by Al Hammadi Holding.	ينطبق الإطار على جميع الموظفين (المدنيين والعسكريين) والمستخدمين والمقاولين ومقدمي الخدمات والاستشاريين الذين توظفهم شركة الحمادي القابضة بشكل مباشر أو غير مباشر.
98	Translated (0%)	It encompasses all digital and technical assets owned by the hospital across its internal and external locations, including associated third parties, subsidiaries, partners, and consultants.	وهو يشمل جميع الأصول الرقمية والتقنية التي يملكها المستشفى عبر مواقعه الداخلية والخارجية، بما في ذلك الأطراف الثالثة والشركات التابعة والشركاء والاستشاريين المرتبطين به.
99	Translated (0%)	It covers data processing systems, industrial control systems, and technical tools owned by the hospital, as well as its data processing facilities.	وهو يغطي أنظمة معالجة البيانات وأنظمة التحكم الصناعي والأدوات التقنية المملوكة للمستشفى، بالإضافة إلى مرافق معالجة البيانات الخاصة به.
100	Translated (0%)	Alignment with National and International Standards	المواءمة مع المعايير الوطنية والدولية
101	Translated (0%)	The Cybersecurity Risk Management Framework is designed to comply with local requirements and align with international standards and best practices, including:	تم تصميم إطار إدارة مخاطر الأمن السيبراني للامتثال للمتطلبات المحلية والمواءمة مع المعايير الدولية وأفضل الممارسات، بما في ذلك:
102	Translated (0%)	<630>Essential Cybersecurity Controls</630> issued by the National Cybersecurity Authority (NCA) (ECC-1:	ضوابط الأمن السيبراني الأساسية<630/> الصادرة عن الهيئة<630> الوطنية للأمن السيبراني (ECC -1):
103	Translated (0%)	2018).	2018).
104	Translated (0%)	<636>ISO 27005:2022</636> standards for information security risk management.	لإدارة مخاطر أمن <636>ISO 27005:2022</636> معايير المعلومات.
105	Translated (0%)	<642>NIST Risk Management Framework (NIST RMF)</642> for cybersecurity.	إطار إدارة مخاطر المعهد الوطني للمعايير والتكنولوجيا<642> للأمن السيبراني (NIST RMF)</642>.
106	Translated (0%)	<648>ISO 31000:2018</648> standards for enterprise risk management.	معايير آيزو 31000:2018<648/> لإدارة المخاطر<648> المؤسسية.
107	Translated	Risk management and business continuity controls issued by the Digital	ضوابط إدارة المخاطر واستمرارية الأعمال الصادرة عن هيئة

	(0%)	Government Authority (DGA).	.الحكومة الرقمية (DGA)
108	Translated (0%)	Roles and <658>Responsibilities</658>	<الأدوار <658>والمسؤوليات</658/>
109	Translated (0%)	Cybersecurity Steering Committee	اللجنة التوجيهية للأمن السيبراني
110	Translated (0%)	Provide necessary support to the cybersecurity management team during the implementation of cybersecurity risk management methodologies and procedures.	تقديم الدعم اللازم لفريق إدارة الأمن السيبراني أثناء تنفيذ منهجيات وإجراءات إدارة مخاطر الأمن السيبراني.
111	Translated (0%)	Review and stay informed about cybersecurity risk management activities and plans on a quarterly basis.	مراجعة أنشطة وخطط إدارة مخاطر الأمن السيبراني والبقاء على اطلاع بها على أساس ربع سنوي.
112	Translated (0%)	Regularly review and monitor the processes for identifying, assessing, and analyzing cybersecurity risks.	مراجعة ومراقبة عمليات تحديد وتقييم وتحليل مخاطر الأمن السيبراني بانتظام.
113	Translated (0%)	Oversee and support the implementation of mitigation plans for potential cybersecurity risks and ensure their effectiveness.	الإشراف على تنفيذ خطط التخفيف من مخاطر الأمن السيبراني المحتملة ودعمها وضمان فعاليتها
114	Translated (0%)	Annually review risk management reports and assess the overall status of cybersecurity risks, ensuring alignment with enterprise risks.	مراجعة تقارير إدارة المخاطر سنويًا وتقييم الحالة العامة لمخاطر الأمن السيبراني، وضمان التوافق مع مخاطر المؤسسة.
115	Translated (0%)	Escalate critical cybersecurity risks to the appropriate authority and the committee responsible for enterprise risk management to take necessary actions.	تصعيد مخاطر الأمن السيبراني الحرجة إلى الجهة المختصة واللجنة المسؤولة عن إدارة مخاطر المؤسسة لاتخاذ الإجراءات اللازمة.
116	Translated (0%)	Cybersecurity Management	إدارة الأمن السيبراني
117	Translated (0%)	Develop and periodically update the Cybersecurity Risk Management Framework as needed to enhance the hospital's risk assessment practices.	تطوير وتحديث إطار إدارة مخاطر الأمن السيبراني بشكل دوري حسب الحاجة لتعزيز ممارسات تقييم المخاطر في المستشفى.
118	Translated (0%)	Conduct cybersecurity risk assessments and mitigation processes in coordination with relevant stakeholders.	إجراء تقييمات مخاطر الأمن السيبراني وعمليات التخفيف منها بالتنسيق مع أصحاب المصلحة المعنيين.
119	Translated (0%)	Monitor and follow up on mitigation plans to protect technical and digital assets effectively.	مراقبة ومتابعة خطط التخفيف لحماية الأصول التقنية والرقمية بشكل فعال.
120	Translated (0%)	Address and coordinate any instances of non-compliance with the Cybersecurity Risk Management Framework	معالجة وتنسيق أي حالات عدم امتثال لإطار عمل إدارة مخاطر الأمن السيبراني
121	Translated (0%)	Share updates, changes, and guidance related to the framework with stakeholders, the oversight committee, and all relevant parties.	مشاركة التحديثات والتغييرات والإرشادات المتعلقة بالإطار مع أصحاب المصلحة ولجنة الرقابة وجميع الجهات ذات الصلة.
122	Translated (0%)	Supervise and coordinate with stakeholders to ensure the implementation of cybersecurity risk mitigation measures and adherence to the cybersecurity risk management policy.	الإشراف والتنسيق مع أصحاب المصلحة لضمان تنفيذ تدابير التخفيف من مخاطر الأمن السيبراني والالتزام بسياسة إدارة مخاطر الأمن السيبراني
123	Translated (0%)	Prepare periodic reports for stakeholders and the oversight committee on cybersecurity risks and the planned mitigation measures	إعداد تقارير دورية لأصحاب المصلحة ولجنة الرقابة حول مخاطر الأمن السيبراني وتدابير التخفيف المخطط لها
124	Translated (76%)	Internal Audit Unit	إدارة التدقيق الداخلي
125	Translated	Evaluate cybersecurity risk reports and records to ensure alignment with	تقييم تقارير وسجلات مخاطر الأمن السيبراني لضمان التوافق مع

	(0%)	annual audit plans, focusing on high-risk areas.	.خطط التدقيق السنوية، مع التركيز على المجالات عالية المخاطر
126	Translated (0%)	Audit cybersecurity risk management processes and provide recommendations to improve internal controls and the effectiveness of cybersecurity risk management measures.	تدقيق عمليات إدارة مخاطر الأمن السيبراني وتقديم توصيات لتحسين الضوابط الداخلية وفعالية تدابير إدارة مخاطر الأمن السيبراني.
127	Translated (0%)	All Other Departments and Divisions	جميع الإدارات والأقسام الأخرى
128	Translated (0%)	Review documents related to cybersecurity risk management, such as the Cybersecurity Risk Management Policy and Framework.	مراجعة الوثائق المتعلقة بإدارة مخاطر الأمن السيبراني، مثل سياسة وإطار إدارة مخاطر الأمن السيبراني.
129	Translated (0%)	Provide continuous support to the cybersecurity management team in identifying, assessing, and addressing cybersecurity risks, recognizing that risk management is a collective responsibility.	تقديم الدعم المستمر لفريق إدارة الأمن السيبراني في تحديد وتقييم ومعالجة مخاطر الأمن السيبراني، مع الاعتراف بأن إدارة المخاطر هي مسؤولية جماعية.
130	Translated (0%)	Collaborate with the cybersecurity management team by providing necessary supporting documents during the risk assessment phase.	التعاون مع فريق إدارة الأمن السيبراني من خلال توفير الوثائق الداعمة اللازمة خلال مرحلة تقييم المخاطر.
131	Translated (0%)	Participate in the development and implementation of mitigation plans for assessed risks to enhance internal controls and minimize cybersecurity risks to the hospital.	المشاركة في تطوير وتنفيذ خطط التخفيف من المخاطر المقدرة لتعزيز الضوابط الداخلية وتقليل مخاطر الأمن السيبراني على المستشفى.
132	Translated (0%)	Cybersecurity Risk Management Methodology	منهجية إدارة مخاطر الأمن السيبراني
133	Translated (0%)	<757/><760>The methodology outlines the process of identifying, analyzing, evaluating, and addressing cybersecurity risks within the organization.</760>	تحدد المنهجية عملية تحديد وتحليل وتقييم<760><757/><760/> ومعالجة مخاطر الأمن السيبراني داخل المؤسسة.
134	Translated (0%)	It consists of eight main stages or activities, as shown in (Figure 1).	وهو يتألف من ثماني مراحل أو أنشطة رئيسية، كما هو موضح في (الشكل 1).
135	Translated (0%)	It also ensures the evaluation of current risks and control measures	كما يضمن تقييم المخاطر الحالية وتدابير الرقابة
136	Translated (0%)	Context Determination - Communication and Consultation Regarding Risks – risk review and monitoring – risk treatment - <766>Risk Analysis - Risk Assessment - Risk Identification - Services | Operations | Systems - Risk Source <779/> Risk Scenario <780/> Control Measures - Risk Analysis - Risk Assessment - Risk Severity - Effectiveness of Control Measures - Residual Risks – Avoidance – Transfer – Mitigation – Accept - </766>Figure 1 - Cybersecurity Risk Management Methodology	تحديد السياق - التواصل والتشاور بشأن المخاطر – مراجعة - المخاطر ومراقبتها – معالجة المخاطر – <766>تحليل المخاطر - تقييم المخاطر - تحديد المخاطر - الخدمات | العمليات | الأنظمة تدابير <780/> التحكم في سيناريوهات <779/> مخاطر مصدر المخاطر - تحليل المخاطر - تقييم المخاطر - شدة المخاطر - فعالية – تدابير الرقابة - المخاطر المتبقية – التجنب – النقل – التخفيف القبول – <766/>الشكل 1 - منهجية إدارة مخاطر الأمن السيبراني
137	Translated (0%)	Context Identification	تحديد السياق
138	Translated (0%)	The <792>context</792> is identified through conducting meetings and workshops, and reviewing the following:	يتم تحديد <792>السياق<792/> من خلال عقد الاجتماعات وورش العمل، ومراجعة ما يلي:
139	Translated (0%)	Meeting with relevant stakeholders to determine the scope of assessments.	.الاجتماع مع أصحاب المصلحة المعنيين لتحديد نطاق التقييمات
140	Translated (0%)	Reviewing records and reports of previous cybersecurity incidents and assessments from external parties.	مراجعة سجلات وتقارير حوادث الأمن السيبراني السابقة والتقييمات من الأطراف الخارجية.

141	Translated (0%)	Reviewing previous internal audit reports related to cybersecurity.	.مراجعة تقارير التدقيق الداخلي السابقة المتعلقة بالأمن السيبراني
142	Translated (0%)	Cataloging relevant digital and technical assets.	.فهرسة الأصول الرقمية والتقنية ذات الصلة
143	Translated (0%)	Risk Identification	تحديد المخاطر
144	Translated (0%)	The <820>purpose</820> of risk identification is to identify potential cybersecurity events that may occur in the near future and impact the hospital's digital and technical assets.	الغرض</820> من تحديد المخاطر هو تحديد أحداث الأمن<820> السيبراني المحتملة التي قد تحدث في المستقبل القريب وتؤثر على .الأصول الرقمية والتقنية للمستشفى
145	Translated (0%)	The process of identifying cybersecurity risks involves determining the source of the risk, the events, and the conditions that could lead to its occurrence.	تتضمن عملية تحديد مخاطر الأمن السيبراني تحديد مصدر المخاطر .والأحداث والظروف التي يمكن أن تؤدي إلى حدوثها
146	Translated (0%)	Then, the applied control measures (such as people, processes, and/or technologies) are assessed for their effectiveness and efficiency.	بعد ذلك، يتم تقييم تدابير التحكم المطبقة (مثل الأشخاص و/أو .العمليات و/أو التقنيات) من حيث فعاليتها وكفاءتها
147	Translated (0%)	The identified risks are recorded in the Cybersecurity Risk Register, as shown in Figure 2.	يتم تسجيل المخاطر المحددة في سجل مخاطر الأمن السيبراني، كما .هو موضح في الشكل 2
148	Translated (0%)	<832>Identifying the Risks - </832>Risk Code - Process <838>I </838>Asset – Risk - Causes/Source of Risk - Expected Risk Scenario - Current Control Measures - <847>Figure 2 • risk register – section for identifying cybersecurity risks</847>	<تحديد المخاطر - </832>رمز المخاطر - العملية <832><838> - الأولى </838>الأصول – المخاطر - أسباب/مصدر المخاطر سيناريو المخاطر المتوقعة - تدابير الرقابة الحالية - <847>الشكل 2 <سجل المخاطر – قسم لتحديد مخاطر الأمن السيبراني</847> •
149	Translated (0%)	When <853>describing</853> a risk scenario, the consequences of the risk on the asset or process must be documented.	عند <853>وصف</853> سيناريو المخاطر، يجب توثيق عواقب .المخاطر على الأصل أو العملية
150	Translated (0%)	The outcomes of cybersecurity incident scenarios should consider the following:	يجب أن تأخذ نتائج سيناريوهات حوادث الأمن السيبراني في الاعتبار :ما يلي
151	Translated (0%)	The health and safety of the organization's personnel.	.صحة وسلامة موظفي المنظمة
152	Translated (0%)	The hospital's local and international reputation.	.سمعة المستشفى المحلية والدولية
153	Translated (0%)	The time required for damage repair and incident investigation.	.الوقت اللازم لإصلاح الأضرار والتحقيق في الحوادث
154	Translated (0%)	The downtime affecting operational processes (e.g., disruption of industrial control systems).	وقت التوقف عن العمل الذي يؤثر على العمليات التشغيلية (على .سبيل المثال، تعطيل أنظمة التحكم الصناعية)
155	Translated (0%)	The estimated financial cost for the skills, tools, or technologies required to remediate the damage.	التكلفة المالية المقدرة للمهارات أو الأدوات أو التقنيات اللازمة .لإصلاح الضرر
156	Translated (0%)	Risk Analysis & Risk Evaluation	تحليل المخاطر وتقييم المخاطر
157	Translated (0%)	Likelihood Matrix	مصفوفة الاحتمالات
158	Translated (0%)	The probability matrix is used to document the likelihood indicators of an event and <872>the</872> expected severity of its occurrence.	تُستخدم مصفوفة الاحتمالات لتوثيق مؤشرات احتمالية الحدث .والشدة المتوقعة لوقوعه <872></872>

159	Translated (0%)	It is divided into five (5) levels, as shown in <878>Table 1.</878>	<878>وهي مقسمة إلى خمسة (5) مستويات، كما هو موضح في الجدول 1.</878>
160	Translated (0%)	Table of Likelihood of Cybersecurity Risk Occurrence - Risk Level - Risk Classification - Classification Description – Rare - Likely to occur at a rate of less than 5% or once every years.	- جدول احتمالية حدوث مخاطر الأمن السيبراني - مستوى المخاطر تصنيف المخاطر - وصف التصنيف – نادر الحدوث - من المحتمل أن يحدث بمعدل أقل من 5 ٪ أو مرة واحدة كل عام.
161	Translated (0%)	– Unlikely - Likely to occur at a rate of 5% to 34.99% or once every two years.	غير محتمل - من المحتمل أن يحدث بمعدل 5 ٪ إلى 34.99 ٪ أو – مرة واحدة كل عامين.
162	Translated (0%)	– Possible - Likely to occur at a rate of 35% to 64.99% or once every year.	ممكن - من المحتمل أن يحدث بمعدل 35 ٪ إلى 64.99 ٪ أو مرة – واحدة كل عام.
163	Translated (0%)	– Likely - Likely to occur at a rate of 65% to 89.99% or once every 6 months.	محتمل - من المحتمل أن يحدث بمعدل 65 ٪ إلى 89.99 ٪ أو – مرة واحدة كل 6 أشهر.
164	Translated (0%)	– Certain - Likely to occur at a rate of 90% or higher, or once every 3 months.	مؤكد - من المحتمل أن يحدث بمعدل 90 ٪ أو أعلى، أو مرة – واحدة كل 3 أشهر.
165	Translated (0%)	- Table 1 • Probability Matrix	الجدول 1 • مصفوفة الاحتمالات -
166	Translated (100%)	Impact Matrix	مصفوفة التأثير
167	Translated (0%)	The <899>impact</899> matrix is used to document the potential consequences on strategic or operational objectives in the event of a risk occurrence.	تُستخدم مصفوفة <899>التأثير</899> لتوثيق العواقب المحتملة على الأهداف الاستراتيجية أو التشغيلية في حالة حدوث مخاطر.
168	Translated (0%)	It is divided into five (5) levels, as shown in <905>Table2.</905>	<905>وهي مقسمة إلى خمسة (5) مستويات، كما هو موضح في الجدول 2.</905>
169	Translated (0%)	Risk Heatmap	خريطة حرارة المخاطر
170	Translated (0%)	<914>The risk </914><917>weight</917><921> matrix is used to measure the level of risk as a result of evaluating the impact and probability.</921>	تُستخدم مصفوفة<917> وزن</917><914> المخاطر لقياس مستوى المخاطر نتيجة لتقييم التأثير </914><921>والاحتمال.</921>
171	Translated (0%)	A 5 × 5 risk weight matrix is adopted to assess the weight of risks in terms of their likelihood of occurrence, impact, and their indicators on the organization, as shown in <924>Table 3</924>.	يتم اعتماد مصفوفة وزن المخاطر 5 × 5 لتقييم وزن المخاطر من حيث احتمالية حدوثها وتأثيرها ومؤشراتها على المنظمة، كما هو موضح في <924>الجدول 3</924>.
172	Translated (0%)	As a result of the assessment of inherent or residual risks, the risks are distributed on the heat map (probability x impact) or (probability x impact – control effectiveness).	نتيجة لتقييم المخاطر الكامنة أو المتبقية، يتم توزيع المخاطر على الخريطة الحرارية (الاحتمال x التأثير) أو (الاحتمال x التأثير – فعالية التحكم).
173	Translated (0%)	The total risk value is then assessed based on <933>Table 4</933>.	ثم يتم تقييم إجمالي قيمة المخاطر بناءً على <933>الجدول 4</933>.
174	Translated (0%)	<939>Risk Weight Matrix (Heatmap) – </939>Probability – Certain – Likely – Possible – Unlikely – Rare – <951>Impact – </951>Low – Minor – Moderate – High – Critical - <966>Table 3 - Risk Heat Map</966>	<939>مصفوفة وزن المخاطر (خريطة حرارية) – </939>الاحتمال – المؤكد – المحتمل – المحتمل – غير المحتمل – النادر – <951>التأثير – </951>منخفض – طفيف – متوسط – مرتفع<951> – حرج - <966>الجدول 3 - خريطة حرارة المخاطر</966>

175	Translated (100%)	Residual Risk	الخطر المتبقي
176	Translated (0%)	After implementing the proposed controls, continuous review is conducted to calculate the risk level and measure the residual risks.	بعد تنفيذ الضوابط المقترحة، يتم إجراء مراجعة مستمرة لحساب مستوى المخاطر وقياس المخاطر المتبقية.
177	Translated (0%)	These should be identified, documented, and approved by the risk owner, with the value recorded in the risk register, as shown in <979>Figure 3.</979>	يجب تحديدها وتوثيقها والموافقة عليها من قبل المسؤول عن المخاطر، مع تسجيل القيمة في سجل المخاطر، كما هو موضح في <979>الشكل 3.</979>
178	Translated (0%)	Risk Monitoring - <989>Current Review Date – Impact – Probability - Residual Risk level – Review</989> <995>Frequency - Next Review</995> <1001>Date – Responsibilities - figure 3 - risk Register - </1001>Risk Monitoring	مراقبة المخاطر - <989>تاريخ المراجعة الحالي – التأثير – الاحتمال - مستوى المخاطر المتبقية –</989> <995>تكرار المراجعة - تاريخ المراجعة التالي</995> <1001>– المسؤوليات - الشكل 3 سجل المخاطر - </1001>مراقبة المخاطر
179	Translated (0%)	</1014><1017>Control Assessment</1017>	<1014/><1017>تقييم التحكم</1017></1014>
180	Translated (0%)	<1020>Risk Level – Assessment – From – To - </1020>Low Risk - Medium Risk - High Risk - Critical Risk - <1026>Table 4 - Risk Assessment</1026>	مستوى المخاطر – التقييم – من – إلى - </1020><1020>مخاطر - منخفضة - مخاطر متوسطة - مخاطر عالية - مخاطر حرجة <1026>الجدول 4 - تقييم المخاطر</1026></1020>
181	Translated (0%)	The adequacy and <1032>effectiveness</1032> of the current controls are analyzed to determine the residual risks by answering the following questions:	يتم تحليل مدى كفاية <1032>وفعالية</1032> الضوابط الحالية لتحديد المخاطر المتبقية من خلال الإجابة على الأسئلة التالية:
182	Translated (0%)	What are the current controls applied to the risk?	ما هي الضوابط الحالية المطبقة على المخاطر ؟
183	Translated (0%)	Are these controls capable of addressing the risk appropriately, or are there temporary alternative controls?	هل هذه الضوابط قادرة على معالجة المخاطر بشكل مناسب، أم أن هناك ضوابط بديلة مؤقتة ؟
184	Translated (0%)	In practice, are the controls working as designed ("effectiveness"), and can their effectiveness be demonstrated when needed?	من الناحية العملية، هل تعمل الضوابط على النحو المصمم (" الفعالية")، وهل يمكن إثبات فعاليتها عند الحاجة ؟
185	Translated (0%)	Based on the available <1050>information</1050> from the previous analysis, the residual risk severity is calculated using the following formula <1056>Figure 4</1056>	بناءً على <1050>المعلومات</1050> المتاحة من التحليل السابق، يتم حساب شدة المخاطر المتبقية باستخدام الصيغة التالية <1056>الشكل 4</1056>
186	Translated (0%)	Remaining Risk Level – Impact – Probability - Effectiveness of Control Measure - figure 4 – assessment of Remaining risks	مستوى المخاطر المتبقية – الأثر – الاحتمال - فعالية تدبير الرقابة - الشكل 4 – تقييم المخاطر المتبقية
187	Translated (0%)	The effectiveness <1069>assessment</1069> scale for the control measures is designed as shown in <1075>Table 5.</1075>	تم تصميم مقياس <1069>تقييم</1069> الفعالية لتدابير الرقابة كما هو موضح في <1075>الجدول 5.</1075>
188	Translated (0%)	Evaluation - Weight for Measuring the Effectiveness of Controls - Description of Control - <1085>No Control - Ineffective Control - Control Requires Improvement - </1085>Partially Effective Control - Fully Applied Control - <1091>Control No:</1091>	التقييم - الوزن لقياس فعالية الضوابط - وصف التحكم - عدم التحكم غير الفعال - التحكم يتطلب التحسين - </1085><1085> - التحكم الفعال جزئيًا - التحكم المطبق بالكامل - <1091>التحكم رقم: </1091>
189	Translated (0%)	Applied or Not Present (Design and Effectiveness) - The control has not been designed effectively or has been applied manually.	مطبقة أو غير موجودة (التصميم والفعالية) - لم يتم تصميم عنصر التحكم بشكل فعال أو تم تطبيقه يدويًا.
190	Translated	- The control lacks a preventive nature, as it is partially automated and	- يفتقر التحكم إلى الطبيعة الوقائية، حيث يتم أتمتته جزئيًا وتطبيقه

	(0%)	applied with appropriate frequency.	.بتردد مناسب
191	Translated (0%)	(The controls are designed to reduce the impact and likelihood of risks partially.)	(.تم تصميم الضوابط للحد من تأثير واحتمال المخاطر جزئيًا)
192	Translated (0%)	- The controls are well-designed and preventive by nature, but they lack full automation or are applied with inappropriate frequency.	الضوابط جيدة التصميم ووقائية بطبيعتها، لكنها تفتقر إلى الأتمتة - .الكاملة أو يتم تطبيقها بتكرار غير مناسب
193	Translated (0%)	These are the control measures that significantly reduce the impact and likelihood of risk occurrence.	هذه هي تدابير الرقابة التي تقلل بشكل كبير من تأثير واحتمال .حدوث المخاطر
194	Translated (0%)	- The controls are well-designed, preventive by nature, fully automated, and applied with appropriate frequency.	،الضوابط مصممة تصميما جيدا، وقائية بطبيعتها، مؤتمتة بالكامل - .وتطبق بتواتر مناسب
195	Translated (0%)	These are the control measures that reduce the impact and likelihood of risks to a very high degree.	هذه هي تدابير الرقابة التي تقلل من تأثير واحتمال المخاطر إلى .درجة عالية جدًا
196	Translated (0%)	*<1091>*- *</1091>*Table S - Evaluation of the Effectiveness of Control Measures	تقييم فعالية تدابير الرقابة - S الجدول*<1091>* -*</1091>*
197	Translated (0%)	*<1101/><1104>*The results of the risk analysis and assessment process are recorded in the Cybersecurity Risk Register, as shown in *<1107>*Figure 5.*</1107></1104>*	يتم تسجيل نتائج عملية تحليل المخاطر وتقييمها*<1101/><1104>* في سجل مخاطر الأمن السيبراني، كما هو موضح في *<1107>*الشكل 5.*</1107></1104>*
198	Translated (0%)	Risk analysis and evaluation	تحليل المخاطر وتقييمها
199	Translated (0%)	Evaluation of current control measures	تقييم تدابير الرقابة الحالية
200	Translated (99%)	Impact	التأثير
201	Translated (0%)	probability	الاحتمال
202	Translated (0%)	Residual risk level	مستوى المخاطر المتبقية
203	Translated (0%)	Figure 5: risk register- risk analysis and assessment	الشكل 5: سجل المخاطر - تحليل المخاطر وتقييمها
204	Translated (0%)	Risk Treatment	معالجة المخاطر
205	Translated (0%)	This process aims to design, build, implement, and monitor the mitigation of cybersecurity risks by the risk owner and those responsible for the mitigation plans.	تهدف هذه العملية إلى تصميم وبناء وتنفيذ ومراقبة التخفيف من مخاطر الأمن السيبراني من قبل مسؤول المخاطر والمسؤولين عن .خطط التخفيف
206	Translated (0%)	During this phase, all data and outputs from the previous stages (risk identification, analysis, and evaluation) are relied upon to determine strategies and plans for mitigating cybersecurity risks at appropriate levels, in order to reduce the impact and likelihood of the identified risks.	خلال هذه المرحلة، يتم الاعتماد على جميع البيانات والمخرجات من المراحل السابقة (تحديد المخاطر وتحليلها وتقييمها) لتحديد الاستراتيجيات والخطط للتخفيف من مخاطر الأمن السيبراني على المستويات المناسبة، من أجل الحد من تأثير واحتمال المخاطر .المحددة
207	Translated	This ensures alignment with the organization's strategic objectives and	وهذا يضمن التوافق مع الأهداف الاستراتيجية للمنظمة ويضمن بقاء

	(0%)	guarantees that risks remain within acceptable levels or thresholds.	.المخاطر ضمن المستويات أو العتبات المقبولة
208	Translated (0%)	Cybersecurity Risk Mitigation Strategy	استراتيجية التخفيف من مخاطر الأمن السيبراني
209	Translated (0%)	Accepting the Risk:	:قبول المخاطر
210	Translated (0%)	This strategy is adopted when accepting the current level of risk without any mitigation, due to reasons such as the cost of mitigation being higher than the potential impact of the risk, or the inability to reject or transfer the risk.	يتم اعتماد هذه الاستراتيجية عند قبول المستوى الحالي للمخاطر دون أي تخفيف، لأسباب مثل أن تكلفة التخفيف أعلى من التأثير .المحتمل للمخاطر، أو عدم القدرة على رفض أو نقل المخاطر
211	Translated (0%)	Avoiding the Risk:	:تجنب المخاطر
212	Translated (0%)	This strategy is used when there is either an inability or unwillingness to accept the risk, leading to stopping the activities that cause it.	تُستخدم هذه الاستراتيجية عندما يكون هناك إما عدم قدرة أو عدم .رغبة في قبول المخاطر، مما يؤدي إلى إيقاف الأنشطة التي تسببها
213	Translated (0%)	Mitigating the Risk:	:التخفيف من المخاطر
214	Translated (0%)	This is the most common strategy, where plans and controls are put in place to reduce the impact and/or likelihood of the risk.	هذه هي الاستراتيجية الأكثر شيوعًا، حيث يتم وضع الخطط .والضوابط لتقليل تأثير و/أو احتمال المخاطر
215	Translated (0%)	Transferring the Risk:	:نقل المخاطر
216	Translated (0%)	This strategy is followed when seeking external parties, such as insurance companies, to bear the consequences of the risk.	يتم اتباع هذه الاستراتيجية عند البحث عن أطراف خارجية، مثل .شركات التأمين، لتحمل عواقب المخاطر
217	Translated (0%)	The results of the risk mitigation process are recorded in the Cybersecurity Risk Register, as shown in Figure 6	يتم تسجيل نتائج عملية التخفيف من المخاطر في سجل مخاطر الأمن السيبراني، كما هو موضح في الشكل 6
218	Translated (0%)	Risk treatment	معالجة المخاطر
219	Translated (100%)	Risk owner	مسؤول إدارة المخاطرة
220	Translated (0%)	Mitigation plan strategy	استراتيجية خطة التخفيف
221	Translated (0%)	Proposed control	الضوابط المقترحة
222	Translated (0%)	Control reference	مرجع التحكم
223	Translated (100%)	Target date	التاريخ المستهدف
224	Translated (0%)	Actual completion date	تاريخ الإنجاز الفعلي
225	Translated (0%)	responsibilities	المسؤوليات
226	Translated	notes	الملاحظات

	(100%)		
227	Translated (100%)	status	الحالة
228	Translated (0%)	Figure 6- risk register- risk treatment	الشكل 6 - سجل المخاطر - معالجة المخاطر
229	Translated (0%)	Risk Acceptance Criteria	معايير قبول المخاطر
230	Translated (0%)	Risk acceptance is the decision by the organization, represented by the risk owner and the cybersecurity oversight committee, to accept the impact of cybersecurity risks.	قبول المخاطر هو القرار الذي تتخذه المنظمة، ممثلة بمسؤول المخاطر ولجنة الإشراف على الأمن السيبراني، لقبول تأثير مخاطر الأمن السيبراني.
231	Translated (0%)	If the risk is accepted, the cybersecurity management team must periodically review all accepted risks to assess their status and report this to the cybersecurity oversight committee.	إذا تم قبول المخاطر، يجب على فريق إدارة الأمن السيبراني مراجعة جميع المخاطر المقبولة بشكل دوري لتقييم حالتها وإبلاغ لجنة الإشراف على الأمن السيبراني بذلك.
232	Translated (0%)	Additionally, mitigation plans for residual risks must be approved.	بالإضافة إلى ذلك، يجب الموافقة على خطط التخفيف من المخاطر المتبقية.
233	Translated (0%)	The following criteria apply for risk acceptance, as detailed in <1201>Table 6</1201>, with the risk acceptance form to be filled out <1207>(Appendix 8.2).</1207>	<تنطبق المعايير التالية لقبول المخاطر، كما هو مفصل في 1201> <الجدول 6</1201>، مع ملء نموذج قبول المخاطر <1207> (الملحق 8.2).</1207>
234	Translated (100%)	Risk assessment	تقييم المخاطر
235	Translated (0%)	Acceptance Criteria	معايير القبول
236	Translated (0%)	Approval Authorities	صلاحيات الموافقة
237	Translated (0%)	Critical risk	مخاطر حرجة
238	Translated (0%)	Critical and High risks are accepted in the following cases:	يتم قبول المخاطر الحرجة والعالية في الحالات التالية:
239	Translated (0%)	<1229/><1232>The cost of implementing the control exceeds the specified budget.</1232>	<1229/><1232>تتجاوز تكلفة تنفيذ الرقابة الميزانية المحددة. </1232>
240	Translated (0%)	<1239/><1242>There is currently no way to mitigate the risk (i.e., no available technical solutions).</1242>	<1239/><1242>لا توجد حاليًا طريقة للتخفيف من المخاطر (أي، <لا توجد حلول تقنية متاحة).1242/>
241	Translated (0%)	The authorized person or the Cybersecurity Oversight Committee.	الشخص المفوض أو لجنة الإشراف على الأمن السيبراني.
242	Translated (100%)	High risk	عالي الخطورة
243	Translated (0%)	<1255/><1258>The risk is accepted temporarily due to the existence of alternative treatment plans, which are planned for future implementation, with the expectation that applying these plans will reduce the risk	<1255/><1258>يتم قبول المخاطر مؤقتًا بسبب وجود خطط علاج بديلة، والتي من المخطط تنفيذها في المستقبل، مع توقع أن <تطبيق هذه الخطط سيقلل من مستوى المخاطر.1258/>

		level.</1258>	
244	Translated (100%)	Medium risk	متوسط الخطورة
245	Translated (0%)	The risk may be accepted or treated by the relevant department manager and the cybersecurity management.	قد يتم قبول المخاطر أو معالجتها من قبل مدير القسم المعني وإدارة الأمن السيبراني.
246	Translated (0%)	The risk owner and cybersecurity management.	المسؤول عن المخاطر وإدارة الأمن السيبراني.
247	Translated (100%)	Low risk	منخفض الخطورة
248	Translated (0%)	Risks with a low severity level are automatically accepted, as they do not affect the safety, security, and availability of sensitive data, systems, and industrial control systems.	يتم قبول المخاطر ذات مستوى الخطورة المنخفض تلقائيًا، لأنها لا تؤثر على سلامة وأمن وتوافر البيانات والأنظمة وأنظمة التحكم الصناعية الحساسة.
249	Translated (100%)	Cybersecurity Management	إدارة الأمن السيبراني
250	Translated (0%)	Table 6- risk acceptance criteria	الجدول 6 - معايير قبول المخاطر
251	Translated (0%)	Cybersecurity Risk Mitigation Based on Risk Severity	التخفيف من مخاطر الأمن السيبراني بناءً على شدة المخاطر
252	Translated (0%)	<1294/><1297>Based on the previous steps and after approving the severity level of cybersecurity risks and their <1300>mitigation</1300> plans, it is crucial to adhere to the specified timeframes for implementing the mitigation plans, as outlined in Table 7.</1297>	بناءً على الخطوات السابقة وبعد الموافقة على<1294/><1297> مستوى خطورة مخاطر الأمن السيبراني وخطط <1300>التخفيف الخاصة بها، من الأهمية بمكان الالتزام بالأطر الزمنية </1300> المحددة لتنفيذ خطط التخفيف، كما هو موضح في الجدول 7.</1297>
253	Translated (0%)	If there are obstacles preventing the implementation of these plans by the approved dates, approval must be obtained from the risk owner and the cybersecurity oversight committee to proceed with the adjusted plans.	إذا كانت هناك عقبات تحول دون تنفيذ هذه الخطط في المواعيد المعتمدة، فيجب الحصول على موافقة من مسؤول المخاطر ولجنة الإشراف على الأمن السيبراني للمضي قدمًا في الخطط المعدلة.
254	Translated (99%)	Risk Assessment	تقييم المخاطر
255	Translated (0%)	priority of treatment	أولوية العلاج
256	Translated (0%)	Required Actions	الإجراءات المطلوبة
257	Translated (99%)	From	من
258	Translated (100%)	To	إلى
259	Translated (100%)	Critical risk	مخاطر حرجة
260	Translated	One week	أسبوع واحد

	(0%)		
261	Translated (0%)	One month	شهر واحد
262	Translated (0%)	<1334/><1337>Immediate action by the Cybersecurity Steering Committee and the authority holder.</1337>	<1334/><1337>اتخاذ إجراء فوري من قبل اللجنة التوجيهية للأمن السيبراني وصاحب الصلاحية.</1337/>
263	Translated (0%)	<1341/><1344>Risk owner to propose mitigation plans for approval by the Steering Committee and authority holder.</1344>	<1341/><1344>يجب على مسؤول المخاطر اقتراح خطط التخفيف للموافقة عليها من قبل اللجنة التوجيهية وصاحب الصلاحية.</1344/>
264	Translated (100%)	High Risk	مخاطرة عالية
265	Translated (100%)	One month	شهر واحد
266	Translated (0%)	Three months	ثلاثة أشهر
267	Translated (0%)	• Immediate intervention by the risk owner's department manager.	• التدخل الفوري من قبل مدير قسم المسؤول عن المخاطر.
268	Translated (0%)	Medium Risk	مخاطر متوسطة
269	Translated (100%)	Three months	ثلاثة أشهر
270	Translated (0%)	Six months	ستة أشهر
271	Translated (0%)	• Risk owner to propose mitigation plans for approval by relevant parties.	• يجب على مسؤول المخاطر اقتراح خطط التخفيف للموافقة عليها من قبل الأطراف ذات الصلة.
272	Translated (100%)	Low Risk	مخاطرة منخفضة
273	Translated (0%)	Does not apply	لا ينطبق
274	Translated (0%)	Table 7- risk treatment priority	الجدول 7 - أولوية معالجة المخاطر
275	Translated (0%)	Risk Monitoring	مراقبة المخاطر
276	Translated (0%)	Key Risk Indicators (KRIs)	مؤشرات المخاطر الرئيسية (KRIs)
277	Translated (0%)	<1387/><1390>Key Risk Indicators (KRIs) are metrics or measures used as an early warning system to detect increased likelihood of cybersecurity risks that could impact the achievement of an organization’s strategic and operational objectives.</1390>	<1387/><1390>هي مقاييس (KRIs) مؤشرات المخاطر الرئيسية أو مقاييس تستخدم كنظام إنذار مبكر للكشف عن زيادة احتمالية مخاطر الأمن السيبراني التي يمكن أن تؤثر على تحقيق الأهداف الاستراتيجية والتشغيلية للمؤسسة.</1390/>
278	Translated	KRIs help in monitoring the state of risks, proactively managing them, and	تساعد مؤشرات المخاطر الرئيسية في مراقبة حالة المخاطر وإدارتها

	(0%)	implementing appropriate mitigation plans to reduce their impact when they occur.	بشكل استباقي وتنفيذ خطط التخفيف المناسبة للحد من تأثيرها عند حدوثها.
279	Translated (0%)	Cybersecurity KRIs are identified for critical and high-risk areas and are categorized into three levels for each key risk indicator (acceptable level, exceeding average, exceeding high).	يتم تحديد مؤشرات المخاطر الرئيسية للأمن السيبراني للمناطق الحرجة وعالية المخاطر ويتم تصنيفها إلى ثلاثة مستويات لكل مؤشر مخاطر رئيسي (مستوى مقبول، يتجاوز المتوسط، يتجاوز المرتفع).
280	Translated (0%)	Reporting and escalation will be based on the degree or level of the indicator, following the methodology outlined in <1393>Table 8</1393>.	يعتمد الإبلاغ والتصعيد على درجة أو مستوى المؤشر، باتباع المنهجية الموضحة في <1393>الجدول 8</1393>.
281	Translated (0%)	#	#
282	Translated (100%)	Indicator Name	اسم المؤشر
283	Translated (0%)	Indicator Description	وصف المؤشر
284	Translated (0%)	Unit of Measure of the Indicator	وحدة قياس المؤشر
285	Translated (0%)	Levels of Key Risk Indicator	مستويات مؤشر المخاطر الرئيسية
286	Translated (0%)	Justifications	المبررات
287	Translated (0%)	Treatment Plans	خطط العلاج
288	Translated (99%)	Target Date	التاريخ المستهدف
289	Translated (100%)	1	1
290	Translated (0%)	Cybersecurity risk indicator definition	تعريف مؤشر مخاطر الأمن السيبراني
291	Translated (0%)	Purpose of monitoring the indicator	الغرض من مراقبة المؤشر
292	Translated (0%)	determine the Measurement Method of the indicator (Percentage /number	تحديد طريقة قياس المؤشر (النسبة /العدد
293	Translated (0%)	Acceptable level	المستوى المقبول
294	Translated (0%)	Medium exceeded	تم تجاوز المتوسط
295	Translated (0%)	High exceeded	تم تجاوز الارتفاع
296	Translated (0%)	Description of Justifications for exceeding the critical risk indicator level	وصف مبررات تجاوز مستوى مؤشر المخاطر الحرجة

297	Translated (0%)	Treatment plans for addressing exceeding acceptable levels	خطط العلاج لمعالجة تجاوز المستويات المقبولة
298	Translated (0%)	Target date addressing exceeding of the main risk indicator level	التاريخ المستهدف الذي يتناول تجاوز مستوى مؤشر المخاطر الرئيسي
299	Translated (0%)	Table 8- key risk indicators	الجدول 8 - مؤشرات المخاطر الرئيسية
300	Translated (0%)	Risk monitoring and reporting should be conducted in cases of significant changes or to prioritize treatment.	يجب إجراء مراقبة المخاطر والإبلاغ عنها في حالات التغييرات المهمة أو لتحديد أولويات العلاج.
301	Translated (0%)	Factors to be monitored and reported include, but are not limited to:	تشمل العوامل التي يجب مراقبتها والإبلاغ عنها، على سبيل المثال لا الحصر:
302	Translated (0%)	Emergence of new incident scenarios	ظهور سيناريوهات جديدة للحوادث
303	Translated (0%)	Increased impact or consequences of incident scenarios and risks, leading to an unacceptable risk level	زيادة تأثير أو عواقب سيناريوهات ومخاطر الحوادث، مما يؤدي إلى مستوى مخاطر غير مقبول
304	Translated (0%)	Effectiveness of current control measures	فعالية تدابير الرقابة الحالية
305	Translated (0%)	Cybersecurity evaluation activities such as vulnerability assessments, penetration testing, security reviews, audit reports	أنشطة تقييم الأمن السيبراني مثل تقييمات الثغرات الأمنية واختبار الاختراق والمراجعات الأمنية وتقارير التدقيق
306	Translated (0%)	<1499/><1502>Escalation mechanisms should be applied for moderate and critical levels as outlined in <1505>Table 9</1505></1502>	يجب تطبيق آليات التصعيد على المستويات<1502><1499/> المعتدلة والحرجة كما هو موضح في <1505>الجدول 9</1505></1502>
307	Translated (100%)	#	#
308	Translated (100%)	Levels of Key Risk Indicator	مستويات مؤشر المخاطر الرئيسية
309	Translated (0%)	Escalation Level	مستوى التصعيد
310	Translated (99%)	Action	الإجراء
311	Translated (100%)	1	1
312	Translated (0%)	High Exceeded	تم تجاوز الحد الأقصى
313	Translated (0%)	The authority holder and the cybersecurity oversight committee	صاحب الصلاحية ولجنة الرقابة على الأمن السيبراني
314	Translated (0%)	Provide support and take necessary actions to develop and implement mitigation plans.	تقديم الدعم واتخاذ الإجراءات اللازمة لوضع وتنفيذ خطط التخفيف.
315	Translated (100%)	2	2

316	Translated (0%)	Medium Exceeded	تم تجاوز المتوسط
317	Translated (0%)	The Cybersecurity Oversight Committee	لجنة الرقابة على الأمن السيبراني
318	Translated (100%)	3	3
319	Translated (0%)	Acceptable Level	المستوى المقبول
320	Translated (100%)	Risk Owner	مسؤول إدارة المخاطرة
321	Translated (0%)	No action required.	.لا يلزم اتخاذ أي إجراء
322	Translated (0%)	Table 9- risk indicator- escalation mechanism	الجدول 9 - مؤشر المخاطر - آلية التصعيد
323	Translated (0%)	<1557/><1560>The results of the risk monitoring process are recorded in the Cybersecurity Risk Register as shown in <1563>Figure 7</1563>.</1560>	يتم تسجيل نتائج عملية مراقبة المخاطر في<1560><1557/> سجل مخاطر الأمن السيبراني كما هو موضح في <1563>الشكل 7</1563>.</1560>
324	Translated (0%)	risk monitoring	رصد المخاطر
325	Translated (0%)	Key risk indicators (KRIs)	(KRIs) مؤشرات المخاطر الرئيسية
326	Translated (0%)	Monitoring/ reporting responsible	مسؤول المراقبة/ الإبلاغ
327	Translated (0%)	Figure 7- risk register- risk monitoring	الشكل 7 - سجل المخاطر - مراقبة المخاطر
328	Translated (0%)	Risk Review	مراجعة المخاطر
329	Translated (0%)	Cybersecurity risks are reviewed by the Cybersecurity Management to ensure their continued relevance, adequacy, and effectiveness.	تتم مراجعة مخاطر الأمن السيبراني من قبل إدارة الأمن السيبراني .لضمان استمرار أهميتها وكفايتها وفعاليتها
330	Translated (0%)	Regular reports are issued to the Cybersecurity Oversight Committee and the risk owner.	يتم إصدار تقارير منتظمة إلى لجنة الإشراف على الأمن السيبراني .والمسؤول عن المخاطر
331	Translated (0%)	The management must also regularly verify that the cybersecurity risk measurement methodology is consistent with the institution’s approved enterprise risk methodology and that changes in the organizational <1593>context</1593> for risk management are considered during the cybersecurity risk assessment process.	يجب على الإدارة أيضًا التحقق بانتظام من أن منهجية قياس مخاطر الأمن السيبراني تتوافق مع منهجية مخاطر المؤسسة المعتمدة <للمؤسسة وأنه يتم النظر في التغييرات في <1593>السياق</1593 التنظيمي لإدارة المخاطر أثناء عملية تقييم مخاطر الأمن السيبراني.
332	Translated (0%)	The monitoring and review activities include, but are not limited to, the following:	تشمل أنشطة المراقبة والمراجعة، على سبيل المثال لا الحصر، ما :يلي
333	Translated	Organizational context	السياق التنظيمي

	(0%)		
334	Translated (0%)	Risk assessment methodology	منهجية تقييم المخاطر
335	Translated (0%)	Impact and likelihood criteria	معايير التأثير والاحتمال
336	Translated (0%)	Risk assessment criteria	معايير تقييم المخاطر
337	Translated (0%)	Risk acceptance criteria	معايير قبول المخاطر
338	Translated (0%)	Reporting	الإبلاغ
339	Translated (0%)	<1621/><1624>As part of the Cybersecurity Risk Management methodology, the process includes the periodic reporting phase to the risk owner and the Cybersecurity Oversight Committee.</1624>	<1621/><1624>،كجزء من منهجية إدارة مخاطر الأمن السيبراني تتضمن العملية مرحلة الإبلاغ الدوري إلى مسؤول المخاطر ولجنة الإشراف على الأمن السيبراني.</1624/>
340	Translated (0%)	These <1627>reports</1627> highlight the status of cybersecurity risks and the progress of mitigation plans within the organization, as well as requesting support from decision-makers.	تسلط هذه <1627>التقارير</1627/> الضوء على حالة مخاطر الأمن السيبراني والتقدم المحرز في خطط التخفيف داخل المنظمة، وكذلك طلب الدعم من صناع القرار.
341	Translated (0%)	<1633>Figure 8</1633> illustrates the periodic report escalation process.	يوضح <1633>الشكل 8</1633/> عملية تصعيد التقرير الدوري.
342	Translated (0%)	Reporting frequency-Monthly-Quarterly-Last meeting of the year for the-cybersecurity steering committee-Risk level at which reports are raised in their status-Medium Risks-High Risks-Critical Risks-High Risks-Critical Risks-Medium Risks-High Risks-Critical Risks-Stakeholders-Cybersecurity Department Manager-Cybersecurity-Department Manager Cybersecurity Steering Committee-Authorized Owner Cybersecurity Steering Committee	وتيرة تقديم التقارير - شهريًا - ربع سنوي - الاجتماع الأخير من السنة للجنة التوجيهية للأمن السيبراني - مستوى المخاطر الذي - ترفع عنده التقارير في حالتها - مخاطر متوسطة - مخاطر عالية - مخاطر حرجة - مخاطر عالية - مخاطر حرجة - مخاطر متوسطة مخاطر عالية - مخاطر حرجة - أصحاب المصلحة - مدير إدارة الأمن السيبراني - مدير إدارة الأمن السيبراني - اللجنة التوجيهية للأمن السيبراني - المسؤول المعتمد - اللجنة التوجيهية للأمن السيبراني
343	Translated (0%)	Communication & Consultation	التواصل والاستشارات
344	Translated (0%)	Communication and consultation with relevant stakeholders in the processes and activities of cybersecurity risk management should occur at all stages.	يجب أن يتم التواصل والتشاور مع أصحاب المصلحة المعنيين في عمليات وأنشطة إدارة مخاطر الأمن السيبراني في جميع المراحل.
345	Translated (0%)	Therefore, the cybersecurity management team must develop a communication and consultation plan early in the cybersecurity risk <1645>assessment</1645> process.	لذلك، يجب على فريق إدارة الأمن السيبراني وضع خطة اتصال واستشارة في وقت مبكر من عملية <1645>تقييم</1645/> مخاطر الأمن السيبراني.
346	Translated (0%)	This plan should address topics related to cybersecurity risks, their causes, and consequences (if known), as well as the measures being taken to address them.	يجب أن تتناول هذه الخطة الموضوعات المتعلقة بمخاطر الأمن السيبراني وأسبابها وعواقبها (إذا كانت معروفة)، بالإضافة إلى التدابير التي يتم اتخاذها لمعالجتها.
347	Translated (0%)	Effective communication with the risk owner and those responsible for implementing the proposed controls should be ensured.	يجب ضمان التواصل الفعال مع المسؤول عن المخاطر والمسؤولين عن تنفيذ الضوابط المقترحة.
348	Translated	Roles and Responsibilities Matrix for the Risk Framework (RASCI)	مصفوفة الأدوار والمسؤوليات لإطار المخاطر (RASCI)

	(0%)		
349	Translated (99%)	Role	الدور
350	Translated (99%)	Responsible	الجهة المسؤولة
351	Translated (0%)	Preparation, Updating, and Review	الإعداد والتحديث والمراجعة
352	Translated (0%)	Approval	الاعتماد
353	Translated (100%)	Publication	النشر
354	Translated (99%)	Compliance	الامتثال
355	Translated (99%)	Implementation	:التنفيذ
356	Translated (0%)	Enforcement of Penalties	تنفيذ العقوبات
357	Translated (0%)	Authority Owner	صاحب الصلاحية
358	Translated (0%)	-	-
359	Translated (0%)	Implementer	المُنفذ
360	Translated (100%)	-	-
361	Translated (100%)	-	-
362	Translated (100%)	Consulted	مُستشار
363	Translated (100%)	-	-
364	Translated (0%)	Cybersecurity Oversight Committee	لجنة الإشراف على الأمن السيبراني
365	Translated (100%)	Responsible	الجهة المسؤولة
366	Translated (99%)	Support	الدعم
367	Translated (100%)	-	-

368	Translated (100%)	Support	الدعم
369	Translated (100%)	Responsible	الجهة المسؤولة
370	Translated (0%)	Responsible & Implementer	الجهة المسؤولة والمنفذة
371	Translated (100%)	Cybersecurity Management	إدارة الأمن السيبراني
372	Translated (100%)	Implementer	المُنفذ
373	Translated (100%)	Responsible	الجهة المسؤولة
374	Translated (100%)	Responsible	الجهة المسؤولة
375	Translated (100%)	Responsible & Implementer	الجهة المسؤولة والمنفذة
376	Translated (100%)	Implementer	المُنفذ
377	Translated (100%)	Support	الدعم
378	Translated (0%)	Public Relations and Media Management	إدارة العلاقات العامة والإعلام
379	Translated (100%)	-	-
380	Translated (100%)	-	-
381	Translated (100%)	Implementer	المُنفذ
382	Translated (100%)	-	-
383	Translated (100%)	-	-
384	Translated (100%)	-	-
385	Translated (0%)	General Administration for Education and Training	الإدارة العامة للتعليم والتدريب
386	Translated (100%)	-	-
387	Translated	-	-

	(100%)		
388	Translated (100%)	-	-
389	Translated (100%)	-	-
390	Translated (100%)	-	-
391	Translated (100%)	-	-
392	Translated (0%)	All IT and Computer Departments in the Organization	جميع أقسام تكنولوجيا المعلومات والحاسوب في المنظمة
393	Translated (100%)	-	-
394	Translated (100%)	-	-
395	Translated (100%)	-	-
396	Translated (100%)	-	-
397	Translated (100%)	Support	الدعم
398	Translated (100%)	-	-
399	Translated (0%)	General Administration of Security and Protection	الإدارة العامة للأمن والحماية
400	Translated (100%)	-	-
401	Translated (100%)	-	-
402	Translated (100%)	-	-
403	Translated (100%)	-	-
404	Translated (100%)	Support	الدعم
405	Translated (100%)	Support	الدعم
406	Translated (0%)	General Administration of Administrative and Financial Affairs	الإدارة العامة للشؤون الإدارية والمالية

407	Translated (100%)	-	-
408	Translated (100%)	-	-
409	Translated (100%)	-	-
410	Translated (100%)	-	-
411	Translated (100%)	Support	الدعم
412	Translated (100%)	-	-
413	Translated (100%)	Internal Audit Unit	إدارة التدقيق الداخلي
414	Translated (100%)	Support	الدعم
415	Translated (100%)	-	-
416	Translated (100%)	-	-
417	Translated (100%)	-	-
418	Translated (100%)	Support	الدعم
419	Translated (100%)	Consulted	مُستشار
420	Translated (100%)	Legal Affairs Department	إدارة الشؤون القانونية
421	Translated (100%)	-	-
422	Translated (100%)	-	-
423	Translated (100%)	-	-
424	Translated (100%)	-	-
425	Translated (100%)	Support	الدعم
426	Translated	-	-

	(100%)		
427	Translated (0%)	All Other Departments and Sections	جميع الإدارات والأقسام الأخرى
428	Translated (100%)	-	-
429	Translated (100%)	-	-
430	Translated (100%)	-	-
431	Translated (100%)	-	-
432	Translated (100%)	Support	الدعم
433	Translated (100%)	-	-
434	Translated (0%)	Terminology and Definitions	المصطلحات والتعاريف
435	Translated (0%)	The following words and <1942>phrases</1942>, wherever they appear in this document, are intended to have the meanings specified in the context of the text, unless otherwise stated:	يقصد بالكلمات <1942>والعبارات</1942> التالية، أينما وردت في هذا المستند، أن يكون لها المعاني المحددة في سياق النص، ما لم ينص على خلاف ذلك:
436	Translated (0%)	Annexes	الملحقات
437	Translated (0%)	<1950/><1953>Risk Register Template</1953>	<نموذج سجل المخاطر</1953></1950/>
438	Translated (0%)	<1962>Identifying the Risks-</1962><1965>Risk Code- <1969>Process / Asset- Risk- <1972>Causes/</1972></1969></1965>	- <تحديد المخاطر - رمز المخاطر</1962></1965></1962> /العملية / الأصول - <1972>أسباب المخاطر</1969> </1972></1969></1965>
439	Translated (0%)	<1975>Source of Risk- </1975>Expected Risk Scenario- <1981>Current</1981>	مصدر المخاطر - </1975><1975>سيناريو المخاطر المتوقع <1981>-1981/>الحالي<
440	Translated (0%)	<1984>Control</1984><1987> </1987><1991>Measures</1991>	تدابير</1991></1984><1991/> الرقابة<1991></1987> <1987> </1984>
441	Translated (0%)	Risk analysis and evaluation-Evaluation of Current Control Measures-Impact-Probability-Residual Risk Level	- تحليل المخاطر وتقييمها - تقييم تدابير الرقابة الحالية - التأثير الاحتمالية - مستوى المخاطر المتبقية
442	Translated (0%)	<2014/><2020><2017>Treatment</2017>-<2023>Risk Owner-Mitigation Plan Strategy-Proposed Control-Control Reference-Target Date-Actual Completion Date-Responsibilities-Notes-Status</2023></2020>	العلاج</2017>- مسؤول إدارة<2014/></2020></2017> - المخاطرة<2023> - استراتيجية خطة التخفيف - التحكم المقترح - مرجع التحكم - التاريخ المستهدف - تاريخ الإنجاز الفعلي - المسؤوليات - الملاحظات - الحالة</2023></2020/>
443	Translated (0%)	<2026>Risk Monitoring- </2026>Key Risk Indicators (KRIs)- Monitoring/Reporting Responsible	مراقبة المخاطر - </2026><2026>مؤشرات المخاطر الرئيسية مسؤول المراقبة/الإبلاغ -(KRIs)

444	Translated (0%)	Risk Monitoring-<2047>Current Review Date-Impact-Probability-Residual Risk</2047> <2053>Level-Review</2053> <2059>Frequency-Next Review</2059> <2065>Date-Responsibilities</2065>	- مراقبة المخاطر -<2047>تاريخ المراجعة الحالي - التأثير الاحتمالية - مستوى المخاطر</2047> <2053>المتبقية - تكرار المراجعة - تاريخ المراجعة التالي -</2053> <2059>2059/></2059> <2065>المسؤوليات</2065>
445	Translated (100%)	Compliance and Adherence	الامتثال والالتزام
446	Translated (100%)	Al Hammadi Holding CEO shall ensure compliance with the cybersecurity policies and standards.	يضمن الرئيس التنفيذي لشركة الحمادي القابضة الامتثال لسياسات ومعايير الأمن السيبراني.
447	Translated (100%)	To ensure compliance, the Cybersecurity department will establish regular reporting by the Cybersecurity Manager, conduct periodic audits, or form a Cybersecurity Committee for oversight.	لضمان الامتثال، سينشئ قسم الأمن السيبراني نظامًا لتقديم تقارير منتظمة يُعدّها مدير الأمن السيبراني، ويجري عمليات تدقيق دورية، أو يشكل لجنة للأمن السيبراني للإشراف.
448	Translated (100%)	The CS manager shall ensure adherence to this policy.	يتعين على مدير الأمن السيبراني ضمان الالتزام بهذه السياسة.
449	Translated (100%)	All employees of Al Hammadi Holding must adhere to this policy.	على جميع موظفي شركة الحمادي القابضة الالتزام بهذه السياسة.
450	Translated (100%)	Violations of this policy may result in legal action in any jurisdiction or other measures as deemed appropriate by the Al Hammadi Holding.	قد تؤدي انتهاكات هذه السياسة إلى اتخاذ إجراءات قانونية في أي ولاية قضائية أو غيرها من التدابير التي تراها شركة الحمادي القابضة مناسبة.
451	Translated (100%)	Exceptions	الاستثناءات
452	Translated (100%)	Violation of cybersecurity policies and standards is prohibited unless a prior justified exception is obtained from the Cybersecurity Department or the Cybersecurity Steering Committee.	يُحظر انتهاك سياسات ومعايير الأمن السيبراني ما لم يتم الحصول على استثناء مبرر مسبق من إدارة الأمن السيبراني أو اللجنة التوجيهية للأمن السيبراني.
453	Translated (100%)	In case of a conflict, applicable legislative and regulatory requirements overrule Al Hammadi Holding policies and standards.	في حالة وجود تعارض، فإن المتطلبات التشريعية والتنظيمية المعمول بها تسود على سياسات ومعايير شركة الحمادي القابضة.
454	Translated (100%)	Revision	المراجعة
455	Translated (99%)	This policy is reviewed annually, after major changes in Al Hammadi Holding’s organizational chart or infrastructure, and more frequently whenever required, to ensure it remains appropriate and current for Al Hammadi Holding, ISO 27001, and NCA requirements	تخضع هذه السياسة لمراجعة سنوية، ولإعادة التقييم بعد أي تغييرات جوهرية في الهيكل التنظيمي أو البنية التحتية لشركة الحمادي القابضة، إضافة إلى مراجعات دورية إضافية عند الضرورة، وذلك لضمان توافقها المستمر مع متطلبات شركة الحمادي القابضة وإرشادات الهيئة الوطنية للأمن، ISO 27001:2022 ومعيار آيزو السيبراني
456	Translated (100%)	Approval Section	قسم الاعتماد
457	Translated (100%)	Prepared by:	إعداد:
458	Translated (100%)	Mr. Mohammed Alamer	السيد/ محمد العامر

459	Translated (100%)	GRC Cybersecurity Specialist	أخصائي حوكمة ومخاطر وامتثال في الأمن السيبراني
460	Translated (100%)	Name	الاسم
461	Translated (100%)	Designation	المسمى الوظيفي
462	Translated (100%)	Signature	التوقيع
463	Translated (100%)	Date	التاريخ
464	Translated (100%)	Reviewed by:	:راجعها
465	Translated (100%)	Ms. Mashael Alotaibi	السيدة/ مشاعل العتيبي
466	Translated (0%)	Cybersecurity Manager	مدير الأمن السيبراني
467	Translated (100%)	Name	الاسم
468	Translated (100%)	Designation	المسمى الوظيفي
469	Translated (100%)	Signature	التوقيع
470	Translated (100%)	Date	التاريخ
471	Translated (100%)	Reviewed by:	:راجعها
472	Translated (0%)	Mr. Wahid Raafat	السيد/ وحيد رأفت
473	Translated (100%)	Chief Audit Executive	المدير التنفيذي لعمليات التدقيق
474	Translated (100%)	Name	الاسم
475	Translated (100%)	Designation	المسمى الوظيفي
476	Translated (100%)	Signature	التوقيع
477	Translated (100%)	Date	التاريخ
478	Translated	Approved by:	:اعتمدها

	(100%)		
479	Translated (100%)	Dr. Abdulaziz Al Hammadi	الحمادي<Bold><Bold> د./ عبد العزيز</Bold></Bold> <Bold><Bold></Bold></Bold>
480	Translated (100%)	Chief Operating Officer	الرئيس التنفيذي للعمليات
481	Translated (100%)	Name	الاسم
482	Translated (100%)	Designation	المسمى الوظيفي
483	Translated (100%)	Signature	التوقيع
484	Translated (100%)	Date	التاريخ
485	Translated (100%)	Approved by:	:اعتمدها
486	Translated (100%)	Mr. Mohammad AlHammadi	السيد/ محمد الحمادي
487	Translated (100%)	Chief Executive Officer	الرئيس التنفيذي
488	Translated (100%)	Name	الاسم
489	Translated (100%)	Designation	المسمى الوظيفي
490	Translated (100%)	Signature	التوقيع
491	Translated (100%)	Date	التاريخ

Segment ID	Segment status	Source segment	Target segment
1	Translated (0%)	<3/>Operation Cybersecurity Web Application Policy<7/><11/>	<11></7>تشغيل تطبيقات الويب للأمن السيبراني</3>سياسة />
2	Translated (100%)	Page <28><19/> of <27/></28>	<28><19/> من <27/></28>صفحة
3	Translated (100%)	Al Hammadi Holding	شركة الحمادي القابضة
4	Translated (0%)	Operation Cybersecurity Web Application Policy	سياسة تشغيل تطبيقات الويب للأمن السيبراني
5	Translated (100%)	CYBERSECURITY DEPARTMENT	إدارة الأمن السيبراني
6	Translated (100%)	Policy ID	معرّف السياسة
7	Translated (100%)	AHH-CS-ISMS-004	AHH-CS-ISMS-004
8	Translated (100%)	Class	الفئة
9	Translated (100%)	Internal Release	إصدار داخلي
10	Not Translated (0%)		
11	Translated (100%)	V1.0	V1.0
12	Translated (100%)	Published at	نُشرت في
13	Translated (100%)	April 2025	أبريل 2025
14	Translated (100%)	Document Owner	المسؤول عن المستند
15	Translated (100%)	Cybersecurity <89>Department</89>	<89>الأمن السيبراني</89>إدارة
16	Translated (100%)	Disclaimer	تنويه
17	Translated (100%)	The information contained in this document is the property of Al Hammadi Holding and must not be copied or communicated to a third party or used for any purpose other than that for which it is supplied, without the written consent of Al Hammadi Holding.	المعلومات الواردة في هذا المستند هي ملك لشركة الحمادي القابضة ولا يجوز نسخها أو إبلاغها إلى طرف ثالث أو استخدامها لأي غرض آخر غير الغرض الذي تم توفيرها من أجله، دون موافقة خطية من شركة الحمادي القابضة.

18	Translated (100%)	Contents	جدول المحتويات
19	Translated (100%)	Document Control	ضبط المستندات
20	Translated (100%)	Document Information	معلومات المستند
21	Translated (100%)	Synopsis	الملخص
22	Translated (100%)	Document Title:	:عنوان المستند
23	Translated (0%)	Operation Cybersecurity Web Application Policy<167> Document Status:</167>	<167> 167/>:حالة وثيقة سياسة تطبيق الويب للأمن السيبراني<
24	Translated (100%)	Approved	معتمد
25	Translated (100%)	Document Effective Date:	:تاريخ سريان المستند
26	Translated (100%)	April 2025	أبريل 2025
27	Translated (100%)	Document Issue Date:	:تاريخ إصدار المستند
28	Translated (100%)	April 2025	أبريل 2025
29	Translated (100%)	Document Next Revision Date:	:تاريخ المراجعة التالية للمستند
30	Translated (100%)	April <212>2026</212>	212/>2026<212> أبريل<
31	Translated (100%)	Key contacts	جهات التواصل الرئيسية
32	Translated (100%)	Document Owner:	:المسؤول عن المستند
33	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
34	Translated (100%)	Approval Authority	جهة الاعتماد
35	Translated (100%)	Document Created by:	:مُنشئ المستند
36	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
37	Translated	Document Reviewed by:	:راجع المستند

	(100%)		
38	Translated (100%)	Al Hammadi Holding CS Manager	مدير الأمن السيبراني في شركة الحمادي القابضة
39	Translated (100%)	Document Approved by:	اعتمد المستند:
40	Translated (100%)	Al Hammadi Holding COO & CEO	الرئيس التنفيذي للعمليات والرئيس التنفيذي في شركة الحمادي القابضة
41	Translated (100%)	Note:	ملاحظة:
42	Translated (100%)	Any additional approval will be added in the document annex	تُضاف أي اعتمادات إضافية في ملحق المستند
43	Translated (100%)	Classification	التصنيف
44	Translated (100%)	<293>Company Internal</293> – to be shared with 3rd parties after consent of CS Manager	داخلي لاستخدام للشركة – <293/>يُسمح بمشاركته مع جهات خارجية<293> بعد موافقة مدير إدارة الأمن السيبراني
45	Translated (100%)	Version / Dates	الإصدار / التواريخ
46	Translated (100%)	Current Version:	الإصدار الحالي:
47	Translated (100%)	V 1.0	V 1.0
48	Translated (100%)	Date Published:	تاريخ النشر:
49	Translated (100%)	April 2025	أبريل 2025
50	Translated (100%)	Date of Next Review:	تاريخ المراجعة التالية:
51	Translated (100%)	April 2026	أبريل 2026
52	Translated (100%)	Document Changes	التغييرات على المستند
53	Translated (100%)	Date	التاريخ
54	Translated (100%)	Version	الإصدار
55	Translated (100%)	Document Owner	المسؤول عن المستند
56	Translated (100%)	Change Description	وصف التغيير

57	Translated (100%)	April <356>2025</356>	<356>أبريل <356/>2025
58	Translated (100%)	1.0	1.0
59	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
60	Translated (100%)	Document Established	تم إنشاء المستند
61	Translated (100%)	Document Circulation	تعميم المستند
62	Translated (100%)	To	إلى
63	Translated (100%)	Date	التاريخ
64	Translated (100%)	Method	الطريقة
65	Translated (100%)	IT Staff	موظفو تكنولوجيا المعلومات
66	Translated (100%)	April 2025	أبريل 2025
67	Translated (100%)	Intranet Portal	بوابة الإنترانت
68	Translated (100%)	All Al Hammadi Staff	جميع موظفي شركة الحمادي
69	Translated (100%)	April 2025	أبريل 2025
70	Translated (100%)	Intranet Portal	بوابة الإنترانت
71	Translated (100%)	Objectives	الأهداف
72	Translated (0%)	This Policy aims to provide the requirements of cybersecurity based on best practices and standards related to the protection of external web applications, in order to ensure the protection of technical and digital resources and assets of the Al Hammadi from internal and external risks and threats.	تهدف هذه السياسة إلى توفير متطلبات الأمن السيبراني بناءً على أفضل الممارسات والمعايير المتعلقة بحماية تطبيقات الويب الخارجية، من أجل ضمان حماية الموارد والأصول التقنية والرقمية للحمادي من المخاطر والتهديدات الداخلية والخارجية.
73	Translated (0%)	Additionally, this Policy aims to comply with the requirements of cybersecurity and related legislative, and regulatory requirements, which are legislative requirements in cybersecurity controls issued by the National Cybersecurity Authority (NCA).	بالإضافة إلى ذلك، تهدف هذه السياسة إلى الامتثال لمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات الصلة، وهي المتطلبات التشريعية في ضوابط الأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني (NCA).

74	Translated (100%)	Key Outcomes of Implementing the Principles and Procedural	النتائج الرئيسية لتنفيذ المبادئ والإجراءات
75	Translated (0%)	This Policy complies with the national legislative and regulatory requirements.	.تتوافق هذه السياسة مع المتطلبات التشريعية والتنظيمية الوطنية
76	Translated (0%)	It is also	كما أنه
77	Translated (0%)	legal requirement as dictated by Control No. (2-15-1) of the Essential Cybersecurity Controls (ECC:1:2018) issued by the National Cybersecurity Authority.	المتطلبات القانونية على النحو الذي تمليه الرقابة رقم (2-15-1) من ضوابط الصادرة عن الهيئة الوطنية للأمن (ECC:1:2018) الأمن السيبراني الأساسية .السيبراني
78	Translated (100%)	Protecting Al Hammadi 's digital data and assets from cybersecurity risks.	.حماية بيانات وأصول شركة الحمادي الرقمية من مخاطر الأمن السيبراني
79	Translated (100%)	Scope	النطاق
80	Translated (100%)	This policy applies to all Al Hammadi Holding Cybersecurity Management operations, assets, and activities, including employees, contractors, suppliers, and third parties under its control.	تنطبق هذه السياسة على جميع عمليات وأصول وأنشطة إدارة الأمن السيبراني لشركة الحمادي القابضة، بما في ذلك الموظفين والمتعاقدين والموردين .والجهات الخارجية الخاضعة لسيطرتها
81	Translated (100%)	It covers all IT systems, information assets, and operational risks relevant to ensuring patient safety, employee well-being, compliance with legal standards, and operational continuity.	تغطي السياسة جميع أنظمة تكنولوجيا المعلومات وأصول المعلومات والمخاطر التشغيلية ذات الصلة بضمان سلامة المرضى ورفاهية الموظفين والامتثال .للمعايير القانونية واستمرارية التشغيل
82	Translated (100%)	Roles and Responsibilities	الأدوار والمسؤوليات
83	Translated (100%)	Al Hammadi Holding management is responsible for implementing, maintaining, and updating this policy with all its contents, in accordance with any changes in the Statement of Applicability, Al Hammadi Holding-SOA Document.	تتحمل إدارة شركة الحمادي القابضة مسؤولية تنفيذ هذه السياسة وحفظها وتحديثها بكامل محتوياتها، وذلك بما يتماشى مع أي تغييرات في بيان التطبيق .الخاص بشركة الحمادي القابضة
84	Translated (100%)	Principles	المبادئ
85	Translated (0%)	Cybersecurity Requirements for Protecting General Web Applications	متطلبات الأمن السيبراني لحماية تطبيقات الويب العامة
86	Translated (0%)	The Cybersecurity Department shall adhere to the following:	:تلتزم إدارة الأمن السيبراني بما يلي
87	Translated (0%)	Ensuring that all external web applications of the Al Hammadi, which are purchased or developed internally, follow the principle of Multi-tier Architecture.	التأكد من أن جميع تطبيقات الويب الخارجية للحمادي، والتي يتم شراؤها أو .تطويرها داخليًا، تتبع مبدأ العمارة متعددة المستويات
88	Translated (0%)	Ensuring that all external web applications of the Al Hammadi<501> </501>use the principle of multi-tier Architecture for external web applications of critical<516> </516>systems, provided that the number of tiers is not less than 3.	التأكد من أن جميع تطبيقات الويب الخارجية للحمادي<501> </501>تستخدم <مبدأ العمارة متعددة المستويات لتطبيقات الويب الخارجية<516> </516> .للأنظمة الحرجة، شريطة ألا يقل عدد المستويات عن 3

89	Translated (0%)	Ensuring that only secure communication protocols are enabled, such as HTTPS, SFTP, Transport Layer Security (TLS) and others.	وأمن SFTP و HTTPS التأكد من تمكين بروتوكولات الاتصال الآمنة فقط، مثل وغيرها (TLS) طبقة النقل.
90	Translated (0%)	<528>Ensuring that the Web Application Firewall (WAF) system is used to protect external web applications from external attacks</528>.	لحماية (WAF) التأكد من استخدام نظام جدار حماية تطبيقات الويب<528> تطبيقات الويب الخارجية من الهجمات الخارجية<528/>.
91	Translated (0%)	Ensuring that the Development Environment, Testing Environment, and	التأكد من أن بيئة التطوير وبيئة الاختبار و
92	Translated (0%)	Production environments are logically isolated.	بيئات الإنتاج معزولة منطقيًا.
93	Translated (0%)	Using data and information protection technologies on the external web	استخدام تقنيات حماية البيانات والمعلومات على الويب الخارجي
94	Translated (0%)	applications in accordance with the policies approved by Al Hammadi.	الطلبات وفقًا للسياسات المعتمدة من قبل الحمادي.
95	Translated (0%)	Implementing the Minimum Application Security and Protection Standards	تطبيق معايير الحد الأدنى لأمن التطبيقات وحمايتها
96	Translated (0%)	(OWASP Top Ten) for External Web Applications for Critical Systems and	لتطبيقات الويب الخارجية للأنظمة الحرجة و (OWASP TOP TEN)
97	Translated (0%)	Industrial Control Systems.	أنظمة التحكم الصناعية.
98	Translated (0%)	Publishing the safe web application usage policy and educating the Al	نشر سياسة استخدام تطبيقات الويب الآمنة وتثقيف
99	Translated (0%)	Hammadi's<579> </579>employees about it.	موظفي الحمادي حول هذا الموضوع<579> </579>.
100	Translated (0%)	Using KPI to ensure the continuous development of an external web application protection.	استخدام مؤشرات الأداء الرئيسية لضمان التطوير المستمر لحماية تطبيقات الويب الخارجية.
101	Translated (0%)	Reviewing this Policy and the cybersecurity requirements for protecting	مراجعة هذه السياسة ومتطلبات الأمن السيبراني لحماية
102	Translated (0%)	<606>external web applications annually</606>.	تطبيقات الويب الخارجية سنويًا<606>606/>.
103	Translated (0%)	Access Requirements for Web Applications:	متطلبات الوصول لتطبيقات الويب:
104	Translated (0%)	The Cybersecurity Department shall ensure that Multi-Factor Authentication is used for user logins on Al Hammadi's<621> </621>external web applications.	يجب على إدارة الأمن السيبراني التأكد من استخدام المصادقة متعددة العوامل لتسجيلات دخول المستخدمين على تطبيقات الويب<621> <621/>الخارجية للحمادي.
105	Translated (0%)	The Cybersecurity Department must document and approve security standards for developing web applications, including, as a minimum, Secure Session Management, Authenticity, Lockout, and Timeout.	يجب على إدارة الأمن السيبراني توثيق واعتماد معايير الأمان لتطوير تطبيقات الويب، بما في ذلك، كحد أدنى، إدارة الجلسة الآمنة، والأصالة، والإغلاق، والمهلة.
106	Translated	The Cybersecurity Department shall ensure that the right of access	يجب على إدارة الأمن السيبراني التأكد من أن حق الوصول إلى أنظمة التشغيل

	(0%)	to operating systems is in accordance with the functional responsibilities of those responsible for web applications.	.يتوافق مع المسؤوليات الوظيفية للمسؤولين عن تطبيقات الويب
107	Translated (0%)	Requirements for Developing or Purchasing Web Applications:	:متطلبات تطوير أو شراء تطبيقات الويب
108	Translated (0%)	The Cybersecurity Department shall conduct a cybersecurity risk assessment when planning to develop or purchase web applications and before launching them into the Production Environment, in accordance with the Al Hammadi's approved Cybersecurity Department policies.	يجب على إدارة الأمن السيبراني إجراء تقييم لمخاطر الأمن السيبراني عند التخطيط لتطوير أو شراء تطبيقات الويب وقبل إطلاقها في بيئة الإنتاج، وفقًا .لسياسات إدارة الأمن السيبراني المعتمدة من الحمادي
109	Translated (0%)	The Cybersecurity Department shall ensure that suppliers comply with cybersecurity policies and standards when purchasing web applications from a third party.	يجب على إدارة الأمن السيبراني التأكد من امتثال الموردين لسياسات ومعايير .الأمن السيبراني عند شراء تطبيقات الويب من طرف ثالث
110	Translated (0%)	The Information Technology Department must obtain prior permission from the Cybersecurity Department before using protected information in the testing environment and use strict controls to protect that data, such as data scrambling techniques, data masking techniques, and deleting it immediately after use.	يجب على إدارة تقنية المعلومات الحصول على إذن مسبق من إدارة الأمن السيبراني قبل استخدام المعلومات المحمية في بيئة الاختبار واستخدام ضوابط صارمة لحماية تلك البيانات، مثل تقنيات تشويش البيانات وتقنيات إخفاء البيانات .وحذفها فورًا بعد الاستخدام
111	Translated (0%)	The General Department of Computer and Information Technology, in cooperation with the Cybersecurity Department, must save the source code in a secure manner and restrict access to Authorized Persons only.	يجب على الإدارة العامة للحاسب الآلي وتقنية المعلومات بالتعاون مع إدارة الأمن السيبراني حفظ الشفرة المصدرية بطريقة آمنة وتقييد الوصول إلى الأشخاص .المصرح لهم فقط
112	Translated (0%)	Penetration testing of the external web application shall be performed in the Testing Environment, while documenting the results and ensuring that all vulnerabilities are addressed before the application is released on the Production Environment.	يجب إجراء اختبار الاختراق لتطبيق الويب الخارجي في بيئة الاختبار، مع توثيق النتائج والتأكد من معالجة جميع نقاط الضعف قبل إصدار التطبيق في بيئة .الإنتاج
113	Translated (0%)	The Cybersecurity Department shall perform a vulnerability scan of the technical components of web applications and ensure that they are addressed by installing Al Hammadi's approved updates and fixed packages.	يجب على إدارة الأمن السيبراني إجراء مسح للثغرات الأمنية للمكونات الفنية لتطبيقات الويب والتأكد من معالجتها من خلال تثبيت تحديثات الحمادي .المعتمدة والحزم الثابتة
114	Translated (0%)	The Cybersecurity Department must approve web applications by the Cybersecurity Steering Committee before they are released into the Environment.	يجب على إدارة الأمن السيبراني الموافقة على تطبيقات الويب من قبل اللجنة .التوجيهية للأمن السيبراني قبل إطلاقها في البيئة
115	Translated (0%)	Cybersecurity Requirements for Protecting Web Applications of Critical Systems	متطلبات الأمن السيبراني لحماية تطبيقات الويب للأنظمة الحرجة
116	Translated (0%)	The Cybersecurity Department must ensure that Secure Session Management, including Authenticity, Lockout, and Timeout, is implemented on all web applications of Al Hammadi ‘s critical systems, provided that they are with more secure settings than non-critical System settings.	يجب على إدارة الأمن السيبراني التأكد من تنفيذ إدارة الجلسة الآمنة، بما في ذلك ،المصادقة والقفل والمهلة، على جميع تطبيقات الويب لأنظمة الحمادي الحرجة .شريطة أن تكون مع إعدادات أكثر أمانًا من إعدادات النظام غير الحرجة

117	Translated (0%)	The principle of Multi-tier Architecture must be used, provided that the number of tires is not less than (3-tier architecture).	يجب استخدام مبدأ العمارة متعددة المستويات، على ألا يقل عدد الإطارات عن (مستويات عمارة 3).
118	Translated (0%)	Cloud Computing Requirements:	متطلبات الحوسبة السحابية:
119	Translated (0%)	The Cybersecurity Department shall ensure that the Identity and Access Management controls are applied to all accounts that have access to web applications on cloud services.	يجب على إدارة الأمن السيبراني التأكد من تطبيق ضوابط إدارة الهوية والوصول على جميع الحسابات التي يمكنها الوصول إلى تطبيقات الويب على الخدمات السحابية.
120	Translated (0%)	The Cybersecurity Department shall ensure that information used by web applications is protected from potential risks, such as:	يجب على إدارة الأمن السيبراني التأكد من حماية المعلومات التي تستخدمها تطبيقات الويب من المخاطر المحتملة، مثل:
121	Translated (0%)	Transmission Incomplete, Misrouting, Unauthorized Modification, Unauthorized Access.	الإرسال غير مكتمل، خطأ في التوجيه، تعديل غير مصرح به، وصول غير مصرح به.
122	Translated (100%)	Compliance and Adherence	الامتثال والالتزام
123	Translated (100%)	Al Hammadi Holding CEO shall ensure compliance with the cybersecurity policies and standards.	يضمن الرئيس التنفيذي لشركة الحمادي القابضة الامتثال لسياسات ومعايير الأمن السيبراني.
124	Translated (100%)	To ensure compliance, the Cybersecurity department will establish regular reporting by the Cybersecurity Manager, conduct periodic audits, or form a Cybersecurity Committee for oversight.	لضمان الامتثال، سينشئ قسم الأمن السيبراني نظامًا لتقديم تقارير منتظمة يُعدّها مدير الأمن السيبراني، ويجري عمليات تدقيق دورية، أو يشكل لجنة للأمن السيبراني للإشراف.
125	Translated (100%)	The CS manager shall ensure adherence to this policy.	يتعين على مدير الأمن السيبراني ضمان الالتزام بهذه السياسة.
126	Translated (100%)	All employees of Al Hammadi Holding must adhere to this policy.	على جميع موظفي شركة الحمادي القابضة الالتزام بهذه السياسة.
127	Translated (100%)	Violations of this policy may result in legal action in any jurisdiction or other measures as deemed appropriate by the Al Hammadi Holding.	قد تؤدي انتهاكات هذه السياسة إلى اتخاذ إجراءات قانونية في أي ولاية قضائية أو غيرها من التدابير التي تراها شركة الحمادي القابضة مناسبة.
128	Translated (100%)	Exceptions	الاستثناءات
129	Translated (100%)	Violation of cybersecurity policies and standards is prohibited unless a prior justified exception is obtained from the Cybersecurity Department or the Cybersecurity Steering Committee.	يُحظر انتهاك سياسات ومعايير الأمن السيبراني ما لم يتم الحصول على استثناء مبرر مسبق من إدارة الأمن السيبراني أو اللجنة التوجيهية للأمن السيبراني.
130	Translated (100%)	In case of a conflict, applicable legislative and regulatory requirements overrule Al Hammadi Holding policies and standards.	في حالة وجود تعارض، فإن المتطلبات التشريعية والتنظيمية المعمول بها تسود على سياسات ومعايير شركة الحمادي القابضة.
131	Translated (100%)	Revision	المراجعة
132	Translated (100%)	This policy is reviewed annually, after major changes in Al Hammadi Holding's organizational chart or infrastructure, and more frequently whenever required, to ensure it remains	تخضع هذه السياسة لمراجعة سنوية، ولإعادة التقييم بعد أي تغييرات جوهرية في الهيكل التنظيمي أو البنية التحتية لشركة الحمادي القابضة، إضافة إلى مراجعات دورية إضافية عند الضرورة، وذلك لضمان توافقها المستمر مع

		appropriate and current for Al Hammadi Holding, ISO 27001, and NCA requirements.	وإرشادات ISO 27001:2022، متطلبات شركة الحمادي القابضة، ومعيار آيزو الهيئة الوطنية للأمن السيبراني.
133	Translated (100%)	Approval Section	قسم الاعتماد
134	Translated (100%)	Prepared by:	إعداد:
135	Translated (100%)	Mr. Mohammed Alamer	السيد/ محمد العامر
136	Translated (100%)	GRC Cybersecurity Specialist	أخصائي حوكمة ومخاطر وامتثال في الأمن السيبراني
137	Translated (100%)	Name	الاسم
138	Translated (100%)	Designation	المسمى الوظيفي
139	Translated (100%)	Signature	التوقيع
140	Translated (100%)	Date	التاريخ
141	Translated (100%)	Reviewed by:	راجعها:
142	Translated (100%)	Ms. Mashael Alotaibi	السيدة/ مشاعل العتيبي
143	Translated (100%)	Cybersecurity Manager	مدير الأمن السيبراني
144	Translated (100%)	Name	الاسم
145	Translated (100%)	Designation	المسمى الوظيفي
146	Translated (100%)	Signature	التوقيع
147	Translated (100%)	Date	التاريخ
148	Translated (100%)	Reviewed by:	راجعها:
149	Translated (100%)	Mr. Deepak Dasan	السيد/ ديباك داسان
150	Translated (100%)	IT Manager	مدير تكنولوجيا المعلومات
151	Translated	Name	الاسم

	(100%)		
152	Translated (100%)	Designation	المسمى الوظيفي
153	Translated (100%)	Signature	التوقيع
154	Translated (100%)	Date	التاريخ
155	Translated (100%)	Approved by:	اعتمدها:
156	Translated (100%)	Dr. Abdulaziz Al Hammadi	الحمادي<Bold><Bold></Bold></Bold> د./ عبد العزيز<Bold><Bold> <Bold><Bold></Bold></Bold>
157	Translated (100%)	Chief Operating Officer	الرئيس التنفيذي للعمليات
158	Translated (100%)	Name	الاسم
159	Translated (100%)	Designation	المسمى الوظيفي
160	Translated (100%)	Signature	التوقيع
161	Translated (100%)	Date	التاريخ
162	Translated (100%)	Approved by:	اعتمدها:
163	Translated (100%)	Mr. Mohammad AlHammadi	السيد/ محمد الحمادي
164	Translated (100%)	Chief Executive Officer	الرئيس التنفيذي
165	Translated (100%)	Name	الاسم
166	Translated (100%)	Designation	المسمى الوظيفي
167	Translated (100%)	Signature	التوقيع
168	Translated (100%)	Date	التاريخ

Segment ID	Segment status	Source segment	Target segment
1	Translated (0%)	<3/> Operation Technology Cybersecurity Policy<7/><11/>	<11></7>العمليات </3> لتكنولوجيا السيبراني الأمن سياسة</>
2	Translated (100%)	Page <25><16/> of <24/></25>	<صفحة <25></16> من <24/></25>
3	Translated (100%)	Al Hammadi Holding	شركة الحمادي القابضة
4	Translated (0%)	Operation Technology Cybersecurity Policy	سياسة الأمن السيبراني لتكنولوجيا العمليات
5	Translated (100%)	CYBERSECURITY DEPARTMENT	إدارة الأمن السيبراني
6	Translated (100%)	Policy ID	معرّف السياسة
7	Translated (100%)	AHH-CS-ISMS-005	AHH-CS-ISMS-005
8	Translated (100%)	Class	الفئة
9	Translated (100%)	Internal Release	إصدار داخلي
10	Not Translated (0%)		
11	Translated (100%)	V0.1	V0.1
12	Translated (100%)	Published at	نُشرت في
13	Translated (100%)	April 2025	أبريل 2025
14	Translated (100%)	Document Owner	المسؤول عن المستند
15	Translated (100%)	Cybersecurity <110>Department</110>	إدارة<110/> الأمن السيبراني<110>
16	Translated (100%)	Disclaimer	تنويه
17	Translated (100%)	The information contained in this document is the property of Hammadi Holding and must not be copied or communicated to a third party or used for any purpose other than that for which it is supplied, without the written consent of Al Hammadi Holding.	المعلومات الواردة في هذا المستند هي ملك لشركة الحمادي القابضة ولا يجوز نسخها أو إبلاغها إلى طرف ثالث أو استخدامها لأي غرض آخر غير الغرض الذي تم توفيرها من أجله، دون موافقة خطية من شركة الحمادي القابضة.

18	Translated (100%)	Contents	جدول المحتويات
19	Translated (100%)	Document Control	ضبط المستندات
20	Translated (100%)	Document Information	معلومات المستند
21	Translated (100%)	Synopsis	الملخص
22	Translated (100%)	Document Title:	:عنوان المستند
23	Translated (100%)	Operation Technology Cybersecurity Policy	سياسة الأمن السيبراني لتكنولوجيا العمليات
24	Translated (100%)	Document Status:	:حالة المستند
25	Translated (100%)	Approved	معتمد
26	Translated (100%)	Document Effective Date:	:تاريخ سريان المستند
27	Translated (100%)	April 2025	أبريل 2025
28	Translated (100%)	Document Issue Date:	:تاريخ إصدار المستند
29	Translated (100%)	April 2025	أبريل 2025
30	Translated (100%)	Document Next Review Date:	:تاريخ المراجعة التالية للمستند
31	Translated (100%)	April <221>2026</221>	<أبريل <221>2026<221/>
32	Translated (100%)	Key contacts	جهات التواصل الرئيسية
33	Translated (100%)	Document Owner:	:المسؤول عن المستند
34	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
35	Translated (100%)	Approval Authority	جهة الاعتماد
36	Translated (100%)	Document Created by:	:مُنشئ المستند
37	Translated	Cybersecurity Department	إدارة الأمن السيبراني

	(100%)		
38	Translated (100%)	Document Reviewed by:	:راجع المستند
39	Translated (100%)	Al Hammadi Holding CS Manager	مدير الأمن السيبراني في شركة الحمادي القابضة
40	Translated (100%)	Document Approved by:	:اعتمد المستند
41	Translated (100%)	Al Hammadi Holding COO & CEO	الرئيس التنفيذي للعمليات والرئيس التنفيذي في شركة الحمادي القابضة
42	Translated (100%)	Note:	:ملاحظة
43	Translated (100%)	Any additional approval will be added in the document annex	تُضاف أي اعتمادات إضافية في ملحق المستند
44	Translated (100%)	Classification	التصنيف
45	Translated (100%)	<302>Company Internal</302> – to be shared with 3rd parties after consent of CS Manager	داخلي لاستخدام للشركة – <302/>يُسمح بمشاركته مع جهات<302> خارجية بعد موافقة مدير إدارة الأمن السيبراني
46	Translated (100%)	Version / Dates	الإصدار / التواريخ
47	Translated (100%)	Current Version:	:الإصدار الحالي
48	Translated (100%)	V 1.0	V 1.0
49	Translated (100%)	Date Published:	:تاريخ النشر
50	Translated (100%)	April 2025	أبريل 2025
51	Translated (100%)	Date of Next Review:	:تاريخ المراجعة التالية
52	Translated (100%)	April 2026	أبريل 2026
53	Translated (100%)	Document Changes	التغييرات على المستند
54	Translated (100%)	Date	التاريخ
55	Translated (100%)	Version	الإصدار
56	Translated (100%)	Document Owner	المسؤول عن المستند

57	Translated (100%)	Change Description	وصف التغيير
58	Translated (100%)	April <365>2025</365>	<365>أبريل <365/>2025
59	Translated (100%)	1.0	1.0
60	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
61	Translated (100%)	Document Established	تم إنشاء المستند
62	Translated (100%)	Document Circulation	تعميم المستند
63	Translated (100%)	To	إلى
64	Translated (100%)	Date	التاريخ
65	Translated (100%)	Method	الطريقة
66	Translated (100%)	IT Staff	موظفو تكنولوجيا المعلومات
67	Translated (100%)	April 2025	أبريل 2025
68	Translated (100%)	Intranet Portal	بوابة الإنترانت
69	Translated (100%)	All Al Hammadi Staff	جميع موظفي شركة الحمادي
70	Translated (100%)	April 2025	أبريل 2025
71	Translated (100%)	Intranet Portal	بوابة الإنترانت
72	Translated (100%)	Objectives	الأهداف
73	Translated (0%)	<426>The</426> objective of this Policy is to ensure the protection of operational technology devices and systems and reduce the chances of their misuse or damage, and to respond to the cybersecurity requirements issued by the National Cybersecurity Authority regarding the protection of Operational Technology devices and systems.	الهدف<426/> من هذه السياسة هو ضمان حماية أجهزة وأنظمة<426> التكنولوجيا التشغيلية وتقليل فرص إساءة استخدامها أو إتلافها، والاستجابة لمتطلبات الأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني فيما يتعلق بحماية أجهزة وأنظمة التكنولوجيا التشغيلية.
74	Translated (100%)	Key Outcomes of Implementing the Principles and Procedural	النتائج الرئيسية لتنفيذ المبادئ والإجراءات

75	Translated (0%)	This Policy adheres to the national legislative and regulatory requirements.	.تلتزم هذه السياسة بالمتطلبات التشريعية والتنظيمية الوطنية
76	Translated (0%)	It is a legislative requirement as mentioned in Operational Technology Cybersecurity	إنه مطلب تشريعي كما هو مذكور في الأمن السيبراني للتكنولوجيا التشغيلية
77	Translated (0%)	Controls (OTCC -1:	:OTCC -1) الضوابط
78	Translated (0%)	2022) (issued by the National Cybersecurity Authority.	.صادر عن الهيئة الوطنية للأمن السيبراني) (2022
79	Translated (0%)	Compliance with the cybersecurity requirements of the controls of Operational Technology devices and systems issued by the National Cybersecurity Authority.	الالتزام بمتطلبات الأمن السيبراني لضوابط أجهزة وأنظمة التكنولوجيا .التشغيلية الصادرة عن الهيئة الوطنية للأمن السيبراني
80	Translated (0%)	Protecting Al Hammadi's Operational Technology control environment devices and systems.	.حماية أجهزة وأنظمة بيئة التحكم في التكنولوجيا التشغيلية في الحمادي
81	Translated (0%)	Reducing cyber risks related to the Operational Technology environment.	.الحد من المخاطر السيبرانية المتعلقة ببيئة التكنولوجيا التشغيلية
82	Translated (100%)	Scope	النطاق
83	Translated (0%)	This policy applies to all Al Hammadi Holding Operational Technology, assets, and activities, including employees, contractors, suppliers, and third parties under its control.	تنطبق هذه السياسة على جميع التقنيات والأصول والأنشطة التشغيلية لشركة الحمادي القابضة، بما في ذلك الموظفين والمقاولين والموردين .والأطراف الثالثة الخاضعة لسيطرتها
84	Translated (0%)	It covers all IT systems, information assets, and operational risks relevant to ensuring patient safety, employee well-being, compliance with legal standards, and operational continuity.	تغطي السياسة جميع أنظمة تكنولوجيا المعلومات وأصول المعلومات والمخاطر التشغيلية ذات الصلة بضمان سلامة المرضى ورفاهية .الموظفين والامتثال للمعايير القانونية واستمرارية التشغيل
85	Translated (100%)	Roles and Responsibilities	الأدوار والمسؤوليات
86	Translated (100%)	Al Hammadi Holding management is responsible for implementing, maintaining, and updating this policy with all its contents, in accordance with any changes in the Statement of Applicability, Al Hammadi Holding-SOA Document.	تتحمل إدارة شركة الحمادي القابضة مسؤولية تنفيذ هذه السياسة وحفظها وتحديثها بكامل محتوياتها، وذلك بما يتماشى مع أي تغييرات في .بيان التطبيق الخاص بشركة الحمادي القابضة
87	Translated (100%)	Principles	المبادئ
88	Translated (0%)	Cybersecurity Risk Management Controls for Operational Technology Systems	ضوابط إدارة مخاطر الأمن السيبراني لأنظمة التكنولوجيا التشغيلية
89	Translated (0%)	The Cybersecurity Department shall establish an Operational Technology Systems (OT/ICS) Cybersecurity Risk Management Methodology within Al Hammadi 's Risk Management and Safety Risk Management Methodology and Procedures.	يجب على إدارة الأمن السيبراني وضع منهجية لإدارة مخاطر الأمن ضمن منهجية (OT/ICS) السيبراني لأنظمة التكنولوجيا التشغيلية .وإجراءات إدارة المخاطر والسلامة في الحمادي
90	Translated (0%)	The Cybersecurity Department must annually assess the cybersecurity risks of Operational Technology Systems, making sure to include the risks	يجب على إدارة الأمن السيبراني تقييم مخاطر الأمن السيبراني لأنظمة التكنولوجيا التشغيلية سنويًا، مع التأكد من تضمين مخاطر توقيع العقود

		of signing contracts and agreements with third parties related to Operational Technology Systems, or when changes occur in relevant legislative and regulatory requirements as part of the assessment.	والاتفاقيات مع أطراف ثالثة تتعلق بأنظمة التكنولوجيا التشغيلية، أو عند حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات الصلة كجزء من التقييم.
91	Translated (0%)	The Cybersecurity Department shall establish a register of cybersecurity risks related to Operational Technology Systems.	يجب على إدارة الأمن السيبراني إنشاء سجل لمخاطر الأمن السيبراني المتعلقة بأنظمة التكنولوجيا التشغيلية.
92	Translated (0%)	In the event that it is not possible to meet the cybersecurity requirements within the environment of Operational Technology Systems, the concerned department or division must clarify the necessary justifications, with documentation and approval by the Cybersecurity Department, and the approval of the Cybersecurity Steering Committee and the Authorized Person.	في حالة تعذر تلبية متطلبات الأمن السيبراني ضمن بيئة أنظمة التقنية التشغيلية، يجب على الإدارة أو القسم المعني توضيح المبررات اللازمة، مع التوثيق والموافقة من قبل إدارة الأمن السيبراني، وموافقة اللجنة التوجيهية للأمن السيبراني والشخص المفوض.
93	Translated (0%)	In the event that it is approved to accept cyber risks, alternative controls must be identified, documented and approved by the Cybersecurity Steering Committee and the Authorized Person.	في حالة الموافقة على قبول المخاطر السيبرانية، يجب تحديد الضوابط البديلة وتوثيقها والموافقة عليها من قبل اللجنة التوجيهية للأمن السيبراني والشخص المفوض.
94	Translated (0%)	The Cybersecurity Department shall ensure that alternative controls are applied effectively at a specified time while continuing to assess and review those risks on an ongoing basis.	يجب على إدارة الأمن السيبراني التأكد من تطبيق الضوابط البديلة بفعالية في وقت محدد مع الاستمرار في تقييم ومراجعة تلك المخاطر بشكل مستمر.
95	Translated (0%)	The Cybersecurity Department must activate the use of Multi-Authentication Factor technologies for the access of users with important and sensitive powers on the OT Systems and devices of Al Hammadi.	يجب على إدارة الأمن السيبراني تفعيل استخدام تقنيات عوامل المصادقة المتعددة للوصول إلى المستخدمين ذوي الصلاحيات المهمة والحساسة على أنظمة تكنولوجيا التشغيل وأجهزة الحمادي.
96	Translated (0%)	The Cybersecurity Department must activate event logs for cybersecurity on Operational technology Systems technical infrastructure networks, and associated communications on the network.	يجب على إدارة الأمن السيبراني تفعيل سجلات الأحداث للأمن السيبراني، على شبكات البنية التحتية التقنية لأنظمة التكنولوجيا التشغيلية والاتصالات المرتبطة بها على الشبكة.
97	Translated (0%)	These logs shall be monitored and checked on an ongoing basis.	يجب مراقبة هذه السجلات وفحصها بشكل مستمر.
98	Translated (0%)	The Cybersecurity Department shall provide the necessary malware protection technologies for Operational Technology to control environmental systems and devices and adjust their settings according to the best security standards.	يجب على إدارة الأمن السيبراني توفير تقنيات الحماية من البرامج الضارة اللازمة للتكنولوجيا التشغيلية للتحكم في الأنظمة والأجهزة البيئية وضبط إعداداتها وفقًا لأفضل المعايير الأمنية.
99	Translated (0%)	The Cybersecurity Department should ensure that OT system network settings, such as proxy servers, firewalls, and data diodes, are set to prevent unauthorized data transfer.	يجب على إدارة الأمن السيبراني التأكد من تعيين إعدادات شبكة نظام OT، مثل الخوادم الوكيلة وجدران الحماية وصمامات البيانات، لمنع نقل البيانات غير المصرح به.
100	Translated (0%)	The Cybersecurity Department shall adjust the settings of components of web-based OT Systems, as follows:	يجب على إدارة الأمن السيبراني ضبط إعدادات مكونات أنظمة التكنولوجيا التشغيلية المستندة إلى الويب، على النحو التالي:
101	Translated (0%)	Using HTTPS for authorized devices only.	استخدام HTTPS للأجهزة المصرح بها فقط.
102	Translated (0%)	Defining and assigning a specific list of applications (Whitelisting) to<738> </738>access web services.	<تحديد وتعيين قائمة محددة من التطبيقات (القائمة البيضاء)738> </738>للوصول إلى خدمات الويب.

103	Translated (0%)	Using Web Application Firewall (WAF) to protect against web attacks on external OT Systems.	للحماية من هجمات الويب (WAF) استخدام جدار حماية تطبيق الويب الخارجية OT على أنظمة.
104	Translated (100%)	Procedural Guidelines	المبادئ التوجيهية الإجرائية
105	Translated (0%)	Cybersecurity procedures for Operational Technology	إجراءات الأمن السيبراني للتكنولوجيا التشغيلية
106	Translated (100%)	The Cybersecurity Department shall adhere to the following procedures:	:تلتزم إدارة الأمن السيبراني بالإجراءات التالية
107	Translated (0%)	Determine the Operational Technology systems in Al Hammadi on which cybersecurity risk assessments must be conducted based on their classification, document the scope of risk assessment work, develop an annual plan for risk assessment, obtain the approval of the Director of the Cybersecurity Department on the plan, and share it with the Cybersecurity Supervisory Committee and relevant parties.	تحديد أنظمة التكنولوجيا التشغيلية في الحمادي التي يجب إجراء تقييمات مخاطر الأمن السيبراني بناءً على تصنيفها، وتوثيق نطاق عمل تقييم المخاطر، ووضع خطة سنوية لتقييم المخاطر، والحصول على موافقة مدير إدارة الأمن السيبراني على الخطة، ومشاركتها مع لجنة الإشراف على الأمن السيبراني والجهات ذات الصلة.
108	Translated (0%)	Assess cybersecurity risks to all of Al Hammadi's operational technology systems based on cybersecurity requirements.	تقييم مخاطر الأمن السيبراني على جميع أنظمة التكنولوجيا التشغيلية في الحمادي بناءً على متطلبات الأمن السيبراني.
109	Translated (100%)	Cybersecurity risk assessment procedures	إجراءات تقييم مخاطر الأمن السيبراني
110	Translated (0%)	Identify events or circumstances that may violate the confidentiality, integrity, and availability of Operational Technology systems, potential threats and related vulnerabilities, and approved controls, and then determine the effects resulting from the loss of confidentiality, integrity, and availability of these assets.	تحديد الأحداث أو الظروف التي قد تنتهك سرية وسلامة وتوافر أنظمة التكنولوجيا التشغيلية والتهديدات المحتملة ونقاط الضعف ذات الصلة والضوابط المعتمدة، ثم تحديد الآثار الناتجة عن فقدان سرية وسلامة وتوافر هذه الأصول.
111	Translated (0%)	Identify the cyber risk response strategy and the controls that will be implemented to reduce the impact or likelihood of the cyber risk occurring in Al Hammadi .	تحديد استراتيجية الاستجابة للمخاطر السيبرانية والضوابط التي سيتم تنفيذها للحد من تأثير أو احتمال حدوث المخاطر السيبرانية في الحمادي .
112	Translated (0%)	Document them in the cybersecurity risk register based on the classification of Al Hammadi ’s business and assets and based on the cybersecurity requirements, share it with the Cybersecurity Steering Committee for approval, and with the relevant parties for implementation and application.	توثيقها في سجل مخاطر الأمن السيبراني بناءً على تصنيف أعمال وأصول الحمادي وبناءً على متطلبات الأمن السيبراني، ومشاركتها مع اللجنة التوجيهية للأمن السيبراني للموافقة عليها، ومع الجهات ذات الصلة للتنفيذ والتطبيق.
113	Translated (100%)	Monitor cybersecurity risks	مراقبة مخاطر الأمن السيبراني
114	Translated (100%)	Review the cybersecurity risk register every Three months and ensure that it is followed up based on cybersecurity requirements and according to business and asset classification.	مراجعة سجل مخاطر الأمن السيبراني كل ثلاثة أشهر والتأكد من متابعته بناءً على متطلبات الأمن السيبراني ووفقًا لتصنيف الأعمال والأصول.
115	Translated (0%)	Test and evaluate remediation plans and applied controls every three months and share reports with the Cybersecurity Steering Committee and relevant parties.	اختبار وتقييم خطط الإصلاح والضوابط المطبقة كل ثلاثة أشهر ومشاركة التقارير مع اللجنة التوجيهية للأمن السيبراني والأطراف ذات الصلة.

116	Translated (0%)	Evaluate the residual risks faced by Al Hammadi for each specific risk every six months, determine whether the risks are within the boundaries of tolerance or acceptability, and share the reports with the Cybersecurity Steering Committee and relevant parties.	تقييم المخاطر المتبقية التي يواجهها الحمادي لكل خطر محدد كل ستة ،أشهر، وتحديد ما إذا كانت المخاطر ضمن حدود التسامح أو القبول ومشاركة التقارير مع اللجنة التوجيهية للأمن السيبراني والأطراف ذات الصلة.
117	Translated (100%)	Compliance and Adherence	الامتثال والالتزام
118	Translated (100%)	Al Hammadi Holding CEO shall ensure compliance with the cybersecurity policies and standards.	يضمن الرئيس التنفيذي لشركة الحمادي القابضة الامتثال لسياسات ومعايير الأمن السيبراني.
119	Translated (100%)	To ensure compliance, the Cybersecurity department will establish regular reporting by the Cybersecurity Manager, conduct periodic audits, or form a Cybersecurity Committee for oversight.	لضمان الامتثال، سينشئ قسم الأمن السيبراني نظامًا لتقديم تقارير منتظمة يُعدّها مدير الأمن السيبراني، ويجري عمليات تدقيق دورية، أو يشكل لجنة للأمن السيبراني للإشراف.
120	Translated (100%)	The CS manager shall ensure adherence to this policy.	يتعين على مدير الأمن السيبراني ضمان الالتزام بهذه السياسة.
121	Translated (100%)	All employees of Al Hammadi Holding must adhere to this policy.	على جميع موظفي شركة الحمادي القابضة الالتزام بهذه السياسة.
122	Translated (100%)	Violations of this policy may result in legal action in any jurisdiction or other measures as deemed appropriate by the Al Hammadi Holding.	قد تؤدي انتهاكات هذه السياسة إلى اتخاذ إجراءات قانونية في أي ولاية قضائية أو غيرها من التدابير التي تراها شركة الحمادي القابضة مناسبة.
123	Translated (100%)	Exceptions	الاستثناءات
124	Translated (100%)	Violation of cybersecurity policies and standards is prohibited unless a prior justified exception is obtained from the Cybersecurity Department or the Cybersecurity Steering Committee.	يُحظر انتهاك سياسات ومعايير الأمن السيبراني ما لم يتم الحصول على استثناء مبرر مسبق من إدارة الأمن السيبراني أو اللجنة التوجيهية للأمن السيبراني.
125	Translated (100%)	In case of a conflict, applicable legislative and regulatory requirements overrule Al Hammadi Holding policies and standards.	في حالة وجود تعارض، فإن المتطلبات التشريعية والتنظيمية المعمول بها تسود على سياسات ومعايير شركة الحمادي القابضة.
126	Translated (100%)	Revision	المراجعة
127	Translated (100%)	This policy is reviewed annually, after major changes in Al Hammadi Holding’s organizational chart or infrastructure, and more frequently whenever required, to ensure it remains appropriate and current for Al Hammadi Holding, ISO 27001, and NCA requirements.	تخضع هذه السياسة لمراجعة سنوية، ولإعادة التقييم بعد أي تغييرات جوهرية في الهيكل التنظيمي أو البنية التحتية لشركة الحمادي القابضة، إضافة إلى مراجعات دورية إضافية عند الضرورة، وذلك لضمان توافقها المستمر مع متطلبات شركة الحمادي القابضة، ومعيار آيزو ISO 27001:2022، وإرشادات الهيئة الوطنية للأمن السيبراني.
128	Translated (100%)	Approval Section	قسم الاعتماد
129	Translated (100%)	Prepared by:	إعداد:
130	Translated (100%)	Mr. Mohammed Alamer	السيد/ محمد العامر
131	Translated (100%)	GRC Cybersecurity Specialist	أخصائي حوكمة ومخاطر وامتثال في الأمن السيبراني

132	Translated (100%)	Name	الاسم
133	Translated (100%)	Designation	المسمى الوظيفي
134	Translated (100%)	Signature	التوقيع
135	Translated (100%)	Date	التاريخ
136	Translated (100%)	Reviewed by:	راجعها:
137	Translated (100%)	Mr. Deepak Dasan	السيد/ ديباك داسان
138	Translated (100%)	IT Manager	مدير تكنولوجيا المعلومات
139	Translated (100%)	Name	الاسم
140	Translated (100%)	Designation	المسمى الوظيفي
141	Translated (100%)	Signature	التوقيع
142	Translated (100%)	Date	التاريخ
143	Translated (100%)	Reviewed by:	راجعها:
144	Translated (100%)	Ms. Mashael Alotaibi	السيدة/ مشاعل العتيبي
145	Translated (100%)	Cybersecurity Manager	مدير الأمن السيبراني
146	Translated (100%)	Name	الاسم
147	Translated (100%)	Designation	المسمى الوظيفي
148	Translated (100%)	Signature	التوقيع
149	Translated (100%)	Date	التاريخ
150	Translated (100%)	Approved by:	اعتمدها:
151	Translated	Dr. Abdulaziz Al Hammadi	الحمادي<Bold><Bold> د./ عبد العزيز</Bold></Bold>

	(100%)		<Bold><Bold></Bold></Bold>
152	Translated (100%)	Chief Operating Officer	الرئيس التنفيذي للعمليات
153	Translated (100%)	Name	الاسم
154	Translated (100%)	Designation	المسمى الوظيفي
155	Translated (100%)	Signature	التوقيع
156	Translated (100%)	Date	التاريخ
157	Translated (100%)	Approved by:	:اعتمدها
158	Translated (100%)	Mr. Mohammad AlHammadi	السيد/ محمد الحمادي
159	Translated (100%)	Chief Executive Officer	الرئيس التنفيذي
160	Translated (100%)	Name	الاسم
161	Translated (100%)	Designation	المسمى الوظيفي
162	Translated (100%)	Signature	التوقيع
163	Translated (100%)	Date	التاريخ

Segment ID	Segment status	Source segment	Target segment
1	Translated (0%)	<3/><7/> <10>Information Security Access Management Policy<17/></10>	<3/><7/> <10>10/></17>سياسة إدارة الوصول إلى أمن المعلومات
2	Translated (100%)	Page <31><22/> of <30/></31>	<31></22> من <30/></31>صفحة
3	Translated (100%)	Al Hammadi Holding	شركة الحمادي القابضة
4	Translated (0%)	<55/>-	<55/>-
5	Translated (0%)	Information Security Access Management Policy	سياسة إدارة الوصول إلى أمن المعلومات
6	Translated (100%)	CYBERSECURITY DEPARTMENT	إدارة الأمن السيبراني
7	Translated (100%)	Policy ID	معرّف السياسة
8	Translated (0%)	AHH-CS-ISMS-006	AHH-CS-ISMS-006
9	Translated (99%)	Class	الفئة
10	Translated (CM)	Internal Release	إصدار داخلي
11	Not Translated (0%)		
12	Translated (100%)	V3.1	V3.1
13	Translated (CM)	Published at	نُشرت في
14	Translated (100%)	April 2025	أبريل 2025
15	Translated (100%)	Document Owner	المسؤول عن المستند
16	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
17	Translated (99%)	Disclaimer	تنويه
18	Translated (96%)	The information contained in this document is the property of Hammadi Holding and must not be copied or communicated to a	المعلومات الواردة في هذا المستند هي ملك لشركة الحمادي القابضة ولا يجوز نسخها أو إبلاغها إلى طرف ثالث أو استخدامها لأي غرض آخر غير الغرض

		third party or used for any purpose other than that for which it is supplied, without the written consent of Al Hammadi Holding.	.الذي تم توفيرها من أجله، دون موافقة خطية من شركة الحمادي القابضة
19	Translated (99%)	Contents	جدول المحتويات
20	Translated (100%)	Document Control	ضبط المستندات
21	Translated (100%)	Document Information	معلومات المستند
22	Translated (100%)	Synopsis	الملخص
23	Translated (100%)	Document Title:	:عنوان المستند
24	Translated (100%)	Information Security Access Management Policy	سياسة إدارة الوصول إلى أمن المعلومات
25	Translated (100%)	Document Status:	:حالة المستند
26	Translated (100%)	Approved	معتمد
27	Translated (100%)	Document Effective Date:	:تاريخ سريان المستند
28	Translated (100%)	December 2024	ديسمبر 2024
29	Translated (100%)	Document Issue Date:	:تاريخ إصدار المستند
30	Translated (99%)	April 2025	أبريل 2025
31	Translated (100%)	Document Next Revision Date:	:تاريخ المراجعة التالية للمستند
32	Translated (100%)	April 2026	أبريل 2026
33	Translated (100%)	Key contacts	جهات التواصل الرئيسية
34	Translated (100%)	Document Owner:	:المسؤول عن المستند
35	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
36	Translated (100%)	Approval Authority	جهة الاعتماد
37	Translated	Document Created by:	:مُنشئ المستند

	(100%)		
38	Translated (100%)	IT Management	إدارة تكنولوجيا المعلومات
39	Translated (100%)	Document Reviewed by:	راجع المستند:
40	Translated (87%)	Al Hammadi Holding CS &IT Managers	مديرو الأمن السيبراني وتكنولوجيا المعلومات في شركة الحمادي القابضة
41	Translated (100%)	Document Approved by:	اعتمد المستند:
42	Translated (100%)	Al Hammadi Holding COO & CEO	الرئيس التنفيذي للعمليات والرئيس التنفيذي في شركة الحمادي القابضة
43	Translated (100%)	Note:	ملاحظة:
44	Translated (100%)	Any additional approval will be added in the document annex	تُضاف أي اعتمادات إضافية في ملحق المستند
45	Translated (100%)	Classification	التصنيف
46	Translated (99%)	<387>Company Internal – </387>to be shared with 3rd parties after consent of CS Manager	داخلي لاستخدام للشركة<387> – </387></387>يُسمح بمشاركته<387> مع جهات خارجية بعد موافقة مدير إدارة الأمن السيبراني
47	Translated (100%)	Version / Dates	الإصدار / التواريخ
48	Translated (0%)	<408>Current Version</408>:	<408>الإصدار الحالي</408>:
49	Translated (100%)	V 3.1	V 3.1
50	Translated (100%)	Date Published:	تاريخ النشر:
51	Translated (100%)	April 2025	أبريل 2025
52	Translated (0%)	<423>Date of Next Review</423>:	<423>تاريخ المراجعة التالية</423>:
53	Translated (100%)	April 2026	أبريل 2026
54	Translated (0%)	<432>Prior Version</432>:	<432>الإصدار السابق</432>:
55	Translated (100%)	V 3.0	V 3.0
56	Translated (100%)	Prior Published:	تاريخ النشر السابق:

57	Translated (100%)	December 2023	ديسمبر 2023
58	Translated (100%)	Document Changes	التغييرات على المستند
59	Translated (100%)	Date	التاريخ
60	Translated (100%)	Version	الإصدار
61	Translated (100%)	Document Owner	المسؤول عن المستند
62	Translated (100%)	Change Description	وصف التغيير
63	Translated (100%)	December 2024	ديسمبر 2024
64	Translated (100%)	3.0	3.0
65	Translated (100%)	IT Management	إدارة تكنولوجيا المعلومات
66	Translated (0%)	Updated policy number to AHH-IT-ISMS-006	AHH-IT-ISMS-006 تحديث رقم السياسة إلى
67	Translated (100%)	April 2025	أبريل 2025
68	Translated (100%)	3.1	3.1
69	Translated (0%)	<507><505>Cybersecurity </505></507><510>Department</510>	<510>507/><505/>الأمن السيبراني <505><507><510/>إدارة<
70	Translated (100%)	Document reviewed and updated based on NCA ECC-2:2024 and ISO27001:2022 requirements	تمت مراجعة المستند وتحديثه استنادًا إلى متطلبات الهيئة الوطنية للأمن السيبراني (NCA) المعيار ECC-2:2024 ومعيار آيزو ISO 27001:2022.
71	Translated (100%)	Document Circulation	تعميم المستند
72	Translated (100%)	To	إلى
73	Translated (100%)	Date	التاريخ
74	Translated (100%)	Method	الطريقة
75	Translated (100%)	IT Staff	موظفو تكنولوجيا المعلومات
76	Translated	April 2025	أبريل 2025

	(100%)		
77	Translated (100%)	Intranet Portal	بوابة الإنترانت
78	Translated (0%)	All Al Hammadi Staff	جميع موظفي شركة الحمادي
79	Translated (100%)	April 2025	أبريل 2025
80	Translated (100%)	Intranet Portal	بوابة الإنترانت
81	Translated (100%)	Objectives	الأهداف
82	Translated (0%)	The purpose of this policy is to set the principles and procedural implementation by which Al Hammadi Holding shall protect its critical information assets by limiting and controlling access to only Al Hammadi Holding authorized users to ensure confidentiality and integrity, in compliance with the requirements specified in	الغرض من هذه السياسة هو وضع المبادئ والتنفيذ الإجرائي الذي يجب على شركة الحمادي القابضة من خلاله حماية أصول المعلومات الهامة الخاصة بها عن طريق الحد من الوصول والتحكم فيه فقط للمستخدمين المصرح لهم من شركة الحمادي القابضة لضمان السرية والنزاهة، وفقًا للمتطلبات المحددة في
83	Translated (84%)	ISO/IEC 27001:2022 Annex-A:	:الملحق أ IEC 27001:2022/معيار آيزو
84	Translated (0%)	A.5.15 Access Control, A.5.16 Identity Management, A.5.17 Authentication information, A.5.18 Access rights, A.8.2 Privileged access rights, A.8.3 Information access restriction, A.8.4 Access to source code, A.8.5 Secure authentication	،أ .5.15 التحكم في الوصول، أ .5.16 إدارة الهوية، أ .5.17 معلومات المصادقة أ .5.18 حقوق الوصول، أ .8.2 حقوق الوصول المميزة، أ .8.3 تقييد الوصول إلى المعلومات، أ .8.4 الوصول إلى الكود المصدري، أ .8.5 المصادقة الآمنة
85	Translated (100%)	NCA ECC-2:2024:	:ECC-2:2024 معيار الهيئة الوطنية للأمن السيبراني رقم
86	Translated (0%)	2-2 Identity and Access Management	إدارة الهوية والوصول 2-2
87	Translated (100%)	Scope	النطاق
88	Translated (0%)	This policy is applicable to all Al Hammadi Holding ISMS information assets, security operations, and all persons doing work under Al Hammadi Holding control.	تنطبق هذه السياسة على جميع أصول معلومات نظام إدارة أمن المعلومات في شركة الحمادي القابضة والعمليات الأمنية وجميع الأشخاص الذين يعملون .تحت إشراف شركة الحمادي القابضة
89	Translated (92%)	This includes employees, contractors, suppliers, and 3rd Parties.	.وتشمل السياسة الموظفين والمتعاقدين والموردين والجهات الخارجية
90	Translated (100%)	Roles and Responsibilities	الأدوار والمسؤوليات
91	Translated (100%)	Al Hammadi Holding Cybersecurity and IT Departments are responsible for maintaining this policy with all its contents, in accordance with any changes in the applicable regulations and legislation, where:	تتولى إدارات الأمن السيبراني وتكنولوجيا المعلومات في شركة الحمادي القابضة مسؤولية حفظ هذه السياسة بجميع محتوياتها، وفقًا لأي تغييرات :تطرأ على اللوائح والتشريعات المعمول بها، وذلك وفقًا لما يلي

92	Translated (100%)	Policy Review and Update:	:مراجعة السياسة وتحديثها
93	Translated (100%)	Cybersecurity Department.	.إدارة الأمن السيبراني
94	Translated (100%)	Policy Implementation and Enforcement:	:تنفيذ السياسة وإنفاذها
95	Translated (100%)	IT Department.	.إدارة تكنولوجيا المعلومات
96	Translated (100%)	Policy Compliance Measurement:	:قياس الامتثال للسياسة
97	Translated (100%)	Cybersecurity Department.	.إدارة الأمن السيبراني
98	Translated (100%)	Principles	المبادئ
99	Translated (0%)	Al Hammadi Holding only authorized users must gain access to resources.	يجب على المستخدمين المصرح لهم فقط من شركة الحمادي القابضة الوصول .إلى الموارد
100	Translated (0%)	Unauthorized users shall be prevented from accessing systems and services	يُمنع المستخدمون غير المصرح لهم من الوصول إلى الأنظمة والخدمات
101	Translated (100%)	Access Control	التحكم في إمكانية الوصول
102	Translated (0%)	All users and systems shall be uniquely identified through managed digital identities.	يجب تحديد جميع المستخدمين والأنظمة بشكل فريد من خلال الهويات .الرقمية المدارة
103	Translated (0%)	Access to Al Hammadi Holding information shall be controlled based on business and security requirements and rules defined for each information system.	يجب التحكم في الوصول إلى معلومات شركة الحمادي القابضة بناءً على .متطلبات وقواعد العمل والأمن المحددة لكل نظام معلومات
104	Translated (0%)	These rules shall consider the following:	:يراعى في هذه القواعد ما يأتي
105	Translated (0%)	Security requirements of the business application(s).	.متطلبات الأمان لتطبيق(تطبيقات) الأعمال
106	Translated (0%)	An identified business requirement for the user to have access to the information or business process (‘need to know’ principle).	متطلب عمل محدد للمستخدم للوصول إلى المعلومات أو العملية التجارية .(" مبدأ "الحاجة إلى المعرفة)
107	Translated (0%)	All access is denied unless specifically approved under the provisions of this policy.	يتم رفض كل الوصول ما لم تتم الموافقة عليه على وجه التحديد بموجب أحكام .هذه السياسة
108	Translated (0%)	Legal and/or contractual obligation to restrict and protect access to information systems.	.الالتزام القانوني و/أو التعاقدي بتقييد وحماية الوصول إلى أنظمة المعلومات
109	Translated (0%)	Al Hammadi Holding Asset owners shall determine appropriate access control rules, access rights, and restrictions for specific user roles.	يجب على مسؤولي إدارة أصول الحمادي القابضة تحديد قواعد التحكم في .الوصول المناسبة وحقوق الوصول والقيود الخاصة بأدوار المستخدم المحددة
110	Translated	Al Hammadi Holding shall consider the segregation of access control	يجب على شركة الحمادي القابضة النظر في الفصل بين أدوار التحكم في

	(0%)	roles, e.g., access request, access authorization, access administration.	.الوصول، على سبيل المثال، طلب الوصول، وتصريح الوصول، وإدارة الوصول
111	Translated (0%)	Access control granting shall be based on the requirements for formal authorization of access requests.	يجب أن يستند منح التحكم في الوصول إلى متطلبات الترخيص الرسمي .لطلبات الوصول
112	Translated (0%)	Al Hammadi Holding logical and physical access controls shall be considered together.	يجب النظر في ضوابط الوصول المنطقية والمادية لشركة الحمادي القابضة .معًا
113	Translated (0%)	Al Hammadi Holding Users and service providers shall be given a clear statement of the business requirements to be met by access controls.	يجب إعطاء مستخدمي شركة الحمادي القابضة ومقدمي الخدمات بيانًا واضحًا .بمتطلبات العمل التي يجب الوفاء بها من خلال ضوابط الوصول
114	Translated (0%)	Access for contractors, consultants or third-party personnel to Al Hammadi Holding's information assets shall be provided only based on a contractual agreement.	يجب توفير الوصول للمقاولين أو الاستشاريين أو موظفي الطرف الثالث إلى .أصول معلومات شركة الحمادي القابضة فقط بناءً على اتفاقية تعاقدية
115	Translated (0%)	This agreement shall include, but not limited to:	:يجب أن تشمل هذه الاتفاقية، على سبيل المثال لا الحصر
116	Translated (0%)	The terms and conditions for access are provided.	.يتم توفير شروط وأحكام الوصول
117	Translated (0%)	The security responsibilities of the contractors, consultants or vendor personnel.	.المسؤوليات الأمنية للمقاولين أو الاستشاريين أو موظفي البائع
118	Translated (0%)	Agreement by the contractors, consultants or third-party personnel to abide to Al Hammadi Holding's information security policies.	موافقة المقاولين أو الاستشاريين أو موظفي الطرف الثالث على الالتزام .بسياسات أمن المعلومات الخاصة بالحمادي القابضة
119	Translated (0%)	Al Hammadi Holding Access control rules shall consider the need-to-know/use principles, information security levels, and classification of information, based on the premise "Everything is generally forbidden unless expressly permitted"	يجب أن تراعي قواعد التحكم في الوصول الخاصة بشركة الحمادي القابضة مبادئ الحاجة إلى المعرفة/الاستخدام ومستويات أمن المعلومات وتصنيف "المعلومات، بناءً على فرضية "كل شيء محظور عمومًا ما لم يُسمح به صراحة
120	Translated (0%)	Al Hammadi Holding shall consider the relevant legislation and contractual obligations regarding limitation of access to data or services.	يجب على شركة الحمادي القابضة النظر في التشريعات والالتزامات التعاقدية .ذات الصلة فيما يتعلق بالحد من الوصول إلى البيانات أو الخدمات
121	Translated (0%)	Al Hammadi Holding shall consider the management of access rights across all platforms and systems, including, cloud, on-premises, and disaster recovery remote locations.	يجب على شركة الحمادي القابضة النظر في إدارة حقوق الوصول عبر جميع المنصات والأنظمة، بما في ذلك المواقع السحابية والمواقع المحلية والمواقع .النائية للتعافي من الكوارث
122	Translated (0%)	Personnel must not use Al Hammadi Holding's information systems to engage in hacking activities that include, but are not limited to:	يجب على الموظفين عدم استخدام أنظمة معلومات شركة الحمادي القابضة :للانخراط في أنشطة القرصنة التي تشمل، على سبيل المثال لا الحصر
123	Translated (0%)	Gaining unauthorized access to any other information systems.	.الوصول غير المصرح به إلى أي أنظمة معلومات أخرى
124	Translated (0%)	Damaging, altering, or disrupting the operations of any other information systems.	.إتلاف أو تغيير أو تعطيل عمليات أي أنظمة معلومات أخرى
125	Translated (0%)	Capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism that could permit unauthorized access.	التقاط أو الحصول على كلمات المرور أو مفاتيح التشفير أو أي آلية أخرى .للتحكم في الوصول يمكن أن تسمح بالوصول غير المصرح به

126	Translated (0%)	All software installed on Al Hammadi Holding multi-user systems must be regulated by an approved access control system that will control a user's session prior to passing control to separate application software.	يجب تنظيم جميع البرامج المثبتة على أنظمة الحمادي القابضة متعددة المستخدمين من خلال نظام معتمد للتحكم في الوصول والذي سيتحكم في جلسة المستخدم قبل تمرير التحكم إلى برنامج تطبيق منفصل.
127	Translated (0%)	Workers who have been authorized to view information classified at a certain sensitivity level must be permitted to access only the information at this level and at less sensitive levels.	يجب السماح للعمال المصرح لهم بعرض المعلومات المصنفة عند مستوى حساسية معين بالوصول إلى المعلومات فقط على هذا المستوى وعلى مستويات أقل حساسية.
128	Translated (0%)	Workers must not move information classified at a certain sensitivity level to a less sensitive level unless this action is a formal part of an approved declassification process.	يجب على العمال عدم نقل المعلومات المصنفة عند مستوى حساسية معين إلى مستوى أقل حساسية ما لم يكن هذا الإجراء جزءًا رسميًا من عملية رفع السرية المعتمدة.
129	Translated (0%)	File access control permissions for all Al Hammadi Holding networked systems must be set to a default that blocks access by unauthorized users.	يجب تعيين أذونات التحكم في الوصول إلى الملفات لجميع أنظمة الحمادي القابضة الشبكية على الوضع الافتراضي الذي يمنع الوصول من قبل المستخدمين غير المصرح لهم.
130	Translated (0%)	The information systems access privileges of all users must be defined based on their officially assigned roles within Al Hammadi Holding Company.	يجب تحديد امتيازات الوصول إلى أنظمة المعلومات لجميع المستخدمين بناءً على أدوارهم المعينة رسميًا داخل شركة الحمادي القابضة.
131	Translated (0%)	All submitted, approved or processed user access requests are to be adequately logged with suitable audit trail implemented	يجب تسجيل جميع طلبات وصول المستخدم المقدمة أو المعتمدة أو المعالجة بشكل مناسب مع تنفيذ مسار تدقيق مناسب
132	Translated (0%)	All user access management activities shall be centralized within an assigned function	يجب أن تكون جميع أنشطة إدارة وصول المستخدم مركزية ضمن وظيفة معينة
133	Translated (0%)	Network Identity and cloud identity services must be governed by this policy.	يجب أن تخضع خدمات هوية الشبكة والهوية السحابية لهذه السياسة.
134	Translated (0%)	Access control rules must consider periodic review of access rights.	يجب أن تراعي قواعد التحكم في الوصول المراجعة الدورية لحقوق الوصول.
135	Translated (0%)	Access to networks and network services	الوصول إلى الشبكات وخدمات الشبكة
136	Translated (0%)	Users shall only be provided with access to the network segment and network services that they have been specifically authorized to use ('need-to-have' principle).	يجب تزويد المستخدمين فقط بإمكانية الوصول إلى شريحة الشبكة وخدمات الشبكة التي تم التصريح لهم على وجه التحديد باستخدامها (" مبدأ الحاجة إلى امتلاكها ").
137	Translated (0%)	Al Hammadi Holding networks and network services which can be accessed shall be defined and controlled.	يجب تحديد ومراقبة شبكات وخدمات شبكة الحمادي القابضة التي يمكن الوصول إليها.
138	Translated (0%)	Al Hammadi Holding shall define authorization procedures for determining who can access which networks and networked services.	تحدد شركة الحمادي القابضة إجراءات الترخيص لتحديد من يمكنه الوصول إلى الشبكات والخدمات الشبكية.
139	Translated (0%)	Al Hammadi Holding shall assign and install management controls and procedures to protect access to network connections and network services.	تقوم شركة الحمادي القابضة بتعيين وتركيب ضوابط وإجراءات الإدارة لحماية الوصول إلى اتصالات الشبكة وخدمات الشبكة.
140	Translated (0%)	The mechanism utilized by Al Hammadi Holding to access networks and network services (e.g., use of VPN or wireless network) shall be	يجب تحديد وإدارة الآلية التي تستخدمها شركة الحمادي القابضة للوصول إلى الشبكات وخدمات الشبكة (على سبيل المثال، استخدام VPN أو الشبكة

		defined and managed.	.(اللاسلكية
141	Translated (0%)	Al Hammadi Holding shall provide user authentication requirements for accessing various network services.	يجب أن توفر شركة الحمادي القابضة متطلبات مصادقة المستخدم للوصول .إلى خدمات الشبكة المختلفة
142	Translated (0%)	Al Hammadi Holding shall continuously monitor the use of network services to detect and prevent unauthorized and insecure connections to network services.	تراقب شركة الحمادي القابضة باستمرار استخدام خدمات الشبكة لاكتشاف .ومنع الاتصالات غير المصرح بها وغير الآمنة بخدمات الشبكة
143	Translated (0%)	Access to shared folders shall consider the following:	:يجب أن يراعي الوصول إلى المجلدات المشتركة ما يلي
144	Translated (0%)	Only authorized for specific persons.	.مصرح به فقط لأشخاص محددين
145	Translated (0%)	Only used for business purpose.	.تستخدم فقط لغرض العمل
146	Translated (0%)	Sharing any unrelated business materials (e.g., photos, videos, audio files, etc.) shall not be permitted.	لا يُسمح بمشاركة أي مواد تجارية غير ذات صلة (مثل الصور ومقاطع الفيديو .(والملفات الصوتية وما إلى ذلك
147	Translated (0%)	All internet access is controlled by Al Hammadi Holding Proxy Servers based on required business approval.	يتم التحكم في جميع الوصول إلى الإنترنت من قبل خوادم وكيل الحمادي .القابضة بناءً على موافقة العمل المطلوبة
148	Translated (0%)	No Access is granted unless there is a business justification and approval from the line manager is obtained through Technology Service Desk Ticket and using Workflow application.	لا يتم منح حق الوصول ما لم يكن هناك مبرر تجاري ويتم الحصول على موافقة من المدير المباشر من خلال تذكرة مكتب خدمة التكنولوجيا واستخدام .تطبيق سير العمل
149	Translated (0%)	All wireless access points must be installed by, configured by, and administered by a designated system admin.	يجب تثبيت جميع نقاط الوصول اللاسلكية وتكوينها وإدارتها بواسطة مسؤول .نظام معين
150	Translated (0%)	User Registration and De-registration	تسجيل المستخدم وإلغاء التسجيل
151	Translated (0%)	All users shall be identified with a unique credential that establishes identity.	.يجب تعريف جميع المستخدمين ببيانات اعتماد فريدة تحدد الهوية
152	Translated (0%)	User credentials shall require at least one factor of authentication (e.g., password, token number, or biometric devices).	يجب أن تتطلب بيانات اعتماد المستخدم عاملًا واحدًا على الأقل للمصادقة .(على سبيل المثال، كلمة المرور أو رقم الرمز المميز أو الأجهزة البيومترية)
153	Translated (0%)	User credentials shall adhere to the following naming convention:	:يجب أن تلتزم بيانات اعتماد المستخدم باتفاقية التسمية التالية
154	Translated (0%)	Normal users:	:المستخدمون العاديون
155	Translated (0%)	“FirstName.LastName”	"الاسم الأول .الاسم الأخير"
156	Translated (0%)	Use of shared IDs must only be permitted where they are necessary for business or operational reasons and must be approved and documented.	يجب السماح باستخدام بطاقات الهوية المشتركة فقط عندما تكون ضرورية .لأسباب تجارية أو تشغيلية ويجب الموافقة عليها وتوثيقها
157	Translated (0%)	Al Hammadi Holding must immediately disable user IDs of terminated employees.	يجب على شركة الحمادي القابضة تعطيل معرفات المستخدمين الخاصة .بالموظفين الذين تم إنهاء خدمتهم على الفور
158	Translated	Head of each Business Units and IT Department shall be periodically	يجب على رئيس كل وحدة عمل وقسم تكنولوجيا المعلومات تحديد وإزالة أو

	(0%)	identifying and removing or disable redundant user IDs.	.تعطيل معرفات المستخدم الزائدة بشكل دوري
159	Translated (0%)	Al Hammadi Holding shall define a formal access control procedure that includes clear steps in relation to requesting, creating, modifying, suspending and revoking user accounts.	يجب على شركة الحمادي القابضة تحديد إجراء رسمي للتحكم في الوصول يتضمن خطوات واضحة فيما يتعلق بطلب وإنشاء وتعديل وتعليق وإلغاء .حسابات المستخدمين
160	Translated (0%)	The granting of user access, changes to existing user access rights and removal of user access shall be authorized by the Asset Owner, considering the following:	يجب أن يكون منح وصول المستخدم، والتغييرات في حقوق وصول المستخدم الحالية وإزالة وصول المستخدم مصرحًا به من قبل مسؤول إدارة الأصل، مع :مراعاة ما يلي
161	Translated (0%)	Least privilege (‘need to know’ principle).	.أقل امتياز (مبدأ "الحاجة إلى المعرفة ")
162	Translated (0%)	Segregation of duties.	.الفصل بين الواجبات
163	Translated (0%)	Level of access required.	.مستوى الوصول المطلوب
164	Translated (0%)	All changes to access rights shall be processed in a timely manner	يجب معالجة جميع التغييرات في حقوق الوصول في الوقت المناسب
165	Translated (0%)	The convention used for Al Hammadi Holding email addresses will be:	:العرف المستخدم لعناوين البريد الإلكتروني لشركة الحمادي القابضة هو
166	Translated (0%)	*<1019>*Doctors, Nurses and Allied Health Professionals - FirstName.LastName@hh.med.sa*</1019>*	- الأطباء والممرضات والمهنيون الصحيون المساعدون*<1019>* FirstName.LastName@hh.med.sa*</1019>*
167	Translated (0%)	*<1025>*Supply Chain Staff - FirstName.LastName@unified.sa*</1025>*	- موظفو سلسلة التوريد*<1025>* FirstName.LastName@unified.sa*</1025>*
168	Translated (0%)	*<1031>*Facility and Maintenance Staff - FirstName.LastName@maintenance.sa*</1031>*	- موظفو المرافق والصيانة*<1031>* FirstName.LastName@maintenance.sa*</1031>*
169	Translated (0%)	*<1040>*Support Services - FirstName.LastName@hospitality.sa*</1040>*	- خدمات الدعم*<1040>* FirstName.LastName@hospitality.sa*</1040>*
170	Translated (0%)	*<1046>*Corporate Medical Administration - FirstName.LastName@alhammadi.med.sa or Designation@ alhammadi.med.sa*</1046>*	- الإدارة الطبية للشركات*<1046>* FirstName.LastName@alhammadi.med.sa أو المسمى الوظيفي@ alhammadi.med.sa*</1046>*
171	Translated (0%)	*<1058>*Corporate Management – Designation@alhammadi.com*</1058>*	*<1058>*إدارة الشركات – Designation@alhammadi.com*</1058>*
172	Translated (0%)	Every user ID established for a non-permanent employee must have a specified expiration date, with a default expiration of 90 days when the actual expiration date is unknown.	يجب أن يكون لكل معرف مستخدم تم إنشاؤه للموظف غير الدائم تاريخ انتهاء صلاحية محدد، مع انتهاء صلاحية افتراضي لمدة 90 يومًا عندما يكون تاريخ .انتهاء الصلاحية الفعلي غير معروف
173	Translated (0%)	All Al Hammadi Holding information systems privileges must be promptly terminated at the time that a worker ceases to provide services to Al Hammadi Holding.	يجب إنهاء جميع امتيازات أنظمة معلومات شركة الحمادي القابضة على الفور في الوقت الذي يتوقف فيه العامل عن تقديم الخدمات إلى شركة الحمادي .القابضة
174	Translated (0%)	A written agreement, which includes a binding commitment to abide by Al Hammadi Holding’s security policies and procedures, must be received by Al Hammadi Holding staff prior to the establishment of a	يجب استلام اتفاقية مكتوبة، والتي تتضمن التزامًا ملزمًا بالالتزام بالسياسات والإجراءات الأمنية لشركة الحمادي القابضة، من قبل موظفي شركة الحمادي .القابضة قبل إنشاء معرف مستخدم لأي طرف ثالث

		user ID for any third party.	
175	Translated (0%)	If the third party is a corporation, a government agency, or some other organization, then an authorized officer must sign the agreement.	إذا كان الطرف الثالث شركة أو وكالة حكومية أو منظمة أخرى، فيجب على المسؤول المفوض توقيع الاتفاقية.
176	Translated (0%)	HR Department shall inform all concerned parties regarding any employee who has joined or left Al Hammadi Holding or has moved to a new role/function.	يجب على إدارة الموارد البشرية إبلاغ جميع الأطراف المعنية فيما يتعلق بأي موظف انضم إلى شركة الحمادي القابضة أو تركها أو انتقل إلى دور/وظيفة جديدة.
177	Translated (0%)	Based on the inputs received, IT shall create access rights in domain with a unique ID for giving access to the network services and to the local PC/Workstation.	بناءً على المدخلات المستلمة، يجب على تكنولوجيا المعلومات إنشاء حقوق وصول في المجال بمعرف فريد لإتاحة الوصول إلى خدمات الشبكة وإلى جهاز الكمبيوتر/محطة العمل المحلية.
178	Translated (0%)	Email IDs shall be created as required.	يجب إنشاء معرفات البريد الإلكتروني كما هو مطلوب.
179	Translated (0%)	NDA Signed between employee and Al Hammadi Holding at the time of employment through the HR Induction Process.	تم توقيع اتفاقية عدم الإفصاح بين الموظف والحمادي القابضة في وقت التوظيف من خلال عملية توجيه الموارد البشرية.
180	Translated (0%)	In case of external parties / third parties user registration, IT and cybersecurity shall authorize the access before IT creates the login in the domain.	في حالة تسجيل مستخدمين من أطراف خارجية/أطراف ثالثة، يجب أن تسمح تكنولوجيا المعلومات والأمن السيبراني بالوصول قبل أن تنشئ تكنولوجيا المعلومات تسجيل الدخول إلى النطاق.
181	Translated (0%)	The process for managing user IDs shall include:	يجب أن تشمل عملية إدارة معرفات المستخدمين ما يلي:
182	Translated (0%)	Using unique user IDs to enable users to be linked to and held responsible for their actions.	استخدام معرفات مستخدم فريدة لتمكين المستخدمين من الارتباط بأفعالهم وتحميلهم المسؤولية عنها.
183	Translated (0%)	Immediately disabling or removing user IDs of users who have left Al Hammadi Holding.	تعطيل أو إزالة معرّفات المستخدم للمستخدمين الذين غادروا شركة الحمادي القابضة على الفور.
184	Translated (0%)	Periodically identifying and removing or disabling redundant user IDs.	تحديد وإزالة أو تعطيل معرفات المستخدم الزائدة بشكل دوري.
185	Translated (0%)	Ensuring that redundant users' IDs are not issued to other users	التأكد من عدم إصدار معرّفات المستخدمين الزائدة عن الحاجة للمستخدمين الآخرين
186	Translated (0%)	User Access Provisioning	توفير وصول المستخدم
187	Translated (0%)	Al Hammadi Holding shall implement a formal user access provisioning process to assign or revoke access rights for all user types to all systems and services, and shall include:	يجب على شركة الحمادي القابضة تنفيذ عملية توفير وصول المستخدم الرسمية لتعيين أو إلغاء حقوق الوصول لجميع أنواع المستخدمين لجميع الأنظمة والخدمات، ويجب أن تشمل:
188	Translated (0%)	Obtaining authorization from the owner of the information system or service for the use of the information system or service.	الحصول على إذن من مسؤول إدارة نظام المعلومات أو الخدمة لاستخدام نظام المعلومات أو الخدمة.
189	Translated (0%)	Separate approval for access rights from risk owners may also be appropriate.	قد يكون من المناسب أيضًا الحصول على موافقة منفصلة على حقوق الوصول من مسؤولي إدارة المخاطر.
190	Translated (0%)	Verifying that the level of access granted is appropriate to Al Hammadi Holding access policies and consistent with segregation of duties.	التحقق من أن مستوى الوصول الممنوح مناسب لسياسات الوصول الخاصة بشركة الحمادي القابضة ومتسق مع الفصل بين الواجبات.

191	Translated (0%)	Maintaining a central record of access rights granted to all Al Hammadi Holding users.	الاحتفاظ بسجل مركزي لحقوق الوصول الممنوحة لجميع مستخدمي شركة الحمادي القابضة.
192	Translated (0%)	Adapting access rights of users who have changed roles or jobs.	تكييف حقوق الوصول للمستخدمين الذين غيروا أدوارهم أو وظائفهم.
193	Translated (0%)	Immediately removing or blocking access rights of users who have left Al Hammadi Holding.	إزالة أو حظر حقوق الوصول للمستخدمين الذين غادروا الحمادي القابضة على الفور.
194	Translated (0%)	Periodically reviewing access rights with owners of the information systems or services.	المراجعة الدورية لحقوق الوصول مع مسؤولي أنظمة أو خدمات المعلومات.
195	Translated (0%)	Ensuring that access rights are not activated (e.g., by system admins) before authorization procedures are completed.	التأكد من عدم تفعيل حقوق الوصول (على سبيل المثال، من قبل مسؤولي النظام) قبل إكمال إجراءات التفويض.
196	Translated (0%)	Management of Privileged Access Rights	إدارة حقوق الوصول المميز
197	Translated (0%)	Al Hammadi Holding allocation of privileged access rights shall be separately controlled through a formal authorization process by:	يجب التحكم في تخصيص شركة الحمادي القابضة لحقوق الوصول المميزة بشكل منفصل من خلال عملية تفويض رسمية من خلال:
198	Translated (0%)	Identifying the privileged access rights associated with each system or process, e.g., operating system, database, applications, and the users to whom they need to be allocated.	تحديد حقوق الوصول المميزة المرتبطة بكل نظام أو عملية، على سبيل المثال، نظام التشغيل وقاعدة البيانات والتطبيقات والمستخدمين الذين يحتاجون إلى تخصيصها لهم.
199	Translated (0%)	Allocating privileged access rights to users on a need-to-use basis and on an event-by-event basis.	تخصيص حقوق وصول مميزة للمستخدمين على أساس الحاجة إلى الاستخدام وعلى أساس كل حدث على حدة.
200	Translated (0%)	Maintaining a record of all allocated privileges.	الاحتفاظ بسجل لجميع الامتيازات المخصصة.
201	Translated (0%)	Maintaining requirements for expiry of privileged access rights.	الحفاظ على متطلبات انتهاء صلاحية حقوق الوصول المميزة.
202	Translated (0%)	Assigning privileged access rights to user IDs different from those used for regular business activities.	تعيين حقوق وصول مميزة لمعرفات المستخدم المختلفة عن تلك المستخدمة في الأنشطة التجارية العادية.
203	Translated (0%)	Regular business activities shall not be performed from privileged ID.	لا يجوز تنفيذ الأنشطة التجارية العادية من بطاقة الهوية المميزة.
204	Translated (0%)	Regularly review the competences of users with privileged access rights.	المراجعة المنتظمة لكفاءات المستخدمين الذين يتمتعون بحقوق وصول مميزة.
205	Translated (0%)	Avoiding the unauthorized use of generic administration user IDs.	تجنب الاستخدام غير المصرح به لمعرفات مستخدم الإدارة العامة.
206	Translated (0%)	Generic and default accounts or tokens shall be renamed, disabled or limited to emergency access only, wherever practical.	يجب إعادة تسمية الحسابات أو الرموز العامة أو الافتراضية أو تعطيلها أو قصرها على الوصول في حالات الطوارئ فقط، حيثما كان ذلك عمليًا.
207	Translated (0%)	All authorized user accessing Al Hammadi Holding information assets shall be defined and documented.	يجب تحديد وتوثيق جميع المستخدمين المصرح لهم بالوصول إلى أصول معلومات شركة الحمادي القابضة.
208	Translated (0%)	Authorization’s process shall be tracked and logged as follows:	يجب تتبع عملية التفويض وتسجيلها على النحو التالي:
209	Translated (0%)	Date of authorization.	تاريخ التفويض.

210	Translated (0%)	Identification of individual approving access.	.تحديد الوصول الفردي للموافقة
211	Translated (0%)	Description of access privileges granted.	.وصف امتيازات الوصول الممنوحة
212	Translated (0%)	Description of why access privileges granted.	.وصف سبب منح امتيازات الوصول
213	Translated (0%)	Segregation of duties and least privileges principles shall be followed when granting access privileges to Al Hammadi Holding users.	يجب اتباع مبادئ الفصل بين الواجبات وأقل الامتيازات عند منح امتيازات .الوصول لمستخدمي شركة الحمادي القابضة
214	Translated (0%)	The risk owner / asset owner shall ensure the following:	:يجب على مسؤول إدارة المخاطرة/مسؤول الأصول ضمان ما يلي
215	Translated (0%)	Every user is assigned only those rights to various resources that are required for doing his/her allotted work.	يتم تعيين كل مستخدم فقط تلك الحقوق في الموارد المختلفة المطلوبة للقيام .بعمله المخصص
216	Translated (0%)	Formal authorization shall be taken for any privilege given to the user and records shall be maintained.	يجب الحصول على إذن رسمي لأي امتياز يُمنح للمستخدم ويجب الاحتفاظ .بالسجلات
217	Translated (0%)	Privileged access rights shall not be granted until the authorization process is complete.	.لا تُمنح حقوق الوصول المميزة حتى تكتمل عملية التفويض
218	Translated (0%)	As a best practice, no privilege shall be given for unlimited time period.	.كأفضل ممارسة، لا يجوز منح أي امتياز لفترة زمنية غير محدودة
219	Translated (0%)	However, privileges shall be provided without any time limit as per the functional roles, business unit needs and policies.	ومع ذلك، يجب توفير الامتيازات دون أي حد زمني وفقًا للأدوار الوظيفية .واحتياجات وسياسات وحدة الأعمال
220	Translated (0%)	The privileges are only given on need basis and shall be removed immediately after expiry period.	تُمنح الامتيازات فقط على أساس الحاجة ويجب إزالتها فور انتهاء فترة .الصلاحية
221	Translated (0%)	Privileged access rights shall be assigned to a user ID different from those used for regular business activities.	يجب تعيين حقوق الوصول المميزة لمعرف مستخدم مختلف عن تلك .المستخدمة في الأنشطة التجارية العادية
222	Translated (0%)	Regular business activities shall not be performed from privileged ID	لا يجوز تنفيذ الأنشطة التجارية العادية من بطاقة الهوية المميزة
223	Translated (0%)	Multi-Factor authentication is to be used when accessing the production environment using a privileged access account	يجب استخدام المصادقة متعددة العوامل عند الوصول إلى بيئة الإنتاج باستخدام حساب وصول متميز
224	Translated (0%)	The competences of users with privileged access rights shall be reviewed regularly in order to verify if they are in line with their duties	يجب مراجعة كفاءات المستخدمين الذين يتمتعون بحقوق وصول مميزة بانتظام من أجل التحقق مما إذا كانوا متوافقين مع واجباتهم
225	Translated (0%)	Specific procedures shall be established and maintained in order to avoid the unauthorized use of generic administration user IDs, according to systems' configuration capabilities	يجب وضع إجراءات محددة والحفاظ عليها من أجل تجنب الاستخدام غير المصرح به لمعرفات مستخدم الإدارة العامة، وفقًا لقدرات تكوين الأنظمة
226	Translated (0%)	The use of generic administration accounts (e.g., Admin, system, etc.) is prohibited.	.يُحظر استخدام حسابات الإدارة العامة (مثل المسؤول والنظام وما إلى ذلك)
227	Translated (0%)	In cases where generic (non-named) accounts must be used due to system limitation/requirement, each account shall have enough justification along with the authorized persons who have access to	في الحالات التي يجب فيها استخدام حسابات عامة (غير مسماة) بسبب قيود/متطلبات النظام، يجب أن يكون لكل حساب مبرر كافٍ إلى جانب .الأشخاص المصرح لهم بالوصول إلى الحسابات المذكورة

		said accounts.	
228	Translated (0%)	The justification is to be approved by the appropriate parties.	.يجب أن تتم الموافقة على التبرير من قبل الأطراف المناسبة
229	Translated (100%)	Management of secret authentication information of users	إدارة معلومات المصادقة السرية للمستخدمين
230	Translated (0%)	Users must be authenticated using multi factor authentication before they can gain access to Al Hammadi Holding's information systems based on a risk assessment.	يجب مصادقة المستخدمين باستخدام المصادقة متعددة العوامل قبل أن يتمكنوا من الوصول إلى أنظمة معلومات شركة الحمادي القابضة بناءً على .تقييم المخاطر
231	Translated (0%)	Service accounts shall not be used to access systems interactively.	.لا يجوز استخدام حسابات الخدمة للوصول إلى الأنظمة بشكل تفاعلي
232	Translated (0%)	User identity shall be verified before modifying any credentials.	.يجب التحقق من هوية المستخدم قبل تعديل أي بيانات اعتماد
233	Translated (0%)	Users shall not share accounts unless there is a documented and approved business justification.	لا يجوز للمستخدمين مشاركة الحسابات ما لم يكن هناك مبرر تجاري موثق .ومعتمد
234	Translated (0%)	Once approved, it must be assigned to a single nominated individual for ownership purposes.	.بمجرد الموافقة، يجب إسنادها إلى فرد محدد واحد لغرض تحمل المسؤولية
235	Translated (0%)	All Al Hammadi Holding's information systems shall require identification and authentication through passwords as a prior to allowing user access:	يجب أن تتطلب جميع أنظمة معلومات شركة الحمادي القابضة تحديد الهوية :والمصادقة من خلال كلمات المرور قبل السماح بوصول المستخدم
236	Translated (0%)	Password shall be minimum of 8 characters' length.	.يجب ألا يقل طول كلمة المرور عن 8 أحرف
237	Translated (0%)	Password shall be combination of:	:يجب أن تكون كلمة المرور مزيجًا من
238	Translated (0%)	At least one uppercase alphabetic character (A-Z).	.(A - Z) حرف أبجدي كبير واحد على الأقل
239	Translated (0%)	At least one lowercase alphabetic character (a-z).	.(a - z) حرف أبجدي صغير واحد على الأقل
240	Translated (0%)	At least one special character (e.g., @, %, &).	.حرف خاص واحد على الأقل (على سبيل المثال، @، %، &)
241	Translated (0%)	At least one number (0-9).	.رقم واحد على الأقل (0-9)
242	Translated (0%)	Password shall not be guessable, or a word found in a dictionary.	.يجب ألا تكون كلمة المرور قابلة للتخمين، أو كلمة موجودة في القاموس
243	Translated (0%)	Blank password shall not be allowed.	.لا يُسمح باستخدام كلمة المرور الفارغة
244	Translated (0%)	Users shall be required to change their password immediately after their first login to any system.	يجب على المستخدمين تغيير كلمة المرور الخاصة بهم فور تسجيل دخولهم .لأول مرة إلى أي نظام
245	Translated (0%)	Password change shall be enforced (by the operating system or the application) at least every 45 days.	يجب فرض تغيير كلمة المرور (بواسطة نظام التشغيل أو التطبيق) كل 45 يومًا .على الأقل

246	Translated (0%)	The new passwords shall not be the same as the previous 24 passwords used (password history).	يجب ألا تكون كلمات المرور الجديدة هي نفسها كلمات المرور الـ 24 السابقة المستخدمة (سجل كلمات المرور).
247	Translated (0%)	For customer facing applications, the password history setting is 3.	بالنسبة للتطبيقات التي تواجه العملاء، يكون إعداد سجل كلمة المرور هو 3.
248	Translated (0%)	User accounts shall be locked after 4 unsuccessful attempts and Account shall be unlocked by IT support.	يجب قفل حسابات المستخدمين بعد 4 محاولات غير ناجحة ويجب إلغاء قفل الحساب من قبل دعم تكنولوجيا المعلومات.
249	Translated (0%)	Initial password shall be only used one time.	يجب استخدام كلمة المرور الأولية مرة واحدة فقط.
250	Translated (0%)	Password shall be stored and transmitted in protected (e.g., encrypted or hashed) form.	يجب تخزين كلمة المرور ونقلها في شكل محمي (على سبيل المثال، مشفر أو مجزأ).
251	Translated (0%)	Passwords shall be immediately changed if there is any suspicion of password compromise and this shall be reported immediately to Information Technology Department.	يجب تغيير كلمات المرور على الفور إذا كان هناك أي اشتباه في اختراق كلمة المرور ويجب إبلاغ قسم تكنولوجيا المعلومات بذلك على الفور.
252	Translated (0%)	Information Technology Department shall change all information system default usernames and passwords before any information system is put into operation:	يجب على إدارة تكنولوجيا المعلومات تغيير جميع أسماء المستخدمين وكلمات المرور الافتراضية لنظام المعلومات قبل تشغيل أي نظام معلومات:
253	Translated (0%)	Temporary or Initial Passwords issued by User Management Admin must be expired, forcing the user to choose another password before the next logon process is completed.	يجب أن تنتهي صلاحية كلمات المرور المؤقتة أو الأولية الصادرة عن مسؤول إدارة المستخدم، مما يجبر المستخدم على اختيار كلمة مرور أخرى قبل اكتمال عملية تسجيل الدخول التالية.
254	Translated (0%)	The Initial or Temporary password for any domain user must be sent through a communications channel other than the channel used to log on to Al Hammadi Holding systems including, but not limited to, SMS to user's mobile, and in-person appearance at a trusted intermediary's office along with the provision of picture identification.	يجب إرسال كلمة المرور الأولية أو المؤقتة لأي مستخدم نطاق من خلال قناة اتصالات أخرى غير القناة المستخدمة لتسجيل الدخول إلى أنظمة الحمادي القابضة بما في ذلك، على سبيل المثال لا الحصر، الرسائل النصية القصيرة إلى هاتف المستخدم المحمول، والمظهر الشخصي في مكتب وسيط موثوق به إلى جانب توفير تحديد الصورة.
255	Translated (0%)	All Al Hammadi Holding computer systems that employ fixed passwords at log on must be configured to permit only five attempts to enter a correct password, after which the user ID is deactivated and can only be reset by the IT Department staff after authenticating the user's identity.	يجب تهيئة جميع أنظمة كمبيوتر شركة الحمادي القابضة التي تستخدم كلمات مرور ثابتة عند تسجيل الدخول للسماح بخمس محاولات فقط لإدخال كلمة مرور صحيحة، وبعد ذلك يتم إلغاء تنشيط معرف المستخدم ولا يمكن إعادة تعيينه إلا من قبل موظفي قسم تكنولوجيا المعلومات بعد مصادقة هوية المستخدم.
256	Translated (0%)	Passwords must never be hard-coded in software developed for or modified for Al Hammadi Holding.	يجب ألا تكون كلمات المرور مشفرة في البرامج التي تم تطويرها أو تعديلها لصالح شركة الحمادي القابضة.
257	Translated (0%)	Users must not construct passwords that are identical or substantially similar to passwords that they had previously employed.	يجب على المستخدمين عدم إنشاء كلمات مرور مماثلة أو مشابهة إلى حد كبير لكلمات المرور التي استخدموها سابقًا.
258	Translated (0%)	All software and files containing formulas, algorithms, and other specifics of the process used to generate passwords or personal identification numbers must be controlled with the most stringent security measures supported by the involved computer system.	يجب التحكم في جميع البرامج والملفات التي تحتوي على الصيغ والخوارزميات وغيرها من تفاصيل العملية المستخدمة لإنشاء كلمات المرور أو أرقام التعريف الشخصية من خلال تدابير الأمان الأكثر صرامة التي يدعمها نظام الكمبيوتر المعني.

259	Translated (0%)	The display and printing of passwords, when end users enter them, must be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them.	يجب إخفاء عرض وطباعة كلمات المرور، عندما يدخلها المستخدمون النهائيون، أو قمعها أو حجبها بطريقة أخرى حتى لا تتمكن الأطراف غير المصرح لها من مراقبتها أو استعادتها لاحقًا.
260	Translated (0%)	All fixed password resets or changes must be promptly confirmed by regular mail so that the authorized user can readily detect and report any fraudulent or abusive behavior.	يجب تأكيد جميع عمليات إعادة تعيين كلمة المرور الثابتة أو التغييرات على الفور عن طريق البريد العادي حتى يتمكن المستخدم المصرح له من اكتشاف أي سلوك احتيالي أو مسيء والإبلاغ عنه بسهولة.
261	Translated (0%)	The password itself must not be transmitted - only the fact that it was changed.	يجب عدم إرسال كلمة المرور نفسها - فقط حقيقة أنه تم تغييرها.
262	Translated (0%)	Whenever user-chosen passwords or encryption keys are specified, they must be entered twice and masked such that the user cannot see what was typed.	عندما يتم تحديد كلمات المرور أو مفاتيح التشفير التي اختارها المستخدم، يجب إدخالها مرتين وإخفائها بحيث لا يتمكن المستخدم من رؤية ما تم كتابته.
263	Translated (0%)	The fixed password change interval must be synchronized across all computer and network platforms at Al Hammadi Holding.	يجب مزامنة الفاصل الزمني الثابت لتغيير كلمة المرور عبر جميع منصات الكمبيوتر والشبكة في شركة الحمادي القابضة.
264	Translated (0%)	The number of domain administrators in active directory, and other accounts with privileged access, shall be limited and provided only to those with a strict requirement in order to perform their assigned tasks.	يجب أن يكون عدد مسؤولي النطاق في الدليل النشط، والحسابات الأخرى ذات الوصول المميز، محدودًا ويتم توفيره فقط لأولئك الذين لديهم متطلبات صارمة من أجل أداء المهام الموكلة إليهم.
265	Translated (0%)	Review of User Access Rights	مراجعة حقوق وصول المستخدم
266	Translated (0%)	A process for regularly reviewing access rights shall be defined and implemented.	يجب تحديد وتنفيذ عملية لمراجعة حقوق الوصول بانتظام.
267	Translated (0%)	User access rights must be reviewed at least annually and upon a user changing role.	يجب مراجعة حقوق وصول المستخدم سنويًا على الأقل وعند تغيير دور المستخدم.
268	Translated (0%)	Privileged accounts must be reviewed at least every 3 months, and system privileges granted to every user must be reevaluated by the user’s direct manager every 3 months to determine whether currently-enabled system privileges are needed to perform the user’s current job duties.	يجب مراجعة الحسابات المميزة كل 3 أشهر على الأقل، ويجب إعادة تقييم امتيازات النظام الممنوحة لكل مستخدم من قبل المدير المباشر للمستخدم كل 3 أشهر لتحديد ما إذا كانت امتيازات النظام الممكّنة حاليًا مطلوبة لأداء واجبات الوظيفة الحالية للمستخدم.
269	Translated (0%)	IT systems and physical access systems shall have the ability to produce enough information to support user access reviews.	يجب أن تتمتع أنظمة تكنولوجيا المعلومات وأنظمة الوصول المادية بالقدرة على إنتاج معلومات كافية لدعم مراجعات وصول المستخدم.
270	Translated (0%)	Upon detection of any misconduct of privileged access rights, the Information Technology Department shall restrict such privileges.	عند اكتشاف أي سوء تصرف في حقوق الوصول المتميزة، تقوم إدارة تكنولوجيا المعلومات بتقييد هذه الامتيازات.
271	Translated (0%)	The Cybersecurity Department must, on a periodic basis, review the granted access privileges of a selected group of users.	يجب على إدارة الأمن السيبراني، على أساس دوري، مراجعة امتيازات الوصول الممنوحة لمجموعة مختارة من المستخدمين.
272	Translated (0%)	This review must illuminate whether the users have only those privileges necessary to perform their jobs and no additional privileges.	يجب أن توضح هذه المراجعة ما إذا كان المستخدمون يتمتعون فقط بالامتيازات اللازمة لأداء وظائفهم ولا يتمتعون بامتيازات إضافية.
273	Translated	User access rights shall be reviewed and re-allocated when moving	يجب مراجعة حقوق وصول المستخدم وإعادة تخصيصها عند الانتقال من دور

	(0%)	from one role to another within the same organization.	.إلى آخر داخل نفس المؤسسة
274	Translated (0%)	Authorizations for privileged access rights shall be reviewed at frequent intervals.	.يجب مراجعة التصاريح الخاصة بحقوق الوصول المتميزة على فترات متكررة
275	Translated (0%)	Changes to privileged accounts shall be logged for periodic review.	.يجب تسجيل التغييرات التي تطرأ على الحسابات المميزة للمراجعة الدورية
276	Translated (0%)	Removal or Adjustment of Access Rights	إزالة أو تعديل حقوق الوصول
277	Translated (0%)	Access rights (logical and/or physical) to information and information processing facilities shall be removed upon termination of the employment or contractual agreement.	يجب إزالة حقوق الوصول (المنطقية و/أو المادية) إلى مرافق معالجة المعلومات والمعلومات عند إنهاء العمل أو الاتفاقية التعاقدية.
278	Translated (0%)	Changes of employment shall be reflected in the removal of all access rights that were not approved for the new employment.	يجب أن تنعكس تغييرات التوظيف في إزالة جميع حقوق الوصول التي لم تتم الموافقة عليها للعمل الجديد.
279	Translated (0%)	Access rights that shall be removed or adjusted include those of physical and logical access.	تشمل حقوق الوصول التي يجب إزالتها أو تعديلها حقوق الوصول المادي والمنطقي.
280	Translated (0%)	Access rights for information and assets shall be reduced or removed before the employment terminates or changes, depending on the evaluation of risk factors such as:	يجب تقليل حقوق الوصول إلى المعلومات والأصول أو إزالتها قبل إنهاء التوظيف أو تغييره، اعتمادًا على تقييم عوامل الخطر مثل:
281	Translated (0%)	whether the termination or change is initiated by the employee, the external party user or by management, and the reason for termination.	ما إذا كان الإنهاء أو التغيير قد بدأ من قبل الموظف أو مستخدم الطرف الخارجي أو من قبل الإدارة، وسبب الإنهاء.
282	Translated (0%)	current responsibilities and value of the assets currently accessible.	.المسؤوليات الحالية وقيمة الأصول التي يمكن الوصول إليها حاليًا
283	Translated (0%)	Revoking of all identity cards (e.g., magnetic cards, or smart cards and keys).	إلغاء جميع بطاقات الهوية (مثل البطاقات الممغنطة أو البطاقات الذكية والمفاتيح).
284	Translated (0%)	Changing of shared access codes (e.g., lock combinations and safe combinations).	تغيير رموز الوصول المشتركة (على سبيل المثال، مجموعات القفل والمجموعات الآمنة).
285	Translated (100%)	Use of secret authentication information	استخدام معلومات المصادقة السرية
286	Translated (0%)	Al Hammadi Holding users shall be authenticated using multi-factor authentication before they can gain access to Al Hammadi Holding's information systems based on a risk assessment.	يجب مصادقة مستخدمي شركة الحمادي القابضة باستخدام المصادقة متعددة العوامل قبل أن يتمكنوا من الوصول إلى أنظمة معلومات شركة الحمادي القابضة بناءً على تقييم المخاطر.
287	Translated (0%)	Al Hammadi Holding users shall keep secret authentication information confidential, ensuring that it is not divulged to any other parties, including people of authority.	يجب على مستخدمي شركة الحمادي القابضة الحفاظ على سرية معلومات المصادقة السرية، وضمان عدم الكشف عنها لأي أطراف أخرى، بما في ذلك أصحاب الصلاحية.
288	Translated (0%)	Al Hammadi Holding users shall avoid keeping a record (e.g., on paper, software file or hand-held device) of secret authentication information, unless this can be stored securely, and the method of storing has been approved (e.g., password vault).	يجب على مستخدمي شركة الحمادي القابضة تجنب الاحتفاظ بسجل (على سبيل المثال، على الورق أو ملف البرنامج أو الجهاز المحمول باليد) لمعلومات المصادقة السرية، ما لم يكن من الممكن تخزينها بشكل آمن، وتمت الموافقة على طريقة التخزين (على سبيل المثال، مخزن كلمات المرور).
289	Translated	Al Hammadi Holding users shall change secret authentication	يجب على مستخدمي شركة الحمادي القابضة تغيير معلومات المصادقة السرية

	(0%)	information whenever there is any indication of its possible compromise.	.كلما كان هناك أي مؤشر على احتمال تعرضها للخطر
290	Translated (0%)	Al Hammadi Holding User identity shall be verified before modifying any credentials.	يجب التحقق من هوية مستخدم شركة الحمادي القابضة قبل تعديل أي بيانات اعتماد.
291	Translated (0%)	Al Hammadi Holding users shall not share accounts unless there is a documented and approved business justification.	لا يجوز لمستخدمي شركة الحمادي القابضة مشاركة الحسابات ما لم يكن هناك مبرر تجاري موثق ومعتمد.
292	Translated (100%)	Once approved, it must be assigned to a single nominated individual for ownership purposes.	بمجرد الموافقة، يجب إسنادها إلى فرد محدد واحد لغرض تحمل المسؤولية.
293	Translated (0%)	Users shall not insert passwords into email messages or electronic communications.	لا يجوز للمستخدمين إدخال كلمات المرور في رسائل البريد الإلكتروني أو الاتصالات الإلكترونية.
294	Translated (0%)	Users shall not distribute their username and password to other users. thus, users shall be accountable for any activity associated with their access rights.	لا يجوز للمستخدمين توزيع اسم المستخدم وكلمة المرور الخاصة بهم على المستخدمين الآخرين. وبالتالي، يكون المستخدمون مسؤولين عن أي نشاط مرتبط بحقوق الوصول الخاصة بهم.
295	Translated (0%)	Users shall not capture or otherwise obtain passwords, decryption keys, or any other access control mechanism, which could permit unauthorized access.	لا يجوز للمستخدمين التقاط أو الحصول على كلمات المرور أو مفاتيح فك التشفير أو أي آلية أخرى للتحكم في الوصول، والتي قد تسمح بالوصول غير المصرح به.
296	Translated (0%)	Users shall not do the following:	:لا يجوز للمستخدمين القيام بما يلي
297	Translated (0%)	Reveal a password over the phone to anyone.	.اكشف عن كلمة المرور عبر الهاتف لأي شخص
298	Translated (0%)	Reveal a password in an email message.	.اكشف عن كلمة مرور في رسالة بريد إلكتروني
299	Translated (0%)	Reveal a password to the boss.	.اكشف عن كلمة المرور للرئيس
300	Translated (0%)	Talk about a password in front of other	تحدث عن كلمة المرور أمام الآخرين
301	Translated (0%)	Hint at the format of a password (e.g., my family name).	.تلميح إلى تنسيق كلمة المرور (على سبيل المثال، اسم عائلتي)
302	Translated (0%)	Reveal a password on questionnaires or security forms.	.اكشف عن كلمة مرور في الاستبيانات أو نماذج الأمان
303	Translated (0%)	Share a password with family members.	.شارك كلمة المرور مع أفراد العائلة
304	Translated (0%)	Reveal a password to co-workers while on vacation.	.اكشف عن كلمة مرور لزملاء العمل أثناء الإجازة
305	Translated (0%)	Users must not store fixed passwords in Internet browsers, or related data communications software at any time.	يجب على المستخدمين عدم تخزين كلمات المرور الثابتة في متصفحات الإنترنت، أو برامج اتصالات البيانات ذات الصلة في أي وقت.
306	Translated (0%)	Al Hammadi Holding computer users must refuse all offers by software to place a cookie on their computer so that they can automatically log on the next time that they visit an Internet site.	يجب على مستخدمي الكمبيوتر في شركة الحمادي القابضة رفض جميع العروض التي يقدمها البرنامج لوضع ملف تعريف ارتباط على جهاز الكمبيوتر الخاص بهم حتى يتمكنوا من تسجيل الدخول تلقائيًا في المرة التالية التي

			.يزورون فيها موقعًا على الإنترنت
307	Translated (0%)	Users must not provide their user-IDs and/or passwords to data aggregators, data summarization/formatting services, or any other third parties.	يجب على المستخدمين عدم تقديم معرفات المستخدم و/أو كلمات المرور الخاصة بهم إلى مجمعي البيانات أو خدمات تلخيص/تنسيق البيانات أو أي .أطراف ثالثة أخرى
308	Translated (0%)	Such disclosures not only cause the involved users to be responsible for all damage that a third party may cause, but this behavior is also justifiable cause for Al Hammadi Holding to terminate the users' privileges on its systems.	مثل هذه الإفصاحات لا تتسبب فقط في أن يكون المستخدمون المعنيون مسؤولين عن جميع الأضرار التي قد يسببها طرف ثالث، ولكن هذا السلوك هو أيضًا سبب مبرر لشركة الحمادي القابضة لإنهاء امتيازات المستخدمين على .أنظمتها
309	Translated (0%)	Workers must not use an electronic mail account assigned to another individual to either send or receive messages.	يجب على العمال عدم استخدام حساب بريد إلكتروني مخصص لفرد آخر .لإرسال الرسائل أو تلقيها
310	Translated (0%)	System and Application Access Control	التحكم في الوصول إلى النظام والتطبيق
311	Translated (0%)	Access to Al Hammadi Holding information and application system functions shall be restricted.	يجب تقييد الوصول إلى معلومات شركة الحمادي القابضة ووظائف نظام .التطبيق
312	Translated (100%)	Information access restriction	تقييد الوصول إلى المعلومات
313	Translated (0%)	Al Hammadi Holding shall conduct the following in order to restrict access to systems and applications:	تقوم شركة الحمادي القابضة بما يلي من أجل تقييد الوصول إلى الأنظمة :والتطبيقات
314	Translated (0%)	Providing menus to control access to application system functions.	.توفير قوائم للتحكم في الوصول إلى وظائف نظام التطبيق
315	Translated (0%)	Appropriate controls shall be defined to control outputs from application systems that handle sensitive information, and those outputs are sent only to authorized personnel.	يجب تحديد الضوابط المناسبة للتحكم في المخرجات من أنظمة التطبيقات التي تتعامل مع المعلومات الحساسة، ويتم إرسال هذه المخرجات فقط إلى .الموظفين المصرح لهم
316	Translated (0%)	Controlling which data can be accessed by a user.	.التحكم في البيانات التي يمكن للمستخدم الوصول إليها
317	Translated (0%)	Controlling the access rights of users, e.g., read, write, delete and execute.	التحكم في حقوق الوصول للمستخدمين، على سبيل المثال، القراءة والكتابة .والحذف والتنفيذ
318	Translated (0%)	Controlling the access rights of other applications.	.التحكم في حقوق الوصول للتطبيقات الأخرى
319	Translated (0%)	Limiting the information contained as outputs.	.الحد من المعلومات الواردة كمخرجات
320	Translated (0%)	Providing physical or logical access controls for the isolation of sensitive applications, application data, or systems.	توفير ضوابط وصول مادية أو منطقية لعزل التطبيقات الحساسة أو بيانات .التطبيقات أو الأنظمة
321	Translated (0%)	Management must define user privileges such that ordinary users cannot gain access to, or otherwise interfere with, either the individual activities of, or the private data of other users.	يجب أن تحدد الإدارة امتيازات المستخدم بحيث لا يتمكن المستخدمون العاديون من الوصول إلى الأنشطة الفردية أو البيانات الخاصة للمستخدمين .الآخرين أو التدخل فيها بطريقة أخرى
322	Translated (0%)	Users must not read, modify, delete, or copy a file belonging to another user without first obtaining permission from the owner of the file.	يجب على المستخدمين عدم قراءة أو تعديل أو حذف أو نسخ ملف ينتمي إلى .مستخدم آخر دون الحصول أولًا على إذن من مسؤول الملف

323	Translated (0%)	Unless general user access is clearly provided, the ability to read, modify, delete, or copy a file belonging to another user does not imply permission to perform these activities.	ما لم يتم توفير وصول المستخدم العام بشكل واضح، فإن القدرة على قراءة أو تعديل أو حذف أو نسخ ملف ينتمي إلى مستخدم آخر لا تعني الإذن بتنفيذ هذه الأنشطة.
324	Translated (0%)	Permission to read a file belonging to another is implied if the owner of the file sends it via email attachment, USB delivery, or other transmission mechanism.	يكون الإذن بقراءة ملف ينتمي إلى ملف آخر ضمنيًا إذا أرسله مسؤول الملف أو أي آلية إرسال أخرى USB عبر مرفق البريد الإلكتروني أو تسليم.
325	Translated (0%)	Without specific written approval from management, administrators must not grant any privileges, beyond electronic mail and word processing, to any user.	دون موافقة خطية محددة من الإدارة، يجب على المسؤولين عدم منح أي امتيازات، تتجاوز البريد الإلكتروني ومعالجة النصوص، لأي مستخدم.
326	Translated (0%)	All production business applications supporting multiple users must be secured by an access control system.	يجب تأمين جميع تطبيقات أعمال الإنتاج التي تدعم مستخدمين متعددين بواسطة نظام التحكم في الوصول.
327	Translated (0%)	No application systems are exempted from this control.	لا توجد أنظمة تطبيق مستثناة من هذا التحكم.
328	Translated (0%)	Systems logs or application audit trails must not be disclosed to any person outside the team of individuals who ordinarily view such information in order to perform their jobs or investigate information security incidents.	يجب عدم الكشف عن سجلات الأنظمة أو مسارات تدقيق التطبيقات لأي شخص خارج فريق الأفراد الذين عادة ما يشاهدون هذه المعلومات من أجل أداء وظائفهم أو التحقيق في حوادث أمن المعلومات.
329	Translated (0%)	All exceptions require the approval of the CS Manager.	تتطلب جميع الاستثناءات موافقة مدير الأمن السيبراني.
330	Translated (0%)	All confidential or proprietary information that has been entrusted to Al Hammadi Holding by a third party must be protected as though it was Al Hammadi Holding confidential information.	يجب حماية جميع المعلومات السرية أو الملكية التي عُهد بها إلى شركة الحمادي القابضة من قبل طرف ثالث كما لو كانت معلومات سرية لشركة الحمادي القابضة.
331	Translated (0%)	All identifying information about customers such as National ID numbers and Mobile Phone numbers, must be accessible only to those Al Hammadi Holding personnel who need such access in order to perform their jobs.	يجب أن تكون جميع المعلومات التعريفية حول العملاء مثل أرقام الهوية الوطنية وأرقام الهواتف المحمولة متاحة فقط لموظفي شركة الحمادي القابضة الذين يحتاجون إلى مثل هذا الوصول من أجل أداء وظائفهم.
332	Translated (0%)	Access to secret information must be granted only to authorized individuals, not groups of individuals.	يجب منح الوصول إلى المعلومات السرية فقط للأفراد المصرح لهم، وليس لمجموعات الأفراد.
333	Translated (0%)	Secure Log-on Procedures	إجراءات تسجيل الدخول الآمنة
334	Translated (0%)	System shall display a general notice warning that the computer shall only be accessed by authorized users.	يجب أن يعرض النظام إشعارًا عامًا يحذر من أنه لا يمكن الوصول إلى الكمبيوتر إلا من قبل المستخدمين المصرح لهم.
335	Translated (0%)	Activities must be logged in accordance with the regulatory, audit and objectives and security requirements.	يجب تسجيل الأنشطة وفقًا للمتطلبات التنظيمية والتدقيق والأهداف والمتطلبات الأمنية.
336	Translated (0%)	Successful and failed access activities for authentication and authorizations must be logged.	يجب تسجيل أنشطة الوصول الناجحة والفاشلة للمصادقة والتفويضات.
337	Translated (0%)	System shall limit the number of unsuccessful logon attempts allowed.	يجب أن يحد النظام من عدد محاولات تسجيل الدخول غير الناجحة المسموح بها.
338	Translated	The following shall be considered:	يراعى ما يلي:

	(0%)		
339	Translated (0%)	Activities on system or application privileged accounts must be logged and reviewed.	يجب تسجيل الأنشطة على الحسابات المميزة للنظام أو التطبيق ومراجعتها.
340	Translated (0%)	The logon process on any system shall display only the limited information about the system and its purposed use.	يجب أن تعرض عملية تسجيل الدخول على أي نظام المعلومات المحدودة فقط حول النظام واستخدامه المقصود.
341	Translated (0%)	Forcing a time delay before further logon attempts are allowed or rejecting any further attempts without specific authorization.	فرض تأخير زمني قبل السماح بمحاولات تسجيل دخول أخرى أو رفض أي محاولات أخرى دون إذن محدد.
342	Translated (0%)	Sending an alarm message to the system console if the maximum number of logon attempts is reached.	إرسال رسالة إنذار إلى وحدة تحكم النظام إذا تم الوصول إلى الحد الأقصى لعدد محاولات تسجيل الدخول.
343	Translated (0%)	System administrators must review all unsuccessful log attempts in a periodically basis and must notice CS department.	يجب على مسؤولي النظام مراجعة جميع محاولات السجل غير الناجحة بشكل دوري ويجب أن يلاحظوا قسم الأمن السيبراني.
344	Translated (0%)	When logging into Al Hammadi Holding computer or data communications system, if any part of the logon sequence is incorrect, the user must be given only feedback that the entire logon process was incorrect.	عند تسجيل الدخول إلى كمبيوتر شركة الحمادي القابضة أو نظام اتصالات البيانات، إذا كان أي جزء من تسلسل تسجيل الدخول غير صحيح، فيجب إعطاء المستخدم ملاحظات فقط بأن عملية تسجيل الدخول بأكملها كانت غير صحيحة.
345	Translated (0%)	A standard warning banner developed by the IT Department and approved by the Legal Department must be displayed when users first connect to Al Hammadi Holding internal computer networks.	يجب عرض لافتة تحذير قياسية تم تطويرها من قبل قسم تكنولوجيا المعلومات ومعتمدة من قبل القسم القانوني عند اتصال المستخدمين لأول مرة بشبكات الكمبيوتر الداخلية لشركة الحمادي القابضة.
346	Translated (0%)	Password Management System	نظام إدارة كلمة المرور
347	Translated (0%)	Any account locked due to incorrect password entries must only be unlocked using Al Hammadi Holding IT processes.	يجب إلغاء قفل أي حساب مقفل بسبب إدخالات كلمة المرور غير الصحيحة فقط باستخدام عمليات تكنولوجيا المعلومات في شركة الحمادي القابضة.
348	Translated (0%)	Passwords must not contain the username associated with the account and technical controls to avoid such a possibility shall be implemented wherever possible.	يجب ألا تحتوي كلمات المرور على اسم المستخدم المرتبط بالحساب ويجب تنفيذ الضوابط الفنية لتجنب مثل هذا الاحتمال حيثما أمكن ذلك.
349	Translated (0%)	Interactive user account passwords shall be changed regularly and at least every 45 days.	يجب تغيير كلمات مرور حساب المستخدم التفاعلي بانتظام وكل 45 يومًا على الأقل.
350	Translated (0%)	Password for service and privileged accounts shall be changed every 30 days or based on the risk assessment.	يجب تغيير كلمة المرور الخاصة بالخدمة والحسابات المميزة كل 30 يومًا أو بناءً على تقييم المخاطر.
351	Translated (0%)	Passwords for service and privileged accounts must meet the following requirements at a minimum:	يجب أن تفي كلمات مرور الخدمة والحسابات المميزة بالمتطلبات التالية كحد أدنى:
352	Translated (0%)	Require a minimum length of at least 12 characters.	يتطلب حدًا أدنى للطول لا يقل عن 12 حرفًا.
353	Translated (0%)	Contain both numeric and alphabetic characters.	تحتوي على أحرف رقمية وأبجدية.
354	Translated (0%)	<1850>New password must not be the same as any of the last </1850>Fifteen<1856> passwords that the user used.</1856>	يجب ألا تكون كلمة المرور الجديدة هي نفسها أي من<1850> كلمات المرور الخمسة عشر الأخيرة التي استخدمها </1850><1856> المستخدم.</1856>
355	Translated	Lockout duration shall be set to 10 minutes.	يجب ضبط مدة القفل على 10 دقائق.

	(0%)		
356	Translated (0%)	If any of the password criteria cannot be met, a business justification must be documented and approved by system owners and Al Hammadi Holding IT based on risk assessment.	إذا تعذر استيفاء أي من معايير كلمة المرور، فيجب توثيق مبرر العمل والموافقة عليه من قبل مسؤولي النظام والحمادي القابضة لتقنية المعلومات بناءً على تقييم المخاطر.
357	Translated (0%)	Passwords must be treated as restricted information.	يجب التعامل مع كلمات المرور على أنها معلومات مقيدة.
358	Translated (0%)	Credentials must be stored and transported securely.	يجب تخزين بيانات الاعتماد ونقلها بشكل آمن.
359	Translated (0%)	A separated channel for sharing user ID and associated credentials to ensure that they are not stored or transmitted together.	قناة منفصلة لمشاركة معرف المستخدم وبيانات الاعتماد المرتبطة به لضمان عدم تخزينها أو نقلها معًا.
360	Translated (0%)	Initial passwords must be changed upon first use or passwords shall:	يجب تغيير كلمات المرور الأولية عند الاستخدام الأول أو يجب أن تكون كلمات المرور:
361	Translated (0%)	be changed after a password reset.	يتم تغييرها بعد إعادة تعيين كلمة المرور.
362	Translated (0%)	default passwords shall be changed.	يجب تغيير كلمات المرور الافتراضية.
363	Translated (0%)	Users shall not store credentials in any form except in Al Hammadi Holding IT approved password vault tools.	لا يجوز للمستخدمين تخزين بيانات الاعتماد بأي شكل من الأشكال إلا في أدوات خزينة كلمة المرور المعتمدة من شركة الحمادي القابضة لتقنية المعلومات.
364	Translated (0%)	Use of Privileged Utility Programs	استخدام برامج المرافق المتميزة
365	Translated (0%)	Access to and use of system programs must be restricted and controlled.	يجب تقييد الوصول إلى برامج النظام واستخدامها والتحكم فيها.
366	Translated (0%)	All unnecessary system utilities and software shall be removed.	يجب إزالة جميع الأدوات المساعدة والبرامج غير الضرورية للنظام.
367	Translated (0%)	No third-party utilities must be installed without prior authorization	يجب عدم تثبيت أي أدوات مساعدة تابعة لجهة خارجية دون إذن مسبق
368	Translated (100%)	Access control to program source code	التحكم في الوصول إلى كود المصدر للبرامج
369	Translated (0%)	Access to program source codes and configurations must be documented and restricted to an authorized personnel.	يجب توثيق الوصول إلى رموز وتكوينات مصدر البرنامج وتقييده على الموظفين المصرح لهم.
370	Translated (0%)	Al Hammadi Holding shall ensure that all source codes are compiled, controlled and maintained centrally.	تضمن شركة الحمادي القابضة تجميع جميع أكواد المصدر والتحكم فيها وصيانتها مركزيًا.
371	Translated (0%)	All program source code used for Al Hammadi Holding production systems must be stored in a secure source code management system with access controls approved by the CS department.	يجب تخزين جميع التعليمات البرمجية المصدر للبرنامج المستخدمة لأنظمة إنتاج الحمادي القابضة في نظام آمن لإدارة التعليمات البرمجية المصدر مع ضوابط الوصول المعتمدة من قبل قسم الأمن السيبراني.
372	Translated (0%)	Al Hammadi Holding production source code must include proper labeling, specified by the Information Security Function, to identify the sensitivity of the code and to allow for easy tracking for	يجب أن تتضمن شفرة مصدر إنتاج شركة الحمادي القابضة وضع العلامات المناسبة، التي تحددها وظيفة أمن المعلومات، لتحديد حساسية الشفرة والسماح بالتتبع السهل للإفصاح العام العرضي.

		accidental public disclosure.	
373	Translated (0%)	All Al Hammadi Holding production source code must be classified at the highest level of sensitivity and include proper labeling as specified by the Information Security Function.	يجب تصنيف جميع التعليمات البرمجية لمصدر إنتاج شركة الحمادي القابضة على أعلى مستوى من الحساسية وتشمل وضع العلامات المناسبة على النحو المحدد من قبل وظيفة أمن المعلومات.
374	Translated (0%)	Privileged and Remote Access Management	إدارة الامتيازات والوصول عن بعد
375	Translated (0%)	Al Hammadi Holding shall ensure that there is no external connection to the IT environment through any unsecure applications like:	تضمن شركة الحمادي القابضة عدم وجود اتصال خارجي ببيئة تكنولوجيا المعلومات من خلال أي تطبيقات غير آمنة مثل:
376	Translated (0%)	P2P applications and so on.	تطبيقات P2P وما إلى ذلك.
377	Translated (0%)	Al Hammadi Holding shall enforce using VPN connection for any external access to the IT environment and the VPN process shall include the following:	لأي وصول VPN يجب على شركة الحمادي القابضة فرض استخدام اتصال VPN خارجي إلى بيئة تكنولوجيا المعلومات ويجب أن تتضمن عملية ما يلي:
378	Translated (0%)	Any user either internally or externally needs access to the IT environment must fill the VPN access form and this form must be approved.	يجب على أي مستخدم يحتاج داخليًا أو خارجيًا إلى الوصول إلى بيئة تكنولوجيا المعلومات ملء نموذج الوصول إلى VPN ويجب الموافقة على هذا النموذج.
379	Translated (0%)	The VPN access request form must include the user data, the VPN usage reason, the needed access time and duration and so on.	بيانات المستخدم وسبب استخدام VPN يجب أن يتضمن نموذج طلب الوصول إلى VPN ووقت ومدة الوصول المطلوبة وما إلى ذلك.
380	Translated (0%)	The VPN access request will be reviewed by CS department and if the reason is valid it will be approved otherwise it will be rejected.	من قبل قسم الأمن السيبراني وإذا كان VPN ستتم مراجعة طلب الوصول إلى السبب صالحًا، فسيتم الموافقة عليه وإلا سيتم رفضه.
381	Translated (0%)	The VPN access shall use multi factor authentication not only user credentials.	المصادقة متعددة العوامل وليس فقط بيانات VPN يجب أن يستخدم وصول اعتماد المستخدم.
382	Translated (0%)	The VPN user password shall be complex and matched with Al Hammadi Holding password policy.	معقدة ومطابقة لسياسة كلمة مرور VPN يجب أن تكون كلمة مرور مستخدم شركة الحمادي القابضة.
383	Translated (0%)	The VPN users shall be reviewed periodically to remove any un-needed user access to ensure that there is no unauthorized user to access Al Hammadi Holding information assets.	بشكل دوري لإزالة أي وصول غير ضروري VPN يجب مراجعة مستخدمي للمستخدم لضمان عدم وجود مستخدم غير مصرح له بالوصول إلى أصول معلومات شركة الحمادي القابضة.
384	Translated (0%)	If there is a third-party company needs access to Al Hammadi Holding assets from outside using a VPN, Al Hammadi Holding shall enforce them to use its VPN channel not using any un-secure software for connecting remotely.	إذا كانت هناك شركة تابعة لجهة خارجية تحتاج إلى الوصول إلى أصول شركة الحمادي القابضة من الخارج باستخدام VPN، فيجب على شركة الحمادي القابضة إجبارها على استخدام قناة VPN الخاصة بها وعدم استخدام أي برنامج غير آمن للاتصال عن بُعد.
385	Translated (0%)	Al Hammadi Holding shall enforce restricting the users to share their VPN account credentials to avoid any credentials theft or also the non-accountability concept.	يجب على شركة الحمادي القابضة فرض قيود على المستخدمين لمشاركة بيانات اعتماد VPN الخاص بهم لتجنب أي سرقة لبيانات الاعتماد أو أيضًا مفهوم عدم المساءلة.
386	Translated (0%)	The VPN access time shall not be unlimited, and the duration shall be defined at the VPN access form and if any VPN access request sent to the authorized persons without limitation for the VPN account it shall be rejected.	غير محدود، ويجب تحديد المدة في نموذج VPN يجب ألا يكون وقت وصول VPN إلى الأشخاص المصرح لهم VPN وإذا تم إرسال أي طلب وصول VPN دون حصر لحساب VPN، فسيتم رفضه.

387	Translated (0%)	For any employee who leaves Al Hammadi Holding if he has a VPN user account it shall be removed, and this shall be a part of the revocation access for him.	بالنسبة لأي موظف يغادر شركة الحمادي القابضة إذا كان لديه حساب VPN، يجب إزالته، ويجب أن يكون ذلك جزءًا من وصول الإلغاء له.
388	Translated (0%)	The VPN session shall be terminated by using any control to disconnect the session when it is not needed by an automatic way.	باستخدام أي عنصر تحكم لفصل الجلسة عندما لا تكون VPN يتم إنهاء جلسة هناك حاجة إليها بطريقة تلقائية.
389	Translated (0%)	The VPN session shall be disconnected if there is no activity from the VPN user for maximum 5 minutes.	لمدة 5 VPN إذا لم يكن هناك نشاط من مستخدم VPN يجب فصل جلسة دقائق كحد أقصى.
390	Translated (100%)	Compliance and Adherence	الامتثال والالتزام
391	Translated (100%)	Al Hammadi Holding CEO shall ensure compliance with the cybersecurity policies and standards.	يضمن الرئيس التنفيذي لشركة الحمادي القابضة الامتثال لسياسات ومعايير الأمن السيبراني.
392	Translated (0%)	<2141>To ensure compliance, the Cybersecurity department will establish regular reporting by the Cybersecurity Manager, conduct periodic audits, or form a Cybersecurity </2141>Steering <2144>Committee for oversight.</2144>	لضمان الامتثال، ستقوم إدارة الأمن السيبراني بإعداد تقارير منتظمة<2141> من قبل مدير الأمن السيبراني، أو إجراء عمليات تدقيق دورية، أو تشكيل لجنة توجيهية للأمن السيبراني للإشراف.<2144>2144/> </2141>
393	Translated (100%)	The CS manager shall ensure adherence to this policy.	يتعين على مدير الأمن السيبراني ضمان الالتزام بهذه السياسة.
394	Translated (100%)	All employees of Al Hammadi Holding must adhere to this policy.	على جميع موظفي شركة الحمادي القابضة الالتزام بهذه السياسة.
395	Translated (100%)	Violations of this policy may result in legal action in any jurisdiction or other measures as deemed appropriate by the Al Hammadi Holding.	قد تؤدي انتهاكات هذه السياسة إلى اتخاذ إجراءات قانونية في أي ولاية قضائية أو غيرها من التدابير التي تراها شركة الحمادي القابضة مناسبة.
396	Translated (100%)	Exceptions	الاستثناءات
397	Translated (100%)	Violation of cybersecurity policies and standards is prohibited unless a prior justified exception is obtained from the Cybersecurity Department or the Cybersecurity Steering Committee.	يُحظر انتهاك سياسات ومعايير الأمن السيبراني ما لم يتم الحصول على استثناء مبرر مسبق من إدارة الأمن السيبراني أو اللجنة التوجيهية للأمن السيبراني.
398	Translated (100%)	In case of a conflict, applicable legislative and regulatory requirements overrule Al Hammadi Holding policies and standards.	في حالة وجود تعارض، فإن المتطلبات التشريعية والتنظيمية المعمول بها تسود على سياسات ومعايير شركة الحمادي القابضة.
399	Translated (99%)	Revision	المراجعة
400	Translated (100%)	This policy is reviewed annually, after major changes in Al Hammadi Holding's organizational chart or infrastructure, and more frequently whenever required, to ensure it remains appropriate and current for Al Hammadi Holding, ISO 27001, and NCA requirements.	تخضع هذه السياسة لمراجعة سنوية، ولإعادة التقييم بعد أي تغييرات جوهرية في الهيكل التنظيمي أو البنية التحتية لشركة الحمادي القابضة، إضافة إلى مراجعات دورية إضافية عند الضرورة، وذلك لضمان توافقها المستمر مع متطلبات شركة الحمادي القابضة، ومعيار آيزو ISO 27001:2022، وإرشادات الهيئة الوطنية للأمن السيبراني.
401	Translated (100%)	Approval Section	قسم الاعتماد
402	Translated	Prepared by:	إعداد:

	(99%)		
403	Translated (100%)	Mr. Mohammed Alamer	السيد/ محمد العامر
404	Translated (100%)	GRC Cybersecurity Specialist	أخصائي حوكمة ومخاطر وامتثال في الأمن السيبراني
405	Translated (100%)	Name	الاسم
406	Translated (99%)	Designation	المسمى الوظيفي
407	Translated (99%)	Signature	التوقيع
408	Translated (99%)	Date	التاريخ
409	Translated (99%)	Reviewed by:	:راجعها
410	Translated (100%)	Mr. Deepak Dasan	السيد/ ديباك داسان
411	Translated (100%)	IT Manager	مدير تكنولوجيا المعلومات
412	Translated (100%)	Name	الاسم
413	Translated (100%)	Designation	المسمى الوظيفي
414	Translated (100%)	Signature	التوقيع
415	Translated (100%)	Date	التاريخ
416	Translated (100%)	Reviewed by:	:راجعها
417	Translated (100%)	Mr. Majid Al Nahdi	السيد/ ماجد النهدي
418	Translated (100%)	HR Manager	مدير الموارد البشرية
419	Translated (100%)	Name	الاسم
420	Translated (100%)	Designation	المسمى الوظيفي
421	Translated (100%)	Signature	التوقيع

422	Translated (100%)	Date	التاريخ
423	Translated (100%)	Reviewed by:	راجعها:
424	Translated (100%)	Ms. Mashael Alotaibi	السيدة/ مشاعل العتيبي
425	Translated (100%)	<2269>Cybersecurity </2269>Manager	<مدير <2269>الأمن السيبراني</2269>
426	Translated (99%)	Name	الاسم
427	Translated (100%)	Designation	المسمى الوظيفي
428	Translated (100%)	Signature	التوقيع
429	Translated (100%)	Date	التاريخ
430	Translated (99%)	Approved by:	اعتمدها:
431	Translated (100%)	Dr. Abdulaziz Al Hammadi	الحمادي<Bold><Bold></Bold></Bold> د./ عبد العزيز<Bold><Bold></Bold></Bold>
432	Translated (99%)	Chief Operating Officer	الرئيس التنفيذي للعمليات
433	Translated (100%)	Name	الاسم
434	Translated (100%)	Designation	المسمى الوظيفي
435	Translated (100%)	Signature	التوقيع
436	Translated (100%)	Date	التاريخ
437	Translated (100%)	Approved by:	اعتمدها:
438	Translated (100%)	Mr. Mohammad AlHammadi	السيد/ محمد الحمادي
439	Translated (99%)	Chief Executive Officer	الرئيس التنفيذي
440	Translated (100%)	Name	الاسم
441	Translated	Designation	المسمى الوظيفي

	(100%)		
442	Translated (100%)	Signature	التوقيع
443	Translated (100%)	Date	التاريخ

Segment ID	Segment status	Source segment	Target segment
1	Translated (0%)	<9>Information Security Cryptography Policy </9><23/><27/>	<9>27></23><9/>سياسة تشفير أمن المعلومات
2	Translated (100%)	Page <41><32/> of <40/></41>	<41><32/>صفحة من <40/></41>
3	Translated (100%)	Al Hammadi Holding	شركة الحمادي القابضة
4	Translated (0%)	Information Security Cryptography Policy	سياسة التشفير في أمن المعلومات
5	Translated (100%)	CYBERSECURITY DEPARTMENT	إدارة الأمن السيبراني
6	Translated (100%)	Policy ID	معرّف السياسة
7	Translated (100%)	AHH-CS-ISMS-007	AHH-CS-ISMS-007
8	Translated (100%)	Class	الفئة
9	Translated (100%)	Internal Release	إصدار داخلي
10	Not Translated (0%)		
11	Translated (100%)	V3.0	V3.0
12	Translated (100%)	Published at	نُشرت في
13	Translated (100%)	April 2025	أبريل 2025
14	Translated (100%)	Document Owner	المسؤول عن المستند
15	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
16	Translated (100%)	Disclaimer	تنويه
17	Translated (100%)	The information contained in this document is property of Al Hammadi Holding and must not be copied or communicated to a third party or used for any purpose other than that for which it is supplied, without the written consent of Al Hammadi Holding.	المعلومات الواردة في هذا المستند هي ملك لشركة الحمادي القابضة ولا يجوز نسخها أو إبلاغها إلى طرف ثالث أو استخدامها لأي غرض آخر غير الغرض الذي تم توفيرها من أجله، دون موافقة خطية من شركة الحمادي القابضة.

18	Translated (100%)	Contents	جدول المحتويات
19	Translated (100%)	Document Control	ضبط المستندات
20	Translated (100%)	Document Information	معلومات المستند
21	Translated (100%)	Synopsis	الملخص
22	Translated (100%)	Document Title:	:عنوان المستند
23	Translated (100%)	Information Security Cryptography Policy	سياسة التشفير في أمن المعلومات
24	Translated (100%)	Document Status:	:حالة المستند
25	Translated (100%)	Approved	معتمد
26	Translated (100%)	Document Effective Date:	:تاريخ سريان المستند
27	Translated (100%)	April 2025	أبريل 2025
28	Translated (100%)	Document Issue Date:	:تاريخ إصدار المستند
29	Translated (100%)	April 2025	أبريل 2025
30	Translated (100%)	Document Next Revision Date:	:تاريخ المراجعة التالية للمستند
31	Translated (100%)	April <322>2026</322>	<أبريل <322>2026<322/>
32	Translated (100%)	Key contacts	جهات التواصل الرئيسية
33	Translated (100%)	Document Owner:	:المسؤول عن المستند
34	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
35	Translated (100%)	Approval Authority	جهة الاعتماد
36	Translated (100%)	Document Created by:	:مُنشئ المستند
37	Translated	IT Management	إدارة تكنولوجيا المعلومات

	(100%)		
38	Translated (100%)	Document Reviewed by:	:راجع المستند
39	Translated (0%)	Al Hammadi Holding CS & IT Managers	مديرو تكنولوجيا المعلومات والخدمات في شركة الحمادي القابضة
40	Translated (100%)	Document Approved by:	:اعتمد المستند
41	Translated (100%)	Al Hammadi Holding COO & CEO	الرئيس التنفيذي للعمليات والرئيس التنفيذي في شركة الحمادي القابضة
42	Translated (100%)	Note:	:ملاحظة
43	Translated (100%)	Any additional approval will be added in the document annex	تُضاف أي اعتمادات إضافية في ملحق المستند
44	Translated (100%)	Classification	التصنيف
45	Translated (100%)	<373>Company Internal – </373>to be shared with 3rd parties after consent of CS Manager	داخلي لاستخدام للشركة<373> – </373><373/>يُسمح بمشاركته<373> مع جهات خارجية بعد موافقة مدير إدارة الأمن السيبراني
46	Translated (100%)	Version / Dates	الإصدار / التواريخ
47	Translated (100%)	<388>Current Version</388>:	:<388>388/>الإصدار الحالي
48	Translated (100%)	V 3.0	V 3.0
49	Translated (100%)	Date Published:	:تاريخ النشر
50	Translated (100%)	April 2025	أبريل 2025
51	Translated (100%)	<400>Date of Next Review</400>:	:<400>400/>تاريخ المراجعة التالية
52	Translated (100%)	April 2026	أبريل 2026
53	Translated (100%)	<418>Prior Version</418>:	:<418>418/>الإصدار السابق
54	Translated (100%)	V 2.0	V 2.0
55	Translated (100%)	Prior Published:	:تاريخ النشر السابق
56	Translated (100%)	December 2023	ديسمبر 2023

57	Translated (100%)	Document Changes	التغييرات على المستند
58	Translated (100%)	Date	التاريخ
59	Translated (100%)	Version	الإصدار
60	Translated (100%)	Document Owner	المسؤول عن المستند
61	Translated (100%)	Change Description	وصف التغيير
62	Translated (100%)	Dec 2024	ديسمبر 2024
63	Translated (100%)	2.0	2.0
64	Translated (100%)	IT Management	إدارة تكنولوجيا المعلومات
65	Translated (0%)	01-Dec -2024	ديسمبر -2024- 01
66	Translated (100%)	April 2025	أبريل 2025
67	Translated (100%)	3.0	3.0
68	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
69	Translated (100%)	Document reviewed and updated based on NCA ECC-2:2024 and ISO27001:2022 requirements	تمت مراجعة المستند وتحديثه استنادًا إلى متطلبات الهيئة الوطنية للأمن السيبراني (NCA) المعيار ECC-2:2024 ومعيار آيزو ISO 27001:2022.
70	Translated (100%)	Document Circulation	تعميم المستند
71	Translated (100%)	To	إلى
72	Translated (100%)	Date	التاريخ
73	Translated (100%)	Method	الطريقة
74	Translated (100%)	IT Staff	موظفو تكنولوجيا المعلومات
75	Translated (100%)	April 2025	أبريل 2025
76	Translated	Intranet Portal	بوابة الإنترانت

	(100%)		
77	Translated (100%)	Objectives	الأهداف
78	Translated (0%)	The purpose of this policy is to set the principles and procedural implementation guidelines, by which Al Hammadi Holding shall ensure proper and effective use of cryptography to protect the confidentiality, integrity, and authenticity of transmitted and stored information, in compliance with the requirements specified in:	الغرض من هذه السياسة هو وضع المبادئ وإرشادات التنفيذ الإجرائية، والتي بموجبها تضمن شركة الحمادي القابضة الاستخدام السليم والفعال للتشفير لحماية سرية وسلامة وصحة المعلومات المنقولة والمخزنة، وفقًا للمتطلبات المحددة في:
79	Translated (100%)	ISO/IEC 27001 Annex-A:	الملحق أ ISO 27001:2022/معيار آيزو:
80	Translated (0%)	A.8.24 Use of cryptography.	A.8.24 استخدام التشفير.
81	Translated (100%)	NCA ECC-2:2024:	ECC-2:2024 معيار الهيئة الوطنية للأمن السيبراني رقم:
82	Translated (0%)	2-8 Cryptography	2-8 التشفير
83	Translated (100%)	Scope	النطاق
84	Translated (100%)	This policy is applicable to all Al Hammadi Holding ISMS information assets, security operations, and all persons doing work under Al Hammadi Holding control.	تنطبق هذه السياسة على جميع أصول معلومات نظام إدارة أمن المعلومات في شركة الحمادي القابضة والعمليات الأمنية وجميع الأشخاص الذين يعملون تحت إشراف شركة الحمادي القابضة.
85	Translated (100%)	This includes employees and contractors, contractors, suppliers, and 3rd Parties.	تشمل السياسة الموظفين والمتعاقدين والمقاولين والموردين والجهات الخارجية.
86	Translated (100%)	Roles and Responsibilities	الأدوار والمسؤوليات
87	Translated (100%)	Al Hammadi Holding Cybersecurity and IT Departments are responsible for maintaining this policy with all its contents, in accordance with any changes in the applicable regulations and legislation, where:	تتولى إدارات الأمن السيبراني وتكنولوجيا المعلومات في شركة الحمادي القابضة مسؤولية حفظ هذه السياسة بجميع محتوياتها، وفقًا لأي تغييرات تطرأ على اللوائح والتشريعات المعمول بها، وذلك وفقًا لما يلي:
88	Translated (100%)	Policy Review and Update:	مراجعة السياسة وتحديثها:
89	Translated (100%)	Cybersecurity Department.	إدارة الأمن السيبراني.
90	Translated (100%)	Policy Implementation and Enforcement:	تنفيذ السياسة وإنفاذها:
91	Translated (100%)	IT Department.	إدارة تكنولوجيا المعلومات.
92	Translated	Policy Compliance Measurement:	قياس الامتثال للسياسة:

	(100%)		
93	Translated (100%)	Cybersecurity Department.	إدارة الأمن السيبراني.
94	Translated (100%)	Principles	المبادئ
95	Translated (99%)	General	أحكام عامة
96	Translated (0%)	The use of cryptographic controls for information assets shall depend on conducting risk assessment taking into consideration the data classification level.	يعتمد استخدام ضوابط التشفير لأصول المعلومات على إجراء تقييم للمخاطر مع مراعاة مستوى تصنيف البيانات.
97	Translated (0%)	Al Hammadi Holding Data shall be encrypted while in transit state, processing and stored according to data classification and the policies and procedures of Al Hammadi Holding, and relevant legislative and regulatory requirements.	يجب تشفير بيانات شركة الحمادي القابضة أثناء وجودها في حالة العبور ومعالجتها وتخزينها وفقًا لتصنيف البيانات وسياسات وإجراءات شركة الحمادي القابضة والمتطلبات التشريعية والتنظيمية ذات الصلة.
98	Translated (0%)	Updated encryption algorithms, keys, and encoders must be used according to the announcements of the National Encryption Standards (NCS-1:2020) issued by NCA..	يجب استخدام خوارزميات التشفير المحدثة والمفاتيح والمشفرات وفقًا لإعلانات معايير التشفير الوطنية (NCS -1:2020) الصادرة عن NCA..
99	Translated (0%)	Strong cryptography and security protocols (such as SHA-1, MD5, SSL, etc.) to safeguard sensitive data shall be used during transmission over open or public networks as permissible by local laws taking the following into consideration:	يجب استخدام بروتوكولات التشفير والأمان القوية (مثل SHA -1 و MD5 و SSL وما إلى ذلك) لحماية البيانات الحساسة أثناء الإرسال عبر الشبكات المفتوحة أو العامة وفقًا لما تسمح به القوانين المحلية مع مراعاة ما يلي:
100	Translated (0%)	Only trusted keys and certificates are accepted.	يتم قبول المفاتيح والشهادات الموثوقة فقط.
101	Translated (0%)	The protocol in use only supports secure versions or configurations.	لا يدعم البروتوكول المستخدم سوى الإصدارات أو التكوينات الآمنة.
102	Translated (0%)	The encryption strength is appropriate for the encryption methodology in use.	قوة التشفير مناسبة لمنهجية التشفير المستخدمة.
103	Translated (0%)	All related critical systems' data shall be encrypted while in transit.	يجب تشفير جميع بيانات الأنظمة الحيوية ذات الصلة أثناء النقل.
104	Translated (0%)	All related critical systems' data shall be encrypted while at rest at the file and database level, or at the level of specific columns within the database.	يجب تشفير جميع بيانات الأنظمة الحرجة ذات الصلة أثناء الراحة على مستوى الملف وقاعدة البيانات، أو على مستوى أعمدة محددة داخل قاعدة البيانات.
105	Translated (0%)	The Key Management Infrastructure (KMI) roles and responsibilities shall be defined and documented the following roles at a minimum:	يجب تحديد أدوار ومسؤوليات البنية التحتية للإدارة الرئيسية وتوثيق الأدوار التالية كحد أدنى:
106	Translated (0%)	System administrator is responsible for protecting and monitoring the encryption keys.	مسؤول النظام مسؤول عن حماية ومراقبة مفاتيح التشفير.
107	Translated (0%)	Key custodians.	الأوصياء الرئيسيون.

108	Translated (0%)	Certification Authorities (CAs).	.(CAs) سلطات التصديق
109	Translated (0%)	Registration Authorities (RAs).	.(RAs) سلطات التسجيل
110	Translated (0%)	Wireless networks that are used to transmit sensitive data or connected to an information processing facility that handles sensitive data shall use industry best practices to implement strong encryption for authentication and transmission.	يجب على الشبكات اللاسلكية المستخدمة لنقل البيانات الحساسة أو المتصلة بمنشأة معالجة المعلومات التي تتعامل مع البيانات الحساسة استخدام أفضل ممارسات الصناعة لتنفيذ تشفير قوي للمصادقة والإرسال.
111	Translated (0%)	Encryption shall be used for all issued mobile devices, including laptops, and removable media storing confidential information.	يجب استخدام التشفير لجميع الأجهزة المحمولة الصادرة، بما في ذلك أجهزة الكمبيوتر المحمولة والوسائط القابلة للإزالة التي تخزن المعلومات السرية.
112	Translated (0%)	For service and systems that are hosted on the cloud, the encryption requirements shall be addressed.	بالنسبة للخدمة والأنظمة المستضافة على السحابة، يجب معالجة متطلبات التشفير.
113	Translated (0%)	Data and information transferred to or transferred from cloud services must be encrypted in accordance with relevant legislative and regulatory requirements.	يجب تشفير البيانات والمعلومات المنقولة إلى الخدمات السحابية أو المنقولة منها وفقًا للمتطلبات التشريعية والتنظيمية ذات الصلة.
114	Translated (0%)	The use of cryptographic controls shall be reviewed annually or if any significant change has been disclosed pertaining to the applied controls and apply mitigation controls wherever required.	يجب مراجعة استخدام ضوابط التشفير سنويًا أو في حالة الكشف عن أي تغيير كبير يتعلق بالضوابط المطبقة وتطبيق ضوابط التخفيف حيثما كان ذلك مطلوبًا.
115	Translated (0%)	Non-console administrative access shall be encrypted using strong cryptography.	يجب تشفير الوصول الإداري غير المرتبط بوحدة التحكم باستخدام تشفير قوي.
116	Translated (0%)	All encryption (including algorithms, software, modules, libraries, and other cryptographic components) must be inventoried, evaluated, and approved by Al Hammadi Holding cybersecurity prior to being used.	يجب جرد جميع التشفير (بما في ذلك الخوارزميات والبرامج والوحدات والمكتبات ومكونات التشفير الأخرى) وتقييمها والموافقة عليها من قبل الأمن السيبراني لشركة الحمادي القابضة قبل استخدامها.
117	Translated (0%)	Under no circumstances should proprietary or self-developed cryptographic algorithms be used to protect confidential information.	لا يجوز تحت أي ظرف من الظروف استخدام خوارزميات التشفير المملوكة أو المطورة ذاتيًا لحماية المعلومات السرية.
118	Translated (0%)	Al Hammadi Holding IT shall develop, maintain and distribute the approved encryption algorithms and cryptographic functions.	تقوم شركة الحمادي القابضة لتقنية المعلومات بتطوير وصيانة وتوزيع خوارزميات التشفير المعتمدة ووظائف التشفير.
119	Translated (0%)	Safe Use of Encryption	الاستخدام الآمن للتشفير
120	Translated (0%)	Encryption algorithms, libraries, modules, and other ciphering components shall be identified, documented, evaluated, and approved by the Cyber Security Department prior to applying it to Al Hammadi Holding.	يجب تحديد خوارزميات التشفير والمكتبات والوحدات ومكونات التشفير الأخرى وتوثيقها وتقييمها والموافقة عليها من قبل إدارة الأمن السيبراني قبل تطبيقها على شركة الحمادي القابضة.
121	Translated (0%)	Ensure that the cryptographic fundamentals used (such as symmetric algorithms and asymmetric algorithms) are applied based on the National Standards for Encryption (NCS-1:2020).	التأكد من تطبيق أساسيات التشفير المستخدمة (مثل الخوارزميات المتماثلة والخوارزميات غير المتماثلة) بناءً على المعايير الوطنية للتشفير (NCS - 1:2020).
122	Translated	The encryption algorithms developed internally are prohibited to	يحظر استخدام خوارزميات التشفير التي تم تطويرها داخليًا، وفقًا لدليل الترميز

	(0%)	be used, according to the OWASP coding guide and National Coding Standards (NCS-1:2020).	.(NCS -1:2020) ومعايير الترميز الوطنية OWASP
123	Translated (0%)	Secure verification (such as the use of public encryption keys, digital signatures, and digital certificates) shall be used to reduce cyber risks and in accordance with the cryptographic solutions approved in Al Hammadi Holding.	يجب استخدام التحقق الآمن (مثل استخدام مفاتيح التشفير العامة والتوقيعات الرقمية والشهادات الرقمية) للحد من المخاطر السيبرانية ووفقًا لحلول التشفير .المعتمدة في شركة الحمادي القابضة
124	Translated (0%)	Identity verification shall be used to transfer confidential data to external parties using Digital Certificates and in accordance with the data protection and information policy of Al Hammadi Holding.	يجب استخدام التحقق من الهوية لنقل البيانات السرية إلى أطراف خارجية باستخدام الشهادات الرقمية ووفقًا لسياسة حماية البيانات والمعلومات الخاصة .بالحمادي القابضة
125	Translated (0%)	Multi-Factor Authentication “MFA” shall be used to verify the user's access to critical systems according to the Access Management policy approved by Al Hammadi Holding.	للتحقق من وصول "MFA" يجب استخدام المصادقة متعددة العوامل المستخدم إلى الأنظمة الحيوية وفقًا لسياسة إدارة الوصول المعتمدة من قبل .شركة الحمادي القابضة
126	Translated (0%)	Encryption standards should be defined into two levels of strength of encryption standards, namely Moderate and Advanced, to ensure implementation flexibility and efficiency based on National Coding Standards (NCS-1:2020).	يجب تحديد معايير التشفير في مستويين من قوة معايير التشفير، وهما المعتدل (NCS - والمتقدم، لضمان مرونة التنفيذ وكفاءته بناءً على معايير الترميز الوطنية 1:2020).
127	Translated (0%)	Coding techniques used in the Industrial Control Systems (OT/ICS) network environment must be compatible with the National Coding Standard (NCS-1:2020).	يجب أن تكون تقنيات الترميز المستخدمة في بيئة شبكة أنظمة التحكم الصناعي .(NCS -1:2020) متوافقة مع معيار الترميز الوطني (OT/ICS)
128	Translated (0%)	Up-to-date and secure methods and algorithms for encryption must be used when creating, saving, transmitting, and over the entire network connection used to transmit data classified as confidential and highly confidential according to the Advanced level based on data cybersecurity controls (DCC-1:2021).	يجب استخدام طرق وخوارزميات حديثة وآمنة للتشفير عند إنشاء وحفظ وإرسال وعبر اتصال الشبكة بأكمله المستخدم لنقل البيانات المصنفة على أنها سرية وسرية للغاية وفقًا للمستوى المتقدم بناءً على ضوابط الأمن السيبراني .(DCC -1:2021) للبيانات
129	Translated (0%)	Up-to-date and secure methods and algorithms for encryption should be used when creating, saving, transmitting, and over the entire network connection used to transmit classified data restricted to the Moderate level based on data cybersecurity controls (DCC-1:2021).	يجب استخدام طرق وخوارزميات محدثة وآمنة للتشفير عند إنشاء وحفظ وإرسال وعبر اتصال الشبكة بأكمله المستخدم لنقل البيانات السرية المقيدة .(DCC -1:2021) بالمستوى المتوسط بناءً على ضوابط الأمن السيبراني للبيانات
130	Translated (0%)	Up-to-date and secure encryption methods and algorithms should be used over the entire network connection used for remote work according to the advanced level within the national encryption standards based on cybersecurity controls for remote work (TCC-1:2021).	يجب استخدام طرق وخوارزميات تشفير حديثة وآمنة عبر اتصال الشبكة بأكمله المستخدم للعمل عن بُعد وفقًا للمستوى المتقدم ضمن معايير التشفير الوطنية .(TCC -1:2021) بناءً على ضوابط الأمن السيبراني للعمل عن بُعد
131	Translated (0%)	Encryption designs and encryption methods (e.g. block cryptography methods, message authentication tokens (MAC), encryption and AEAD authentication (AEAD), etc.) should be used based on national encryption standards (NCS-1:2020).	،يجب استخدام تصميمات التشفير وطرق التشفير (مثل طرق تشفير الكتلة وما إلى ،(AEAD) AEAD والتشفير ومصادقة ،(MAC) ورموز مصادقة الرسائل .(NCS -1:2020) ذلك) بناءً على معايير التشفير الوطنية
132	Translated	Common encryption protocols	بروتوكولات التشفير الشائعة

	(0%)		
133	Translated (0%)	Encryption protocols such as IPSec and TLS should be ensured and considered based on the National Encryption Standards (NCS-1:2020).	والنظر فيها بناءً على TLS و IPSec يجب ضمان بروتوكولات التشفير مثل .(NCS -1:2020) معايير التشفير الوطنية
134	Translated (0%)	Acceptable versions must ensure that the protocols used in (secure telematics, Bluetooth, UMTS/LTE/5G, and WIFI) are used based on the National Encryption Standards (NCS-1:2020).	يجب أن تضمن الإصدارات المقبولة استخدام البروتوكولات المستخدمة في بناءً (WIFI و ،UMTS/LTE/5G الاتصالات المعلوماتية الآمنة، والبلوتوث، و) .(NCS -1:2020) على معايير التشفير الوطنية
135	Translated (0%)	Public Key Infrastructure	البنية التحتية للمفتاح العام
136	Translated (0%)	Ensure that certificate algorithms are used for Public Key Infrastructure (PKI) based on National Encryption Standards (NCS-1:2020).	بناءً (PKI) التأكد من استخدام خوارزميات الشهادة للبنية التحتية للمفتاح العام .(NCS -1:2020) على معايير التشفير الوطنية
137	Translated (0%)	The validity of the certificates used must be ensured based on the National Cryptographic Standards (NCS-1:2020).	(NCS يجب ضمان صحة الشهادات المستخدمة بناءً على معايير التشفير الوطنية .(1:2020-
138	Translated (0%)	The data and information used with the keys must be managed securely.	.يجب إدارة البيانات والمعلومات المستخدمة مع المفاتيح بشكل آمن
139	Translated (0%)	The roles and responsibilities related to the management of Public Key Infrastructure (PKI) should be limited to at least the following roles:	يجب أن تقتصر الأدوار والمسؤوليات المتعلقة بإدارة البنية التحتية للمفاتيح :على الأدوار التالية على الأقل (PKI) العامة
140	Translated (0%)	Keying Material Manager as cybersecurity manager.	.مدير المواد الرئيسي كمدير للأمن السيبراني
141	Translated (0%)	Cryptographic administrators are responsible for key protection (Key Custodians) and are only authorized to replace keys when needed.	مسؤولو التشفير مسؤولون عن حماية المفاتيح (أمناء الحفظ الرئيسيين) .ومصرح لهم فقط باستبدال المفاتيح عند الحاجة
142	Translated (0%)	Certification authorities "CAs"), so that they are reliable and secure.	.بحيث تكون موثوقة وآمنة ،("CAs" جهات التصديق
143	Translated (0%)	Registration authorities (RAs), so that they are reliable and secure.	.بحيث تكون موثوقة وآمنة ،(RAs) سلطات التسجيل
144	Translated (0%)	Managing Encryption Keys	إدارة مفاتيح التشفير
145	Translated (0%)	Key Lifecycle Management processes shall be maintained securely and ensured that they are used properly and effectively.	يجب الحفاظ على عمليات إدارة دورة الحياة الرئيسية بشكل آمن وضمان .استخدامها بشكل صحيح وفعال
146	Translated (0%)	Al Hammadi Holding IT shall document and implement procedures to protect encryption keys used to secure stored sensitive data against disclosure and misuse.	يجب على شركة الحمادي القابضة لتكنولوجيا المعلومات توثيق وتنفيذ إجراءات لحماية مفاتيح التشفير المستخدمة لتأمين البيانات الحساسة المخزنة .ضد الكشف وسوء الاستخدام
147	Translated (0%)	Al Hammadi Holding IT shall document and implement all key-management processes and procedures for cryptographic keys used for the encryption of sensitive data (i.e. cardholder data), including the following:	يجب على شركة الحمادي القابضة لتكنولوجيا المعلومات توثيق وتنفيذ جميع عمليات وإجراءات إدارة المفاتيح لمفاتيح التشفير المستخدمة لتشفير البيانات :الحساسة (أي بيانات حامل البطاقة)، بما في ذلك ما يلي

148	Translated (0%)	Generation of strong cryptographic keys.	.توليد مفاتيح تشفير قوية
149	Translated (0%)	Secure cryptographic key distribution.	.توزيع آمن لمفتاح التشفير
150	Translated (0%)	Secure cryptographic key storage.	.تخزين آمن لمفتاح التشفير
151	Translated (0%)	Cryptographic key changes for keys that have reached the end of their crypto period.	.تغييرات مفتاح التشفير للمفاتيح التي وصلت إلى نهاية فترة التشفير الخاصة بها
152	Translated (0%)	Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised.	سحب المفاتيح أو استبدالها (على سبيل المثال، الأرشفة و/أو إتلافها و/أو إلغائها) حسب الضرورة عندما يتم إضعاف سلامة المفتاح (على سبيل المثال، مغادرة موظف لديه معرفة بمكون مفتاح نص واضح)، أو يشتبه في تعرض المفاتيح للخطر.
153	Translated (0%)	Archived cryptographic keys should only be used for decryption/verification purposes.	.يجب استخدام مفاتيح التشفير المؤرشفة فقط لأغراض فك التشفير/التحقق
154	Translated (0%)	Digital certificates shall be issued by the internal certification authority in Al Hammadi Holding or by a trusted external authority.	يتم إصدار الشهادات الرقمية من قبل جهة التصديق الداخلية في شركة الحمادي القابضة أو من قبل جهة خارجية موثوق بها.
155	Translated (0%)	The private keys shall be kept safe and secure (especially if it is used for digital signatures), and prevent unauthorized access, including certification bodies.	يجب الحفاظ على المفاتيح الخاصة آمنة ومأمونة (خاصة إذا تم استخدامها للتوقيعات الرقمية)، ومنع الوصول غير المصرح به، بما في ذلك هيئات التصديق.
156	Translated (0%)	Technologies of Tamper Resistant Safe shall be provided.	.يجب توفير تقنيات الخزنة المقاومة للعبث
157	Translated (0%)	The Private Key shall be protected by a password and/or by storing it on a secure medium and in accordance with the approved cryptographic procedures.	يجب حماية المفتاح الخاص بكلمة مرور و/أو عن طريق تخزينه على وسيط آمن ووفقًا لإجراءات التشفير المعتمدة.
158	Translated (0%)	Private encryption keys shall be classified as "highly confidential" in accordance with the data classification policy of Al Hammadi Holding.	يجب تصنيف مفاتيح التشفير الخاصة على أنها "سرية للغاية" وفقًا لسياسة تصنيف البيانات الخاصة بالحمادي القابضة.
159	Translated (0%)	Event logs shall be activated for cryptographic key management and monitored periodically.	.يجب تفعيل سجلات الأحداث لإدارة مفاتيح التشفير ومراقبتها بشكل دوري
160	Translated (0%)	The Duration to use the cipher keys shall be specified, along with the starting date, and the expiry date for each key.	يجب تحديد مدة استخدام مفاتيح التشفير، إلى جانب تاريخ البدء وتاريخ انتهاء الصلاحية لكل مفتاح.
161	Translated (0%)	Encryption keys shall be renewed before expiry.	.يجب تجديد مفاتيح التشفير قبل انتهاء صلاحيتها
162	Translated (0%)	Certificate Revocation List shall be used to prevent the use of expired certificates or being subjected to a security violation, to ensure they are not used in future transactions.	يجب استخدام قائمة إلغاء الشهادات لمنع استخدام الشهادات منتهية الصلاحية أو التعرض لانتهاك أمني، لضمان عدم استخدامها في المعاملات المستقبلية.
163	Translated (0%)	If the private keys by Al Hammadi Holding was subjected to a security violation or if a key is not available (due to damage to the	إذا تعرضت المفاتيح الخاصة من قبل شركة الحمادي القابضة لمخالفة أمنية أو إذا لم يكن المفتاح متاحًا (بسبب تلف وسائط التخزين الرئيسية)، فيجب إبلاغ

		key storage media), the certification authority shall be informed immediately to cancel it and re-issue the encryption Private Key.	.جهة التصديق على الفور بإلغائه وإعادة إصدار المفتاح الخاص للتشفير
164	Translated (0%)	The certification authority shall be obligated, if the private keys being subjected to a security violation, to inform Al Hammadi Holding, cancel all certificates immediately, and replace the key for the authority issuing the certificates.	تلتزم الجهة المصدقة في حالة تعرض المفاتيح الخاصة لمخالفة أمنية بإبلاغ شركة الحمادي القابضة وإلغاء جميع الشهادات على الفور واستبدال مفتاح .الجهة المصدرة للشهادات
165	Translated (0%)	In case that the keys cannot be exchanged safely and securely over the network, the encryption keys shall be transferred using out-of-band alternative channels.	في حالة تعذر تبادل المفاتيح بأمان وأمان عبر الشبكة، يجب نقل مفاتيح التشفير .باستخدام قنوات بديلة خارج النطاق
166	Translated (0%)	The requirements for the length of ciphers shall be reviewed and updated based on the latest relevant technical updates at least once a year and in accordance with national encryption standards.	يجب مراجعة متطلبات طول الأصفار وتحديثها بناءً على آخر التحديثات الفنية .ذات الصلة مرة واحدة على الأقل في السنة ووفقًا لمعايير التشفير الوطنية
167	Translated (0%)	Key Custodians are responsible for protecting the ciphers and the only authorized to replace cryptographic keys when needed.	أمناء الحفظ الرئيسيون مسؤولون عن حماية الشفرات والوحيدون المصرح لهم .باستبدال مفاتيح التشفير عند الحاجة
168	Translated (0%)	It is forbidden to store cryptographic keys on the main memory or on the same systems to which encryption is applied.	يحظر تخزين مفاتيح التشفير على الذاكرة الرئيسية أو على نفس الأنظمة التي يتم .تطبيق التشفير عليها
169	Translated (0%)	Instead, it is recommended to store them on Peripheral Hardware Devices, such as Hardware Security Modules (HSM), Key Loaders, or other devices designated for this purpose.	بدلًا من ذلك، يوصى بتخزينها على أجهزة الأجهزة الطرفية، مثل وحدات أمان .أو اللوادر الرئيسية أو الأجهزة الأخرى المخصصة لهذا الغرض (HSM) الأجهزة
170	Translated (0%)	If manual clear-text cryptographic key-management operations are used, these operations shall be managed using split knowledge and dual control.	في حالة استخدام عمليات إدارة مفاتيح التشفير اليدوي للنص الواضح، يجب .إدارة هذه العمليات باستخدام المعرفة المقسمة والتحكم المزدوج
171	Translated (100%)	Note:	:ملاحظة
172	Translated (0%)	Examples of manual key-management operations include, but are not limited to key generation, transmission, loading, storage and destruction.	تشمل أمثلة عمليات إدارة المفاتيح اليدوية، على سبيل المثال لا الحصر، توليد .المفاتيح ونقلها وتحميلها وتخزينها وتدميرها
173	Translated (0%)	Prevention of unauthorized substitution of cryptographic keys	منع الاستبدال غير المصرح به لمفاتيح التشفير
174	Translated (0%)	Requirement for cryptographic key custodians to acknowledge that they understand and accept their key-custodian responsibilities.	إلزام أمناء الحفظ الرئيسيين للتشفير بالإقرار بأنهم يفهمون ويقبلون مسؤولياتهم .الرئيسية
175	Translated (0%)	All encryption key recovery passwords shall be protected by strong access controls, stored in the fewest possible locations, and restricted to those who have a need to access them.	يجب حماية جميع كلمات مرور استعادة مفتاح التشفير من خلال عناصر تحكم قوية في الوصول، وتخزينها في أقل عدد ممكن من المواقع، وتقتصر على أولئك .الذين يحتاجون إلى الوصول إليها
176	Translated (0%)	All access to key recovery passwords shall be recorded and monitored.	يجب تسجيل جميع عمليات الوصول إلى كلمات مرور الاسترداد الرئيسية .ومراقبتها
177	Translated (0%)	Cryptographic private or shared keys, cryptographic secrets, or authentication secrets or hashes will be classified at the highest classification level.	سيتم تصنيف مفاتيح التشفير الخاصة أو المشتركة أو أسرار التشفير أو أسرار .المصادقة أو التجزئة على أعلى مستوى تصنيف

178	Translated (0%)	The keys and relevant encryption certificates should be stored in a separate external media and one copy should be kept at an offsite location.	يجب تخزين المفاتيح وشهادات التشفير ذات الصلة في وسائط خارجية منفصلة ويجب الاحتفاظ بنسخة واحدة في موقع خارج الموقع.
179	Translated (0%)	Clear text encryption keys and their associated data shall not reside on the same device or system.	يجب ألا توجد مفاتيح تشفير النص الواضحة والبيانات المرتبطة بها على نفس الجهاز أو النظام.
180	Translated (0%)	The use of hard coded encryption keys or default encryption keys shall not be allowed.	لا يُسمح باستخدام مفاتيح التشفير المشفرة أو مفاتيح التشفير الافتراضية.
181	Translated (100%)	Other Requirements	متطلبات أخرى
182	Translated (0%)	The KPI shall be used to ensure the continuous improvement of the effective use of cryptographic.	يجب استخدام مؤشر الأداء الرئيسي لضمان التحسين المستمر للاستخدام الفعال للتشفير.
183	Translated (0%)	All cybersecurity requirements for encryption shall be reviewed periodically.	يجب مراجعة جميع متطلبات الأمن السيبراني للتشفير بشكل دوري.
184	Translated (0%)	This policy shall be reviewed once a year; at least.	يجب مراجعة هذه السياسة مرة واحدة في السنة؛ على الأقل.
185	Translated (100%)	Compliance and Adherence	الامتثال والالتزام
186	Translated (100%)	Al Hammadi Holding CEO shall ensure compliance with the cybersecurity policies and standards.	يضمن الرئيس التنفيذي لشركة الحمادي القابضة الامتثال لسياسات ومعايير الأمن السيبراني.
187	Translated (100%)	To ensure compliance, the Cybersecurity department will establish regular reporting by the Cybersecurity Manager, conduct periodic audits, or form a Cybersecurity Committee for oversight.	لضمان الامتثال، سينشئ قسم الأمن السيبراني نظامًا لتقديم تقارير منتظمة يُعدّها مدير الأمن السيبراني، ويجري عمليات تدقيق دورية، أو يشكل لجنة للأمن السيبراني للإشراف.
188	Translated (100%)	The CS manager shall ensure adherence to this policy.	يتعين على مدير الأمن السيبراني ضمان الالتزام بهذه السياسة.
189	Translated (100%)	All employees of Al Hammadi Holding must adhere to this policy.	على جميع موظفي شركة الحمادي القابضة الالتزام بهذه السياسة.
190	Translated (100%)	Violations of this policy may result in legal action in any jurisdiction or other measures as deemed appropriate by the Al Hammadi Holding.	قد تؤدي انتهاكات هذه السياسة إلى اتخاذ إجراءات قانونية في أي ولاية قضائية أو غيرها من التدابير التي تراها شركة الحمادي القابضة مناسبة.
191	Translated (100%)	Exceptions	الاستثناءات
192	Translated (100%)	Violation of cybersecurity policies and standards is prohibited unless a prior justified exception is obtained from the Cybersecurity Department or the Cybersecurity Steering Committee.	يُحظر انتهاك سياسات ومعايير الأمن السيبراني ما لم يتم الحصول على استثناء مبرر مسبق من إدارة الأمن السيبراني أو اللجنة التوجيهية للأمن السيبراني.
193	Translated (100%)	In case of a conflict, applicable legislative and regulatory requirements overrule Al Hammadi Holding policies and standards.	في حالة وجود تعارض، فإن المتطلبات التشريعية والتنظيمية المعمول بها تسود على سياسات ومعايير شركة الحمادي القابضة.
194	Translated (100%)	Revision	المراجعة

195	Translated (100%)	This policy is reviewed annually, after major changes in Al Hammadi Holding's organizational chart or infrastructure, and more frequently whenever required, to ensure it remains appropriate and current for Al Hammadi Holding, ISO 27001, and NCA requirements.	تخضع هذه السياسة لمراجعة سنوية، ولإعادة التقييم بعد أي تغييرات جوهرية في الهيكل التنظيمي أو البنية التحتية لشركة الحمادي القابضة، إضافة إلى مراجعات دورية إضافية عند الضرورة، وذلك لضمان توافقها المستمر مع متطلبات شركة الحمادي القابضة، ومعيار آيزو ISO 27001:2022، وإرشادات الهيئة الوطنية للأمن السيبراني.
196	Translated (100%)	Approval Section	قسم الاعتماد
197	Translated (100%)	Prepared by:	إعداد:
198	Translated (100%)	Mr. Mohammed Alamer	السيد/ محمد العامر
199	Translated (100%)	GRC Cybersecurity Specialist	أخصائي حوكمة ومخاطر وامتثال في الأمن السيبراني
200	Translated (100%)	Name	الاسم
201	Translated (100%)	Designation	المسمى الوظيفي
202	Translated (100%)	Signature	التوقيع
203	Translated (100%)	Date	التاريخ
204	Translated (100%)	Reviewed by:	راجعها:
205	Translated (100%)	Mr. Deepak Dasan	السيد/ ديباك داسان
206	Translated (100%)	IT Manager	مدير تكنولوجيا المعلومات
207	Translated (100%)	Name	الاسم
208	Translated (100%)	Designation	المسمى الوظيفي
209	Translated (100%)	Signature	التوقيع
210	Translated (100%)	Date	التاريخ
211	Translated (100%)	Reviewed by:	راجعها:
212	Translated (100%)	Ms. Mashael Alotaibi	السيدة/ مشاعل العتيبي

213	Translated (100%)	<1252>Cybersecurity </1252>Manager	<مدير <1252>الأمن السيبراني</1252>
214	Translated (100%)	Name	الاسم
215	Translated (100%)	Designation	المسمى الوظيفي
216	Translated (100%)	Signature	التوقيع
217	Translated (100%)	Date	التاريخ
218	Translated (100%)	Approved by:	:اعتمدها
219	Translated (100%)	Dr. Abdulaziz Al Hammadi	<Bold><Bold>د./ عبد العزيز</Bold></Bold>الحمادي <Bold><Bold></Bold></Bold>
220	Translated (100%)	Chief Operating Officer	الرئيس التنفيذي للعمليات
221	Translated (100%)	Name	الاسم
222	Translated (100%)	Designation	المسمى الوظيفي
223	Translated (100%)	Signature	التوقيع
224	Translated (100%)	Date	التاريخ
225	Translated (100%)	Approved by:	:اعتمدها
226	Translated (100%)	Mr. Mohammad AlHammadi	السيد/ محمد الحمادي
227	Translated (100%)	Chief Executive Officer	الرئيس التنفيذي
228	Translated (100%)	Name	الاسم
229	Translated (100%)	Designation	المسمى الوظيفي
230	Translated (100%)	Signature	التوقيع
231	Translated (100%)	Date	التاريخ

Segment ID	Segment status	Source segment	Target segment
1	Translated (0%)	Sample Copy	نسخة نموذجية
2	Translated (0%)	<7/><11/><18><14> </14><17>Information Security Operations <22/>Policy</17></18>	سياسة عمليات <22/>أمن المعلومات<17><14> </14><11/><7/> </17></18>
3	Translated (100%)	Sample Copy	نسخة نموذجية
4	Translated (0%)	Page <43><34/> of <42/></43>	<صفحة <43><34/> من <42/></43>
5	Translated (0%)	Al Hammadi Holding	شركة الحمادي القابضة
6	Translated (0%)	Information Security Operations Management Policy	سياسة إدارة عمليات أمن المعلومات
7	Translated (0%)	CYBERSECURITY DEPARTMENT	إدارة الأمن السيبراني
8	Translated (0%)	Policy ID	معرّف السياسة
9	Translated (100%)	AHH-CS-ISMS-008	AHH-CS-ISMS-008
10	Translated (100%)	Class	الفئة
11	Translated (0%)	Internal Release	إصدار داخلي
12	Not Translated (0%)		
13	Translated (100%)	V3.1	V3.1
14	Translated (100%)	Published at	نُشرت في
15	Translated (100%)	April 2025	أبريل 2025
16	Translated (100%)	Document Owner	المسؤول عن المستند
17	Translated (0%)	Cybersecurity Department	إدارة الأمن السيبراني
18	Translated (100%)	Disclaimer	تنويه

19	Translated (0%)	The information contained in this document is property of Al Hammadi Holding and must not be copied or communicated to a third party or used for any purpose other than that for which it is supplied, without the written consent of Al Hammadi Holding.	المعلومات الواردة في هذا المستند هي ملك لشركة الحمادي القابضة ولا يجوز نسخها أو إبلاغها إلى طرف ثالث أو استخدامها لأي غرض آخر غير الغرض الذي تم توفيرها من أجله، دون موافقة خطية من شركة الحمادي القابضة.
20	Translated (100%)	Contents	جدول المحتويات
21	Translated (0%)	Document Control	ضبط المستندات
22	Translated (100%)	Document Information	معلومات المستند
23	Translated (100%)	Synopsis	الملخص
24	Translated (100%)	Document Title:	عنوان المستند:
25	Translated (0%)	Information Security Operations Policy	سياسة عمليات أمن المعلومات
26	Translated (0%)	Document Status:	حالة المستند:
27	Translated (99%)	Approved	معتمد
28	Translated (0%)	Document Effective Date:	تاريخ سريان المستند:
29	Translated (100%)	April 2025	أبريل 2025
30	Translated (0%)	Document Issue Date:	تاريخ إصدار المستند:
31	Translated (100%)	April 2025	أبريل 2025
32	Translated (0%)	Document Next Revision Date:	تاريخ المراجعة التالية للمستند:
33	Translated (0%)	April <356>2026</356>	أبريل <356>2026<356/>
34	Translated (0%)	Key contacts	جهات التواصل الرئيسية
35	Translated (99%)	Document Owner:	المسؤول عن المستند:
36	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
37	Translated	Approval Authority	جهة الاعتماد

	(100%)		
38	Translated (0%)	Document Created by:	:مُنشئ المستند
39	Translated (0%)	IT Management	إدارة تكنولوجيا المعلومات
40	Translated (0%)	Document Reviewed by:	:راجع المستند
41	Translated (0%)	Al Hammadi Holding CS&IT Managers	مديرو الأمن السيبراني وتكنولوجيا المعلومات في شركة الحمادي القابضة
42	Translated (0%)	Document Approved by:	:اعتمد المستند
43	Translated (0%)	Al Hammadi Holding COO & CEO	الرئيس التنفيذي للعمليات والرئيس التنفيذي في شركة الحمادي القابضة
44	Translated (99%)	Note:	:ملاحظة
45	Translated (0%)	Any additional approval will be added in the document annex	تُضاف أي اعتمادات إضافية في ملحق المستند
46	Translated (99%)	Classification	التصنيف
47	Translated (0%)	Company Internal – to be shared with 3rd parties after consent of CS Manager	داخلي لاستخدام للشركة – يُسمح بمشاركته مع جهات خارجية بعد موافقة مدير إدارة الأمن السيبراني
48	Translated (0%)	Version / Dates	الإصدار / التواريخ
49	Translated (0%)	Current Version:	:الإصدار الحالي
50	Translated (100%)	V3.1	V3.1
51	Translated (0%)	Date Published:	:تاريخ النشر
52	Translated (100%)	April 2025	أبريل 2025
53	Translated (0%)	Date of Next Review:	:تاريخ المراجعة التالية
54	Translated (100%)	April 2026	أبريل 2026
55	Translated (0%)	Prior Version:	:الإصدار السابق
56	Translated (100%)	V3.0	V3.0

57	Translated (0%)	Prior Published:	تاريخ النشر السابق:
58	Translated (99%)	December 2023	ديسمبر 2023
59	Translated (0%)	Document Changes	التغييرات على المستند
60	Translated (100%)	Date	التاريخ
61	Translated (99%)	Version	الإصدار
62	Translated (100%)	Document Owner	المسؤول عن المستند
63	Translated (0%)	Change Description	وصف التغيير
64	Translated (0%)	<497>December </497>2024	ديسمبر <497/>2024<497>
65	Translated (0%)	3.0	3.0
66	Translated (100%)	IT Management	إدارة تكنولوجيا المعلومات
67	Translated (0%)	Updated policy number to	تحديث رقم السياسة إلى
68	Translated (100%)	AHH-IT-ISMS-009	AHH-IT-ISMS-009
69	Translated (100%)	April 2025	أبريل 2025
70	Translated (100%)	3.1	3.1
71	Translated (0%)	CS Department	قسم خدمات العملاء
72	Translated (0%)	Document reviewed and updated based on NCA ECC-2:2024 and ISO27001:2022 requirements	تمت مراجعة المستند وتحديثه استنادًا إلى متطلبات الهيئة الوطنية للأمن السيبراني (NCA) المعيار ECC-2:2024 ومعيار آيزو ISO 27001:2022.
73	Translated (0%)	Document Circulation	تعميم المستند
74	Translated (99%)	To	إلى
75	Translated (100%)	Date	التاريخ
76	Translated	Method	الطريقة

	(100%)		
77	Translated (0%)	IT Staff	موظفو تكنولوجيا المعلومات
78	Translated (100%)	April 2025	أبريل 2025
79	Translated (0%)	Intranet Portal	بوابة الإنترانت
80	Translated (99%)	Objectives	الأهداف
81	Translated (0%)	The purpose of this policy is to set the principles and procedural implementation guidelines, by which Al Hammadi Holding shall manage and control its critical information assets to ensure its protection and continuous availability against possible threats, unauthorized use, and unplanned outages, in compliance with the requirements specified in:	الغرض من هذه السياسة هو وضع المبادئ وإرشادات التنفيذ الإجرائية، والتي بموجبها تقوم شركة الحمادي القابضة بإدارة أصول المعلومات الهامة الخاصة بها والتحكم فيها لضمان حمايتها وتوافرها المستمر ضد التهديدات المحتملة والاستخدام غير المصرح به والانقطاعات غير المخطط لها، وفقًا للمتطلبات المحددة في:
82	Translated (0%)	ISO/IEC 27001 Annex-A:	الملحق أ ISO 27001:2022/معيار آيزو:
83	Translated (0%)	A.5.37 Documented operating procedures, A.8.6 Capacity management, A.8.7 Protection against malware,A.8.8 Management of technical vulnerabilities, A.8.9 Configuration management, A.8.10 Information deletion, A.8.15 Logging, A.8.16 Monitoring activities, A.8.17 Clock synchronization, A.8.19 Installation of software on operational systems, A.8.31 Separation of development, test and production environments, A.8.32 Change management	أ .5.37 إجراءات التشغيل الموثقة، أ .8.6 إدارة السعة، أ .8.7 الحماية من البرامج الضارة، أ .8.8 إدارة الثغرات الفنية، أ .8.9 إدارة التكوين، أ .8.10 حذف المعلومات، أ .8.15 التسجيل، أ .8.16 أنشطة المراقبة، أ .8.17 مزامنة الساعة، أ .8.19 تثبيت البرامج على الأنظمة التشغيلية، أ .8.31 الفصل بين بيئات التطوير والاختبار والإنتاج، أ .8.32 إدارة التغيير
84	Translated (0%)	NCA ECC-2:2024:	معيار الهيئة الوطنية للأمن السيبراني رقم ECC-2:2024:
85	Translated (0%)	2-9 Backup and Recovery Management, 2-10 Vulnerability Management, 2-11 Penetration Testing, 2-12 Cybersecurity Event Logs and Monitoring Management	إدارة النسخ الاحتياطي والاسترداد، 2-10 إدارة الثغرات الأمنية، 2-11 2-9 اختبار الاختراق، 2-12 سجلات أحداث الأمن السيبراني وإدارة المراقبة
86	Translated (99%)	Scope	النطاق
87	Translated (0%)	This policy is applicable to all Al Hammadi Holding ISMS information assets, security operations, and all persons working under Al Hammadi Holding control.	تنطبق هذه السياسة على جميع أصول معلومات نظام إدارة أمن المعلومات في شركة الحمادي القابضة والعمليات الأمنية وجميع الأشخاص الذين يعملون تحت سيطرة شركة الحمادي القابضة.
88	Translated (0%)	This includes employees and contractors, suppliers, and 3rd Parties.	تشمل السياسة الموظفين والمتعاقدين والموردين والجهات الخارجية.
89	Translated (100%)	Roles and Responsibilities	الأدوار والمسؤوليات

90	Translated (0%)	Al Hammadi Holding Cybersecurity and IT Departments are responsible for maintaining this policy with all its contents, in accordance with any changes in the applicable regulations and legislation, where:	تتولى إدارات الأمن السيبراني وتكنولوجيا المعلومات في شركة الحمادي القابضة مسؤولية حفظ هذه السياسة بجميع محتوياتها، وفقًا لأي تغييرات تطرأ على اللوائح والتشريعات المعمول بها، وذلك وفقًا لما يلي:
91	Translated (0%)	Policy Review and Update:	مراجعة السياسة وتحديثها:
92	Translated (0%)	Cybersecurity Department.	إدارة الأمن السيبراني.
93	Translated (0%)	Policy Implementation and Enforcement:	تنفيذ السياسة وإنفاذها:
94	Translated (0%)	IT Department.	إدارة تكنولوجيا المعلومات.
95	Translated (0%)	Policy Compliance Measurement:	قياس الامتثال للسياسة:
96	Translated (100%)	Cybersecurity Department.	إدارة الأمن السيبراني.
97	Translated (100%)	Operational procedures and responsibilities	الإجراءات التشغيلية والمسؤوليات
98	Translated (0%)	Documented operating procedures	إجراءات التشغيل الموثقة
99	Translated (0%)	Al Hammadi Holding Operating procedures shall be documented and made appropriately available to all Al Hammadi Holding users.	يجب توثيق إجراءات تشغيل شركة الحمادي القابضة وإتاحتها بشكل مناسب لجميع مستخدمي شركة الحمادي القابضة.
100	Translated (0%)	Documented procedures shall be prepared for operational IT Department activities such as computer start-up and close-down procedures, and backup.	يجب إعداد إجراءات موثقة لأنشطة إدارة تكنولوجيا المعلومات التشغيلية مثل إجراءات بدء تشغيل الكمبيوتر وإغلاقه والنسخ الاحتياطي.
101	Translated (0%)	Al Hammadi Holding operating procedures shall specify instructions, including:	يجب أن تحدد إجراءات تشغيل شركة الحمادي القابضة التعليمات، بما في ذلك:
102	Translated (0%)	installation and configuration.	التثبيت والتكوين.
103	Translated (0%)	scheduling interdependencies with other systems.	جدولة الترابط مع الأنظمة الأخرى.
104	Translated (0%)	earliest job start & latest completion times.	أقرب وقت لبدء العمل وأحدث أوقات الإنجاز.
105	Translated (0%)	instructions for handling errors or exceptional conditions.	تعليمات للتعامل مع الأخطاء أو الظروف الاستثنائية.
106	Translated (0%)	support and escalation contacts, internal and external.	جهات اتصال الدعم والتصعيد، الداخلية والخارجية.
107	Translated (0%)	restart and recovery procedures for use in the event of failure.	إجراءات إعادة التشغيل والاسترداد للاستخدام في حالة الفشل.

108	Translated (0%)	audit-trail, system log information, and monitoring procedures.	.مسار التدقيق ومعلومات سجل النظام وإجراءات المراقبة
109	Translated (100%)	Change management	إدارة التغيير
110	Translated (0%)	Al Hammadi Holding changes to business processes, information processing facilities and systems that affect information security must be controlled by implementing the following:	يجب التحكم في تغييرات شركة الحمادي القابضة على العمليات التجارية ومرافق معالجة المعلومات والأنظمة التي تؤثر على أمن المعلومات من خلال تنفيذ ما يلي:
111	Translated (0%)	Vulnerability and risk assessment and remediation will be performed prior to deployment of all the changes except standard changes.	سيتم إجراء تقييم نقاط الضعف والمخاطر ومعالجتها قبل نشر جميع التغييرات باستثناء التغييرات القياسية.
112	Translated (0%)	identification and recording of significant changes.	.تحديد وتسجيل التغييرات الهامة
113	Translated (0%)	planning and testing of changes.	.تخطيط واختبار التغييرات
114	Translated (0%)	Assessment of potential impacts, including security impacts of changes.	.تقييم الآثار المحتملة، بما في ذلك الآثار الأمنية للتغييرات
115	Translated (0%)	formal approval procedure for proposed changes.	.إجراءات الموافقة الرسمية على التغييرات المقترحة
116	Translated (0%)	Verification of fulfillment of information security requirements.	.التحقق من استيفاء متطلبات أمن المعلومات
117	Translated (0%)	Communication of change details to all relevant parties.	.إبلاغ جميع الأطراف ذات الصلة بتفاصيل التغيير
118	Translated (0%)	fallback procedures for aborting and recovering unsuccessful changes.	.إجراءات احتياطية لإجهاض واستعادة التغييرات غير الناجحة
119	Translated (0%)	Provision of an emergency change process.	.توفير عملية تغيير طارئة
120	Translated (0%)	Formal responsibilities must be in place to ensure control of all changes.	.يجب أن تكون المسؤوليات الرسمية قائمة لضمان السيطرة على جميع التغييرات
121	Translated (0%)	When changes are made, an audit log containing all relevant information must be retained.	عند إجراء تغييرات، يجب الاحتفاظ بسجل تدقيق يحتوي على جميع المعلومات ذات الصلة.
122	Translated (0%)	Conducting a configurations' review, secure configuration and hardening and patching before changes or going live for technology projects.	إجراء مراجعة للتكوينات وتأمين التكوين والتصلب والتصحيح قبل التغييرات أو بدء التشغيل المباشر لمشاريع التكنولوجيا.
123	Translated (0%)	All change requests shall be classified in terms of benefits, urgency, effort required and potential impact on operations.	يجب تصنيف جميع طلبات التغيير من حيث الفوائد والإلحاح والجهد المطلوب والتأثير المحتمل على العمليات.
124	Translated (0%)	Any changes that are minor or low risk in nature shall not require to go through the formal change management process.	لا تتطلب أي تغييرات طفيفة أو منخفضة المخاطر بطبيعتها المرور بعملية إدارة التغيير الرسمية.
125	Translated (0%)	Al Hammadi Holding IT team is required to define the list of such changes and keep record of them.	يُطلب من فريق تكنولوجيا المعلومات في شركة الحمادي القابضة تحديد قائمة هذه التغييرات والاحتفاظ بسجل لها.

126	Translated (0%)	Emergency changes shall be followed for changes which are urgently required in order to resolve a major incident or problem.	يجب اتباع التغييرات الطارئة للتغييرات المطلوبة بشكل عاجل من أجل حل حادث أو مشكلة كبيرة.
127	Translated (0%)	These will be fast-tracked through the change management process and given additional resources where required.	سيتم تسريع هذه الإجراءات من خلال عملية إدارة التغيير وإعطاء موارد إضافية عند الاقتضاء.
128	Translated (0%)	Changes shall be assessed from both technical and business risk perspectives.	يجب تقييم التغييرات من منظور كل من المخاطر الفنية ومخاطر الأعمال.
129	Translated (0%)	Change initiators shall not assess their own changes and where possible the assessor(s) of a change shall be different from the approver(s).	لا يجوز لمبادري التغيير تقييم التغييرات الخاصة بهم، وحيثما أمكن، يجب أن يكون مقيّم(مقيّمي) التغيير مختلفًا عن المعتمد(المعتمدين).
130	Translated (0%)	The processes for change, configuration, release and deployment management shall be integrated together to ensure proper alignment and implementation.	يجب دمج عمليات إدارة التغيير والتكوين والإصدار والنشر معًا لضمان المواءمة والتنفيذ المناسبين.
131	Translated (0%)	All changes shall be recorded and tracked centrally.	يجب تسجيل جميع التغييرات وتتبعها مركزيًا.
132	Translated (0%)	The Head of the Cybersecurity Department and IT Department will be responsible for reviewing and approving all the level 2 – minor and level 3 – standard changes.	سيكون رئيس قسم الأمن السيبراني وقسم تكنولوجيا المعلومات مسؤولًا عن مراجعة واعتماد جميع التغييرات القياسية من المستوى 2 – التغييرات الثانوية والمستوى 3 – التغييرات القياسية.
133	Translated (0%)	Chief Executive Officer shall approve the changes if cost is involved.	يجب على الرئيس التنفيذي الموافقة على التغييرات إذا كانت التكلفة متضمنة.
134	Translated (0%)	All changes will be categorized based on the following criteria:	سيتم تصنيف جميع التغييرات بناءً على المعايير التالية:
135	Translated (0%)	Category of Changes	فئة التغييرات
136	Translated (0%)	Examples of Application Changes	أمثلة على تغييرات التطبيق
137	Translated (0%)	Example of Infrastructure Changes	مثال على تغييرات البنية التحتية
138	Translated (0%)	<1115>Level 0</1115> - <1121>Emergency Change:</1121>	<1115>المستوى 0</1115> - <1121>التغيير الطارئ:</1121><1115>
139	Translated (0%)	Changes that, if not implemented immediately, will leave Al Hammadi Holding open to significant risk.	إذا لم يتم تنفيذ التغييرات على الفور، فستترك شركة الحمادي القابضة عرضة لمخاطر كبيرة.
140	Translated (0%)	These changes are critical to the continuity of business.	هذه التغييرات حاسمة لاستمرارية الأعمال.
141	Translated (0%)	This type of change has a separate approval process.	هذا النوع من التغيير له عملية موافقة منفصلة.
142	Translated (0%)	Changes must be done immediately within 4 hours	يجب إجراء التغييرات على الفور في غضون 4 ساعات
143	Translated (0%)	Application failure, Application timeout	فشل التطبيق، مهلة التطبيق

144	Translated (0%)	Core system failure like firewall, core switch, exchange, databases etc.	فشل النظام الأساسي مثل جدار الحماية والمفتاح الأساسي والتبادل وقواعد البيانات وما إلى ذلك.
145	Translated (0%)	<1136>Level 1</1136> - <1142>Major Change:</1142>	<1136>المستوى 1</1136> - <1142>تغيير كبير:</1142><1136></1136>
146	Translated (0%)	Major changes involve a large amount of build or run time, complex issues or significant expenditures.	تنطوي التغييرات الرئيسية على قدر كبير من وقت البناء أو التشغيل أو المشكلات المعقدة أو النفقات الكبيرة.
147	Translated (0%)	The Major change is passed to the Sr. Management for assessment, approval and scheduling.	يتم تمرير التغيير الرئيسي إلى الإدارة العليا للتقييم والموافقة والجدولة.
148	Translated (0%)	The change will impact the majority of the users in Al Hammadi Holding .	. سيؤثر التغيير على غالبية المستخدمين في شركة الحمادي القابضة
149	Translated (0%)	Changes must be done immediately within 2 day	يجب إجراء التغييرات على الفور في غضون يومين
150	Translated (0%)	Implementing a new module in applications like ERP etc., Vendor involved in customization of the application.	،.تنفيذ وحدة جديدة في تطبيقات مثل تخطيط موارد المؤسسات وما إلى ذلك البائع المشارك في تخصيص التطبيق.
151	Translated (0%)	System architecture re-designing, new system implementation & integration, major system upgrades & system replacement	إعادة تصميم بنية النظام، وتنفيذ النظام الجديد وتكامله، وترقيات النظام الرئيسية واستبدال النظام
152	Translated (0%)	Level 2 - Minor Change:	المستوى 2 - تغيير طفيف:
153	Translated (0%)	Minor Change does not involve large amounts of build or run time, complex issues or significant expenditures.	لا ينطوي التغيير الطفيف على كميات كبيرة من وقت البناء أو التشغيل أو المشكلات المعقدة أو النفقات الكبيرة.
154	Translated (0%)	The minor change is passed to the IT Performance Management Expert for assessment, approval and scheduling.	يتم تمرير التغيير الطفيف إلى خبير إدارة أداء تكنولوجيا المعلومات للتقييم والموافقة والجدولة.
155	Translated (0%)	The change will impact a user or group of users or a particular department.	.سيؤثر التغيير على مستخدم أو مجموعة من المستخدمين أو قسم معين
156	Translated (0%)	Changes must be done within 2 weeks	يجب إجراء التغييرات في غضون أسبوعين
157	Translated (0%)	Small design and functionality change like addition of new reports, addition of new screens, addition of new fields etc.	يتغير التصميم والوظائف الصغيرة مثل إضافة تقارير جديدة وإضافة شاشات جديدة وإضافة حقول جديدة وما إلى ذلك.
158	Translated (0%)	Minor system upgrades, break fix on non-core systems etc.	.ترقيات طفيفة للنظام، وإصلاح الأعطال في الأنظمة غير الأساسية وما إلى ذلك
159	Translated (0%)	Level 3 - Standard Change:	المستوى 3 - التغيير القياسي:
160	Translated (0%)	Changes in this level are planned through the defined update cycle for software/hardware releases and hardware upgrades or the implementation plans of new services.	يتم التخطيط للتغييرات في هذا المستوى من خلال دورة التحديث المحددة لإصدارات البرامج/الأجهزة وترقيات الأجهزة أو خطط تنفيذ الخدمات الجديدة.
161	Translated (0%)	This is a part of the standard operating procedure.	.هذا جزء من إجراءات التشغيل القياسية
162	Translated (0%)	Changes must be done within the set deadline	يجب إجراء التغييرات خلال الموعد النهائي المحدد

163	Translated (0%)	Patch upgrades, operating system configurations as part of daily IT operations, with minimal or no impact to IT service availability.	ترقيات التصحيح، وتكوينات نظام التشغيل كجزء من عمليات تكنولوجيا المعلومات اليومية، مع تأثير ضئيل أو معدوم على توافر خدمة تكنولوجيا المعلومات.
164	Translated (0%)	Virus updates, running routine batch files, changing phone extensions, updating phone directory etc.	تحديثات الفيروسات، وتشغيل ملفات الدفعات الروتينية، وتغيير ملحقات الهاتف، وتحديث دليل الهاتف، وما إلى ذلك.
165	Translated (0%)	Capacity management	إدارة القدرات
166	Translated (0%)	Al Hammadi Holding use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	يجب مراقبة استخدام شركة الحمادي القابضة للموارد وضبطها ووضع توقعات لمتطلبات السعة المستقبلية لضمان أداء النظام المطلوب.
167	Translated (0%)	Al Hammadi Holding capacity requirements shall be identified, taking into account the business criticality of the concerned system.	يجب تحديد متطلبات الطاقة الاستيعابية لشركة الحمادي القابضة، مع مراعاة أهمية الأعمال للنظام المعني.
168	Translated (0%)	System tuning and monitoring shall be applied to ensure and, where necessary, improve the availability and efficiency of systems.	يجب تطبيق ضبط النظام ومراقبته لضمان، وعند الضرورة، تحسين توافر الأنظمة وكفاءتها.
169	Translated (0%)	Detective controls shall be put in place to indicate problems in due time.	يجب وضع ضوابط مخبرية للإشارة إلى المشاكل في الوقت المناسب.
170	Translated (0%)	Projections of future capacity requirements shall take account of new business and system requirements and current and projected trends in Al Hammadi Holding’s information processing capabilities.	يجب أن تأخذ توقعات متطلبات السعة المستقبلية في الاعتبار متطلبات الأعمال والنظام الجديدة والاتجاهات الحالية والمتوقعة في قدرات معالجة المعلومات في شركة الحمادي القابضة.
171	Translated (0%)	Particular attention needs to be paid to any resources with long procurement lead times or high costs.	يجب إيلاء اهتمام خاص لأي موارد ذات مهل شراء طويلة أو تكاليف عالية.
172	Translated (0%)	Al Hammadi Holding shall monitor the utilization of key system resources.	تراقب شركة الحمادي القابضة استخدام موارد النظام الرئيسية.
173	Translated (0%)	Al Hammadi Holding shall identify trends in usage, particularly in relation to business applications or information systems management tools.	يجب على شركة الحمادي القابضة تحديد اتجاهات الاستخدام، لا سيما فيما يتعلق بتطبيقات الأعمال أو أدوات إدارة أنظمة المعلومات.
174	Translated (0%)	Al Hammadi Holding shall identify and avoid potential bottlenecks and dependence on key personnel that might present a threat to system security or services, and plan appropriate action.	يجب على شركة الحمادي القابضة تحديد وتجنب الاختناقات المحتملة والاعتماد على الموظفين الرئيسيين الذين قد يشكلون تهديدًا لأمن النظام أو خدماته، وتخطيط الإجراء المناسب.
175	Translated (0%)	Al Hammadi Holding sufficient capacity can be achieved by increasing capacity or by reducing demand, including:	يمكن تحقيق القدرة الكافية لشركة الحمادي القابضة عن طريق زيادة السعة أو عن طريق تقليل الطلب، بما في ذلك:
176	Translated (0%)	deletion of obsolete data (disk space).	حذف البيانات القديمة (مساحة القرص).
177	Translated (0%)	decommissioning of applications, systems, or databases.	إيقاف تشغيل التطبيقات أو الأنظمة أو قواعد البيانات.
178	Translated	optimizing batch processes and schedules.	تحسين عمليات وجداول الدفعات.

	(0%)		
179	Translated (0%)	optimizing application logic or database queries.	.تحسين منطق التطبيق أو استعلامات قاعدة البيانات
180	Translated (0%)	denying or restricting bandwidth for resource-hungry services.	.رفض أو تقييد عرض النطاق الترددي للخدمات المتعطشة للموارد
181	Translated (0%)	Al Hammadi Holding shall address the capacity of the technical human resources.	.يجب على شركة الحمادي القابضة معالجة قدرة الموارد البشرية الفنية
182	Translated (0%)	IT shall conduct an evaluation of IT investments and consider the total cost of ownership for the entire period that the IT solution is required, in accordance with identified business requirements, reliability, performance, scalability, security, maintenance requirements, legal risks, ease of customization, and ease of migration.	يجب على تكنولوجيا المعلومات إجراء تقييم لاستثمارات تكنولوجيا المعلومات والنظر في التكلفة الإجمالية للملكية لكامل الفترة التي يكون فيها حل تكنولوجيا المعلومات مطلوبًا، وفقًا لمتطلبات العمل المحددة والموثوقية والأداء وقابلية التوسع والأمن ومتطلبات الصيانة والمخاطر القانونية وسهولة التخصيص وسهولة .الترحيل
183	Translated (0%)	IT shall conduct proper due diligence when estimating any IT Project demand based on the initial maturity stage (inception or baseline) and report the actual effort spent on each initiative/project at different stages.	يجب على قسم تكنولوجيا المعلومات إجراء العناية الواجبة المناسبة عند تقدير أي طلب على مشروع تكنولوجيا المعلومات بناءً على مرحلة النضج الأولية والإبلاغ عن الجهد الفعلي المبذول في كل (البداية أو خط الأساس) .مبادرة/مشروع في مراحل مختلفة
184	Translated (0%)	Each IT related business request shall be clearly specified and documented before approval is granted.	يجب تحديد وتوثيق كل طلب عمل متعلق بتكنولوجيا المعلومات بوضوح قبل .منح الموافقة
185	Translated (0%)	All requests shall be raised with the resource capacity estimate required to implement the business request.	.يجب رفع جميع الطلبات مع تقدير سعة الموارد المطلوبة لتنفيذ طلب العمل
186	Translated (0%)	All applications, software packages, Information Technology solutions, infrastructure and expansion Demands are subject to the terms of this policy and the related processes and procedures.	تخضع جميع التطبيقات وحزم البرامج وحلول تكنولوجيا المعلومات والبنية .التحتية وطلبات التوسع لشروط هذه السياسة والعمليات والإجراءات ذات الصلة
187	Translated (0%)	Any exception would require an approval from the IT Strategy and Planning Function.	.سيتطلب أي استثناء موافقة من قسم استراتيجية وتخطيط تكنولوجيا المعلومات
188	Translated (0%)	IT investments shall reduce the total cost of ownership (TCO) while maximizing flexibility and reuse.	يجب أن تقلل استثمارات تكنولوجيا المعلومات من التكلفة الإجمالية للملكية .مع زيادة المرونة وإعادة الاستخدام (TCO)
189	Translated (0%)	IT investments shall facilitate the consolidation of platforms that provide the highest flexibility and scalability in order to achieve best value and economies of scale while meeting business requirements.	يجب أن تسهل استثمارات تكنولوجيا المعلومات توحيد المنصات التي توفر أعلى قدر من المرونة وقابلية التوسع من أجل تحقيق أفضل قيمة ووفورات الحجم مع .تلبية متطلبات العمل
190	Translated (0%)	IT investments shall facilitate the access to information technology resources for all individuals.	يجب أن تسهل استثمارات تكنولوجيا المعلومات الوصول إلى موارد تكنولوجيا .المعلومات لجميع الأفراد
191	Translated (0%)	The available capacity vs. required capacity formula has to be approved by the IT Strategy and Planning Function.	يجب أن تتم الموافقة على صيغة السعة المتاحة مقابل السعة المطلوبة من قبل .وظيفة استراتيجية وتخطيط تكنولوجيا المعلومات
192	Translated (0%)	The implication of any proposed demand expansion i.e., the existing capacity of the running application and infrastructure plus the changes to be introduced, shall be prepared by the business	يجب إعداد الآثار المترتبة على أي توسع مقترح في الطلب، أي السعة الحالية للتطبيق الجاري والبنية التحتية بالإضافة إلى التغييرات التي سيتم إدخالها، من قبل الشركة التي تترجم أحجام محركات الأعمال المتوقعة، ثم تترجم تكنولوجيا

		translating the expected business driver volumes, and then IT translates that into additional IT resource capacity.	.المعلومات ذلك إلى سعة إضافية لموارد تكنولوجيا المعلومات
193	Translated (0%)	The Al Hammadi Holding shall identify capacity requirements on the basis of Al Hammadi Holding business plans, business requirements, SLAs, if any, with Al Hammadi Holding business units and risk assessments.	يجب على شركة الحمادي القابضة تحديد متطلبات السعة على أساس خطط أعمال شركة الحمادي القابضة ومتطلبات الأعمال واتفاقيات مستوى الخدمة، إن وجدت، مع وحدات أعمال شركة الحمادي القابضة وتقييمات المخاطر.
194	Translated (0%)	Capacity requirements shall be considered in the development and negotiation of SLA's, if any, with Al Hammadi Holding business units.	يجب مراعاة متطلبات السعة عند تطوير اتفاقيات مستوى الخدمة والتفاوض عليها، إن وجدت، مع وحدات أعمال الحمادي القابضة.
195	Translated (0%)	The business plans and requirements shall be assessed periodically to determine their impact on the current capacity of IT systems, the IT infrastructure and resources, and on the forecast of future IT resource usage.	يجب تقييم خطط ومتطلبات الأعمال بشكل دوري لتحديد تأثيرها على القدرة الحالية لأنظمة تكنولوجيا المعلومات والبنية التحتية لتكنولوجيا المعلومات ومواردها وعلى التنبؤ باستخدام موارد تكنولوجيا المعلومات في المستقبل.
196	Translated (0%)	Based upon this assessment, the capacity plan shall be updated to ensure requirements reflect agreed upon changes required by the business.	بناءً على هذا التقييم، يجب تحديث خطة السعة لضمان أن تعكس المتطلبات التغييرات المتفق عليها التي تتطلبها الشركة.
197	Translated (0%)	The forecasted business workload estimates shall be translated to specific IT resources requirements.	يجب ترجمة تقديرات عبء العمل المتوقع إلى متطلبات محددة لموارد تكنولوجيا المعلومات.
198	Translated (0%)	The associated costs for the current and forecasted IT resources required to meet the business objective and achieve the service level targets shall be assessed periodically.	يجب تقييم التكاليف المرتبطة بموارد تكنولوجيا المعلومات الحالية والمتوقعة المطلوبة لتحقيق هدف العمل وتحقيق أهداف مستوى الخدمة بشكل دوري.
199	Translated (0%)	Each Business Unit shall be responsible to provide the appropriate demand forecasts to Al Hammadi Holding for capacity planning as soon as the requirements are identified.	تكون كل وحدة أعمال مسؤولة عن تقديم توقعات الطلب المناسبة إلى شركة الحمادي القابضة لتخطيط السعة بمجرد تحديد المتطلبات.
200	Translated (0%)	Performance exceptions and resource utilization exceptions shall be reviewed to identify the areas that can be tuned or optimized for efficient utilization of system resources and to improve the overall level of the IT service performance.	يجب مراجعة استثناءات الأداء واستثناءات استخدام الموارد لتحديد المجالات التي يمكن ضبطها أو تحسينها للاستخدام الفعال لموارد النظام ولتحسين المستوى العام لأداء خدمة تكنولوجيا المعلومات.
201	Translated (0%)	System and performance tuning shall be tested and shall be constructed as a baseline or modeled prior to the implementation in the production environment.	يجب اختبار النظام وضبط الأداء وإنشاءهما كخط أساس أو نمذجة قبل التنفيذ في بيئة الإنتاج.
202	Translated (0%)	Controls shall be in place to proactively identify the additional system capacity requirements to minimize the risk of systems failure due to capacity shortage.	يجب وضع ضوابط لتحديد متطلبات سعة النظام الإضافية بشكل استباقي لتقليل مخاطر فشل الأنظمة بسبب نقص السعة.
203	Translated (0%)	Monitoring, gathering data, analyzing, reporting, and reviewing capacity will be performed by the Al Hammadi Holding IT periodically.	سيتم إجراء المراقبة وجمع البيانات والتحليل والإبلاغ ومراجعة القدرات من قبل شركة الحمادي القابضة لتقنية المعلومات بشكل دوري.
204	Translated (0%)	Capacity reports shall be submitted to cybersecurity steering committee bi-annual.	يجب تقديم تقارير السعة إلى اللجنة التوجيهية للأمن السيبراني مرتين في السنة.

205	Translated (0%)	Separation of development, testing and operational environments	الفصل بين بيئات التطوير والاختبار والتشغيل
206	Translated (0%)	Al Hammadi Holding development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	يجب فصل بيئات التطوير والاختبار والتشغيل لشركة الحمادي القابضة لتقليل مخاطر الوصول غير المصرح به أو التغييرات في البيئة التشغيلية.
207	Translated (0%)	Al Hammadi Holding level of separation between operational, testing, and development environments to prevent operational conflicts shall be identified and implemented.	يجب تحديد وتنفيذ مستوى فصل شركة الحمادي القابضة بين بيئات التشغيل والاختبار والتطوير لمنع النزاعات التشغيلية.
208	Translated (0%)	Rules for the transfer of software from development to operational status shall be defined and documented.	يجب تحديد وتوثيق قواعد نقل البرمجيات من مرحلة التطوير إلى مرحلة التشغيل.
209	Translated (0%)	Development and operational software shall run on different systems or computer processors and in different domains or directories.	يجب أن تعمل برامج التطوير والتشغيل على أنظمة أو معالجات كمبيوتر مختلفة وفي مجالات أو أدلة مختلفة.
210	Translated (0%)	Changes to operational systems and applications shall be tested in a testing or staging environment prior to being applied to operational systems.	يجب اختبار التغييرات التي تطرأ على الأنظمة والتطبيقات التشغيلية في بيئة الاختبار أو التدريج قبل تطبيقها على الأنظمة التشغيلية.
211	Translated (0%)	Unless exceptional circumstances exist, testing shall not be done on operational systems.	ما لم تكن هناك ظروف استثنائية، لا يجوز إجراء الاختبار على الأنظمة التشغيلية.
212	Translated (0%)	Al Hammadi Holding users shall use different user profiles for operational and testing systems, and menus shall display appropriate identification messages to reduce the risk of error.	يجب على مستخدمي شركة الحمادي القابضة استخدام ملفات تعريف مستخدمين مختلفة لأنظمة التشغيل والاختبار، ويجب أن تعرض القوائم رسائل تعريف مناسبة لتقليل مخاطر الخطأ.
213	Translated (0%)	Al Hammadi Holding sensitive data shall not be copied into the testing system environment unless equivalent controls are provided for the testing system	لا يجوز نسخ البيانات الحساسة لشركة الحمادي القابضة في بيئة نظام الاختبار ما لم يتم توفير ضوابط مكافئة لنظام الاختبار
214	Translated (0%)	To avoid introducing unauthorized and untested code or alter operational data, Al Hammadi Holding testing personnel shall only have access with the presence of business owners of operational systems.	لتجنب إدخال التعليمات البرمجية غير المصرح بها وغير المختبرة أو تغيير البيانات التشغيلية، يجب ألا يتمكن موظفو اختبار شركة الحمادي القابضة من الوصول إلا بحضور أصحاب الأعمال للأنظمة التشغيلية.
215	Translated (100%)	Protection from malware	الحماية من البرمجيات الخبيثة
216	Translated (0%)	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	يجب تنفيذ ضوابط الكشف والوقاية والتعافي للحماية من البرامج الضارة، جنبًا إلى جنب مع توعية المستخدم المناسبة.
217	Translated (0%)	Protection against malware shall be based on malware detection and repair software, information security awareness, and appropriate system access and change management controls.	يجب أن تستند الحماية من البرامج الضارة إلى برامج الكشف عن البرامج الضارة وإصلاحها، والوعي بأمن المعلومات، والوصول المناسب إلى النظام وضوابط إدارة التغيير.
218	Translated (0%)	Al Hammadi Holding shall prohibit the use of unauthorized software and malicious websites by implementing controls that prevent or detect this behavior.	تحظر شركة الحمادي القابضة استخدام البرامج غير المصرح بها والمواقع الضارة من خلال تنفيذ الضوابط التي تمنع أو تكشف هذا السلوك.

219	Translated (0%)	Al Hammadi Holding shall protect against risks associated with obtaining files and software either from or via external networks or on any other medium.	يجب على شركة الحمادي القابضة الحماية من المخاطر المرتبطة بالحصول على الملفات والبرامج إما من أو عبر الشبكات الخارجية أو على أي وسيط آخر.
220	Translated (0%)	Al Hammadi Holding shall reduce vulnerabilities that could be exploited by malware through technical vulnerability management.	يجب على شركة الحمادي القابضة تقليل الثغرات التي يمكن استغلالها بواسطة البرامج الضارة من خلال إدارة الثغرات الفنية.
221	Translated (0%)	Al Hammadi Holding shall conduct regular reviews of the software and data content of systems supporting critical business processes.	يجب على شركة الحمادي القابضة إجراء مراجعات منتظمة للبرمجيات ومحتوى البيانات للأنظمة التي تدعم العمليات التجارية الهامة.
222	Translated (0%)	Al Hammadi Holding shall install and update of malware detection and repair software to scan computers and media as a precautionary control on a routine basis.	يجب على شركة الحمادي القابضة تثبيت وتحديث برامج الكشف عن البرامج الضارة وإصلاحها لمسح أجهزة الكمبيوتر والوسائط كعنصر تحكم احترازي بشكل روتيني.
223	Translated (0%)	Al Hammadi Holding shall implement procedures to regularly collect information, such as subscribing to mailing lists or verifying websites giving information about new malware.	يجب على شركة الحمادي القابضة تنفيذ إجراءات لجمع المعلومات بانتظام، مثل الاشتراك في القوائم البريدية أو التحقق من مواقع الويب التي تقدم معلومات حول البرامج الضارة الجديدة.
224	Translated (0%)	Al Hammadi Holding users shall be made aware of viruses and hoaxes and what to do on receipt of them.	يجب أن يكون مستخدمو شركة الحمادي القابضة على دراية بالفيروسات والخدع وما يجب القيام به عند استلامها.
225	Translated (0%)	Al Hammadi Holding shall protect against the introduction of malware during maintenance and emergency procedures, which may bypass normal malware protection controls	يجب على شركة الحمادي القابضة الحماية من إدخال البرامج الضارة أثناء إجراءات الصيانة والطوارئ، والتي قد تتجاوز ضوابط الحماية من البرامج الضارة العادية
226	Translated (0%)	Appropriate informative communication channels shall be maintained and established to obtain latest details of malicious code.	يجب الحفاظ على قنوات الاتصال الإعلامية المناسبة وإنشاءها للحصول على أحدث تفاصيل التعليمات البرمجية الضارة.
227	Translated (0%)	Al Hammadi Holding IT shall implement a controlled environment in order to safeguard systems against malicious code.	يجب على شركة الحمادي القابضة لتقنية المعلومات تنفيذ بيئة خاضعة للرقابة من أجل حماية الأنظمة من التعليمات البرمجية الضارة.
228	Translated (0%)	Procedures shall be developed for recovering from malicious code.	يجب وضع إجراءات للتعافي من التعليمات البرمجية الضارة.
229	Translated (0%)	Protection against malware shall be deployed using best of breed anti-malware software.	يجب نشر الحماية ضد البرامج الضارة باستخدام أفضل برامج مكافحة البرامج الضارة.
230	Translated (0%)	Anti-malware signatures shall be updated on a regular basis and any available updates shall be deployed to endpoints.	يجب تحديث توقيعات مكافحة البرامج الضارة على أساس منتظم ويجب نشر أي تحديثات متاحة على نقاط النهاية.
231	Translated (0%)	The generated audit logs from all devices shall be retained and periodically reviewed to identify warnings, alerts and remediation actions.	يجب الاحتفاظ بسجلات التدقيق التي تم إنشاؤها من جميع الأجهزة ومراجعتها بشكل دوري لتحديد التحذيرات والتنبيهات وإجراءات الإصلاح.
232	Translated (0%)	Anti-malware software shall be used to scan in real time for malicious code.	يجب استخدام برنامج مكافحة البرامج الضارة للمسح في الوقت الفعلي بحثًا عن التعليمات البرمجية الضارة.
233	Translated (0%)	Anti-malware software shall be configured to continuously detect and clean malware, if cleaning is not possible then quarantine option shall be enabled with appropriate access controls.	يجب تكوين برامج مكافحة البرامج الضارة للكشف المستمر عن البرامج الضارة وتنظيفها، وإذا لم يكن التنظيف ممكنًا، فيجب تمكين خيار الحجر الصحي مع عناصر التحكم المناسبة في الوصول.

234	Translated (0%)	Anti-malware mechanisms shall run actively and shall not be disabled or altered by users.	يجب أن تعمل آليات مكافحة البرامج الضارة بنشاط ولا يجوز تعطيلها أو تغييرها من قبل المستخدمين.
235	Translated (0%)	If anti-malware protection needs to be disabled for a specific purpose, it shall be authorized by Al Hammadi Holding IT Department.	إذا كانت الحماية من البرامج الضارة بحاجة إلى تعطيل لغرض معين، فيجب أن تكون مصرحًا بها من قبل إدارة تكنولوجيا المعلومات بالحمادي القابضة.
236	Translated (0%)	In case access is required from a third-party computing system, it shall be ensured that the system is suitably protected from malware.	في حالة طلب الوصول من نظام حوسبة تابع لجهة خارجية، يجب التأكد من أن النظام محمي بشكل مناسب من البرامج الضارة.
237	Translated (0%)	Regular reviews of software and data content of systems supporting business processes shall be conducted and the presence of any malicious files or artefacts shall be investigated.	يجب إجراء مراجعات منتظمة للبرامج ومحتوى البيانات للأنظمة التي تدعم العمليات التجارية والتحقيق في وجود أي ملفات أو قطع أثرية ضارة.
238	Translated (0%)	Systems considered to be not commonly affected by malicious software shall be periodically evaluated in order to identify whether such systems require anti-malware software.	يجب تقييم الأنظمة التي تعتبر غير متأثرة بشكل عام بالبرامج الضارة بشكل دوري من أجل تحديد ما إذا كانت هذه الأنظمة تتطلب برامج مكافحة البرامج الضارة.
239	Translated (0%)	The Al Hammadi Holding shall define and provide modern and advanced protection techniques and mechanisms and ensure its reliability.	تقوم شركة الحمادي القابضة بتحديد وتوفير تقنيات وآليات الحماية الحديثة والمتقدمة وضمان موثوقيتها.
240	Translated (0%)	Protection techniques and mechanisms shall be applied to protect users' devices, mobile devices, and servers from malware and to manage them securely.	يجب تطبيق تقنيات وآليات الحماية لحماية أجهزة المستخدمين والأجهزة المحمولة والخوادم من البرامج الضارة وإدارتها بشكل آمن.
241	Translated (0%)	Ensure that protection technologies and mechanisms can detect and remove all known types of malware, such as viruses, Trojan horses, worms, spyware, adware, and Rootkits.	تأكد من أن تقنيات وآليات الحماية يمكنها اكتشاف وإزالة جميع أنواع البرامج الضارة المعروفة، مثل الفيروسات وأحصنة طروادة والديدان وبرامج التجسس والبرامج الإعلانية والجذور الخفية.
242	Translated (0%)	Ensure the compatibility of the protection technologies and mechanisms to Al Hammadi Holding operating systems prior to the acquirements such as Windows, UNIX, Linux, Mac, and others.	ضمان توافق تقنيات وآليات الحماية مع أنظمة تشغيل شركة الحمادي القابضة قبل عمليات الاستحواذ مثل ويندوز ويونيكس ولينكس وماك وغيرها.
243	Translated (0%)	Ensure that the protection technologies are recoverable to the previous version, if any update causes damage to the systems or business requirements.	تأكد من أن تقنيات الحماية قابلة للاسترداد إلى الإصدار السابق، إذا تسبب أي تحديث في تلف الأنظمة أو متطلبات العمل.
244	Translated (0%)	Ensure the restriction of installation disablement, cancelation or setting changes of the protection technologies to be granted to security system administrators only.	التأكد من تقييد تعطيل التثبيت أو الإلغاء أو تعيين تغييرات تقنيات الحماية التي سيتم منحها لمسؤولي نظام الأمان فقط.
245	Translated (0%)	Protection Techniques and Mechanisms from Malwares	تقنيات وآليات الحماية من مالواريس
246	Translated (0%)	The protection technologies and mechanisms shall be adjusted according to the security technical standards approved by the Al Hammadi Holding, with considering supplier’s instructions and recommendations.	يجب تعديل تقنيات وآليات الحماية وفقًا للمعايير الفنية الأمنية المعتمدة من قبل شركة الحمادي القابضة، مع مراعاة تعليمات وتوصيات المورد.
247	Translated	Antivirus appliances shall be deployed to email servers to scan all	يجب نشر أجهزة مكافحة الفيروسات على خوادم البريد الإلكتروني لمسح جميع

	(0%)	incoming and outgoing emails.	.رسائل البريد الإلكتروني الواردة والصادرة
248	Translated (0%)	Third-party people are prohibited to connect to the Al Hammadi Holding network or wireless network without updating the anti-virus software and adjusting the appropriate settings.	يحظر على الأشخاص الخارجيين الاتصال بشبكة الحمادي القابضة أو الشبكة .اللاسلكية دون تحديث برنامج مكافحة الفيروسات وضبط الإعدادات المناسبة
249	Translated (0%)	Anti-malware software servers shall be available, and the backup environment shall be suitable for anti-malware software servers intended for non- critical tasks.	يجب أن تكون خوادم برامج مكافحة البرامج الضارة متاحة، ويجب أن تكون بيئة النسخ الاحتياطي مناسبة لخوادم برامج مكافحة البرامج الضارة المخصصة للمهام .غير الحرجة
250	Translated (0%)	Access to websites and other sources on the Internet known to host malicious software shall be blocked by the Web Content Filtering mechanisms.	يجب حظر الوصول إلى مواقع الويب والمصادر الأخرى على الإنترنت المعروفة .باستضافة البرامج الضارة بواسطة آليات تصفية محتوى الويب
251	Translated (0%)	Clock Synchronization shall be centralized and comes from an accurate and reliable source for all malware protection technologies and mechanisms.	يجب أن تكون مزامنة الساعة مركزية وتأتي من مصدر دقيق وموثوق لجميع .تقنيات وآليات الحماية من البرامج الضارة
252	Translated (0%)	Malware protection technology shall be configured to perform checks on suspicious content on isolated sources such as the Sandbox.	يجب تكوين تقنية الحماية من البرامج الضارة لإجراء فحوصات على المحتوى .Sandbox المشبوه على مصادر معزولة مثل
253	Translated (0%)	Periodic scans of users' devices and servers shall be performed to ensure that they are safe from malware.	يجب إجراء عمليات مسح دورية لأجهزة المستخدمين وخوادمهم للتأكد من أنها .آمنة من البرامج الضارة
254	Translated (0%)	Malware protection technologies shall be updated automatically when new versions are released, with consideration of the policy of patch management.	يجب تحديث تقنيات الحماية من البرامج الضارة تلقائيًا عند إصدار إصدارات .جديدة، مع مراعاة سياسة إدارة التصحيح
255	Translated (0%)	Protection of email and internet surfing shall be provided against advanced persistent threats (APT), which typically use Zero-Day Malware, along with their proper deployment and management.	يجب توفير حماية للبريد الإلكتروني وتصفح الإنترنت ضد التهديدات المستمرة (APT) المتقدمة، والتي تستخدم عادةً البرامج الضارة Zero - Day، إلى جانب .نشرها وإدارتها بشكل صحيح
256	Translated (0%)	Security configuration shall allow whitelisting only specific list of applications and programs to work on servers for critical systems.	يجب أن يسمح تكوين الأمان للقائمة البيضاء فقط بقائمة محددة من التطبيقات .والبرامج للعمل على خوادم للأنظمة الحيوية
257	Translated (0%)	Servers for critical systems shall be protected by end-point protection security technologies approved by the Al Hammadi Holding.	يجب حماية خوادم الأنظمة الحرجة بواسطة تقنيات أمن حماية نقطة النهاية .المعتمدة من قبل شركة الحمادي القابضة
258	Translated (0%)	Periodic reports on the status of malware protection shall be prepared to clarify the number of devices and servers associated with the protection technologies and their status (such as up-to-date, out-of-date, offline, etc.),and submitted to IT Manager.	يجب إعداد تقارير دورية عن حالة الحماية من البرامج الضارة لتوضيح عدد الأجهزة والخوادم المرتبطة بتقنيات الحماية وحالتها (مثل محدثة، قديمة، غير .متصلة بالإنترنت، وما إلى ذلك)،وتقديمها إلى مدير تكنولوجيا المعلومات
259	Translated (0%)	Malware protection techniques management shall be centralized and continuously monitored.	يجب أن تكون إدارة تقنيات الحماية من البرامج الضارة مركزية ومراقبتها .باستمرار
260	Translated (0%)	The Cybersecurity Department shall ensure that all employees have the necessary security awareness regarding malware and their associated risks.	يجب على إدارة الأمن السيبراني التأكد من أن جميع الموظفين لديهم الوعي الأمني .اللازم فيما يتعلق بالبرامج الضارة والمخاطر المرتبطة بها
261	Translated	The requirements of cybersecurity shall be reviewed periodically	يجب مراجعة متطلبات الأمن السيبراني بشكل دوري لحماية أجهزة المستخدمين

	(0%)	to protect the users' devices and servers of the Al Hammadi Holding.	.وخوادم شركة الحمادي القابضة
262	Translated (100%)	Configuration Management	إدارة التكوين
263	Translated (0%)	All systems, networks, and applications must be configured securely and consistently to mitigate potential risks.	يجب تكوين جميع الأنظمة والشبكات والتطبيقات بشكل آمن ومتسق للتخفيف .من المخاطر المحتملة
264	Translated (0%)	Information Security will maintain documented procedures for secure configuration management across its IT infrastructure.	سيحافظ أمن المعلومات على إجراءات موثقة لإدارة التكوين الآمن عبر البنية .التحتية لتكنولوجيا المعلومات الخاصة به
265	Translated (0%)	Configuration management procedures should cover, at least:	:يجب أن تغطي إجراءات إدارة التكوين، على الأقل
266	Translated (0%)	Initial setup of systems and network devices	الإعداد الأولي للأنظمة وأجهزة الشبكة
267	Translated (0%)	Hardening procedures (e.g., removal of unnecessary services, secure configuration settings)	إجراءات التقوية (على سبيل المثال، إزالة الخدمات غير الضرورية، إعدادات (التكوين الآمنة
268	Translated (0%)	Changes to configurations will be logged and monitored to detect any unauthorized changes or misconfigurations.	سيتم تسجيل التغييرات في التكوينات ومراقبتها للكشف عن أي تغييرات أو .تكوينات خاطئة غير مصرح بها
269	Translated (0%)	Configuration audits will be performed regularly to ensure that systems adhere to security policies and procedures.	سيتم إجراء عمليات تدقيق التكوين بانتظام لضمان التزام الأنظمة بالسياسات .والإجراءات الأمنية
270	Translated (0%)	Non-compliance with configuration management procedures will be addressed promptly through corrective actions and remediation plans	سيتم معالجة عدم الامتثال لإجراءات إدارة التكوين على الفور من خلال الإجراءات التصحيحية وخطط الإصلاح
271	Translated (99%)	Backup	نسخة احتياطية
272	Translated (0%)	Al Hammadi Holding shall regularly keep and test backup copies of critical information, software, and system images.	يجب على شركة الحمادي القابضة الاحتفاظ بنسخ احتياطية من المعلومات الهامة .والبرامج وصور النظام واختبارها بانتظام
273	Translated (0%)	All business-related data shall be stored and maintained on the provided backup facilities by the Al Hammadi Holding IT Department.	يجب تخزين جميع البيانات المتعلقة بالأعمال والاحتفاظ بها في مرافق النسخ .الاحتياطي المقدمة من قبل إدارة تكنولوجيا المعلومات بالحمادي القابضة
274	Translated (0%)	Al Hammadi Holding is not responsible for taking backup of any business-related data that end users may have stored on other storage systems unless there is an arrangement with the Al Hammadi Holding IT Department.	الحمادي القابضة ليست مسؤولة عن أخذ نسخة احتياطية من أي بيانات متعلقة بالأعمال قد يكون المستخدمون النهائيون قد قاموا بتخزينها على أنظمة تخزين .أخرى ما لم يكن هناك ترتيب مع إدارة تكنولوجيا المعلومات في الحمادي القابضة
275	Translated (0%)	The backup and recovery procedures shall be developed and regularly reviewed to ensure that they are effective to cover the business continuity requirements.	يجب تطوير إجراءات النسخ الاحتياطي والاسترداد ومراجعتها بانتظام للتأكد من .فعاليتها في تغطية متطلبات استمرارية الأعمال
276	Translated (0%)	Business owners have to provide the backup and retention requirements for their corresponding business-related data.	يتعين على أصحاب الأعمال توفير متطلبات النسخ الاحتياطي والاحتفاظ بالبيانات .ذات الصلة بالأعمال
277	Translated (0%)	For services that are hosted on cloud environment, the backup and restoration requirements shall be covered in the contract with	بالنسبة للخدمات المستضافة على البيئة السحابية، يجب تغطية متطلبات النسخ بما في ذلك ،(CSP) الاحتياطي والاستعادة في العقد مع مزود الخدمة السحابية

		the Cloud Service Provider (CSP), including demonstrating the success or failure of backup and restore processes.	.إثبات نجاح أو فشل عمليات النسخ الاحتياطي والاستعادة
278	Translated (0%)	Al Hammadi Holding IT Department shall conduct regular restoration tests to verify the readability of backup media and the results of such tests shall be maintained.	يجب على قسم تكنولوجيا المعلومات في شركة الحمادي القابضة إجراء اختبارات ترميم منتظمة للتحقق من سهولة قراءة الوسائط الاحتياطية ويجب الحفاظ على .نتائج هذه الاختبارات
279	Translated (0%)	In case the restoration tests have failed due to backup media, Al Hammadi Holding IT Department will dispose of the backup media and shall take a fresh backup.	في حالة فشل اختبارات الاستعادة بسبب الوسائط الاحتياطية، سيتخلص قسم تكنولوجيا المعلومات في شركة الحمادي القابضة من الوسائط الاحتياطية .وسيأخذ نسخة احتياطية جديدة
280	Translated (0%)	Al Hammadi Holding IT Department will be responsible for developing a restoration plan that will be reviewed regularly for its effectiveness.	سيكون قسم تكنولوجيا المعلومات في شركة الحمادي القابضة مسؤولًا عن وضع .خطة ترميم سيتم مراجعتها بانتظام للتأكد من فعاليتها
281	Translated (0%)	Al Hammadi Holding IT Department shall ensure that the restored data is deleted after successful completion of restoration testing.	يجب على قسم تكنولوجيا المعلومات في شركة الحمادي القابضة التأكد من .حذف البيانات المستعادة بعد الانتهاء بنجاح من اختبار الاستعادة
282	Translated (0%)	Data will be backed up on at least two separate media with standard labelling. at least one of the backup media will be stored in an off-site location.	سيتم الاحتفاظ بنسخة احتياطية من البيانات على اثنين على الأقل من الوسائط المنفصلة مع وضع العلامات القياسية. سيتم تخزين واحدة على الأقل من وسائط .النسخ الاحتياطي في موقع خارج الموقع
283	Translated (0%)	Daily incremental backup shall be done on-site using tapes or the latest backup technology.	يجب إجراء النسخ الاحتياطي التزايدي اليومي في الموقع باستخدام الأشرطة أو .أحدث تقنيات النسخ الاحتياطي
284	Translated (0%)	Weekly full backup shall be done and stored off-site using tapes or latest backup technology.	يجب إجراء النسخ الاحتياطي الكامل الأسبوعي وتخزينه خارج الموقع باستخدام .الأشرطة أو أحدث تقنيات النسخ الاحتياطي
285	Translated (0%)	Both onsite and offsite backups shall be stored in secure locations, maintained in a fire-resistant environment and shall be provided with appropriate physical security controls.	يجب تخزين النسخ الاحتياطية في الموقع وخارجه في مواقع آمنة، والحفاظ .عليها في بيئة مقاومة للحريق ويجب تزويدها بضوابط أمنية مادية مناسبة
286	Translated (0%)	The activities and events of backup and restore shall be logged.	.يجب تسجيل أنشطة وأحداث النسخ الاحتياطي والاستعادة
287	Translated (0%)	Access to backup media will be restricted to approved personnel.	.سيقتصر الوصول إلى الوسائط الاحتياطية على الموظفين المعتمدين
288	Translated (0%)	The backups shall be kept and retained to a minimum period as per business, legal and regulatory requirements.	يجب الاحتفاظ بالنسخ الاحتياطية والاحتفاظ بها إلى الحد الأدنى من الفترة وفقًا .للمتطلبات التجارية والقانونية والتنظيمية
289	Translated (0%)	Effective disposal measures shall be followed after the retention period.	.يجب اتباع تدابير التخلص الفعالة بعد فترة الاحتفاظ
290	Translated (0%)	Al Hammadi Holding IT Department shall implement additional controls over the information contained in backup media to ensure the confidentiality of the information.	يجب على قسم تكنولوجيا المعلومات في شركة الحمادي القابضة تنفيذ ضوابط .إضافية على المعلومات الواردة في الوسائط الاحتياطية لضمان سرية المعلومات
291	Translated (0%)	The retention period for essential business information shall be determined, taking into account any requirement for archive copies to be permanently retained.	يتم تحديد فترة الاحتفاظ بالمعلومات التجارية الأساسية، مع مراعاة أي متطلبات .للاحتفاظ بنسخ الأرشيف بشكل دائم
292	Translated (0%)	Al Hammadi Holding shall define the backup retention and protection requirements.	يجب على شركة الحمادي القابضة تحديد متطلبات الاحتفاظ بالنسخ الاحتياطي .والحماية

293	Translated (0%)	Specific data retention periods are set out below:	وفيما يلي فترات محددة للاحتفاظ بالبيانات:
294	Translated (99%)	Document Type	نوع المستند
295	Translated (0%)	Retention Period	فترة الحفظ
296	Translated (100%)	Hard Copy	نسخة ورقية
297	Translated (0%)	Soft Copy	نسخة إلكترونية
298	Translated (0%)	Administrative Policy and Procedures	السياسة والإجراءات الإدارية
299	Translated (100%)	3 years	3 سنوات
300	Translated (0%)	Department Policy and Procedures	سياسة القسم وإجراءاته
301	Translated (99%)	1 year	سنة واحدة
302	Translated (0%)	IT Department Plans and Manuals	خطط وكتيبات قسم تكنولوجيا المعلومات
303	Translated (100%)	1 year	سنة واحدة
304	Translated (100%)	Document Type	نوع المستند
305	Translated (100%)	Retention Period	فترة الحفظ
306	Translated (100%)	Hard Copy	نسخة ورقية
307	Translated (100%)	Soft Copy	نسخة إلكترونية
308	Translated (0%)	Request Forms	نماذج الطلب
309	Translated (0%)	HIS Access Request	طلب الوصول إلى نظام معلومات المستشفى
310	Translated (0%)	New Procedure Code Request	طلب رمز إجراء جديد
311	Translated (0%)	Modification of Laboratory/Radiology Reports	تعديل تقارير المختبر/الأشعة
312	Translated	Report Request	طلب التقرير

	(0%)		
313	Translated (0%)	IT Work Request	طلب عمل تكنولوجيا المعلومات
314	Translated (0%)	Change Request	طلب تغيير
315	Translated (100%)	Archive	أرشيف
316	Translated (0%)	Hospital Information System (HIS)	(HIS) نظام معلومات المستشفى
317	Translated (100%)	Archive	أرشيف
318	Translated (0%)	Laboratory Information System (LIS)	(LIS) نظام المعلومات المختبرية
319	Translated (100%)	10 years	سنوات 10
320	Translated (0%)	Picture Archiving and Communication System (PACS)	(PACS) نظام أرشفة الصور والاتصالات
321	Translated (100%)	5 years	سنوات 5
322	Translated (0%)	Financial and Accounting Management System	نظام الإدارة المالية والمحاسبية
323	Translated (100%)	10 years	سنوات 10
324	Translated (0%)	Human Resource Management System (HRMS)	(HRMS) نظام إدارة الموارد البشرية
325	Translated (100%)	10 years	سنوات 10
326	Translated (0%)	Network System and Security Records	نظام الشبكة والسجلات الأمنية
327	Translated (100%)	Archive	أرشيف
328	Translated (0%)	Contracts and Purchasing Records	العقود وسجلات المشتريات
329	Translated (100%)	3 years	سنوات 3
330	Translated (0%)	Accurate and complete records of the backup copies and documented restoration procedures shall be produced.	.يجب تقديم سجلات دقيقة وكاملة للنسخ الاحتياطية وإجراءات الاستعادة الموثقة
331	Translated (0%)	Extent (full or differential backup) and frequency of backups shall reflect Al Hammadi Holding business requirements, Al Hammadi	يجب أن يعكس مدى (النسخ الاحتياطي الكامل أو التفاضلي) وتواتر النسخ الاحتياطية متطلبات أعمال شركة الحمادي القابضة، ومتطلبات أمن شركة

		Holding security requirements, and the criticality of the information to the continued operations.	.الحمادي القابضة، وأهمية المعلومات للعمليات المستمرة
332	Translated (0%)	Testing of data restoration procedures shall be regularly conducted.	.يجب إجراء اختبار إجراءات استعادة البيانات بانتظام
333	Translated (0%)	Adequate backup facilities shall be provided to ensure that all essential information and software can be recovered following a disaster or media failure.	يجب توفير مرافق احتياطية كافية لضمان إمكانية استرداد جميع المعلومات .والبرامج الأساسية بعد حدوث كارثة أو فشل في الوسائط
334	Translated (0%)	Backups shall be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site.	يجب تخزين النسخ الاحتياطية في موقع بعيد، على مسافة كافية للهروب من أي .ضرر ناتج عن كارثة في الموقع الرئيسي
335	Translated (0%)	Backup information shall be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site.	يجب إعطاء المعلومات الاحتياطية مستوى مناسب من الحماية المادية والبيئية بما .يتفق مع المعايير المطبقة في الموقع الرئيسي
336	Translated (0%)	Backup media shall be regularly tested to ensure that they can be relied upon for emergency use when necessary.	يجب اختبار الوسائط الاحتياطية بانتظام للتأكد من إمكانية الاعتماد عليها .للاستخدام في حالات الطوارئ عند الضرورة
337	Translated (0%)	In situations where confidentiality is of importance, backups shall be protected by means of encryption.	في الحالات التي تكون فيها السرية ذات أهمية، يجب حماية النسخ الاحتياطية عن .طريق التشفير
338	Translated (0%)	Operational procedures shall monitor the execution of backups and address failures of scheduled backups to ensure completeness of backups according to the backup policy.	يجب أن تراقب الإجراءات التشغيلية تنفيذ النسخ الاحتياطية ومعالجة فشل النسخ الاحتياطية المجدولة لضمان اكتمال النسخ الاحتياطية وفقًا لسياسة النسخ .الاحتياطي
339	Translated (0%)	Backup arrangements for individual systems and services shall be regularly tested to ensure that they meet the requirements of business continuity plans.	يجب اختبار ترتيبات النسخ الاحتياطي للأنظمة والخدمات الفردية بانتظام للتأكد .من أنها تفي بمتطلبات خطط استمرارية الأعمال
340	Translated (0%)	In the case of critical systems and services, backup arrangements shall cover all systems information, applications and data necessary to recover the complete system in the event of a disaster.	في حالة الأنظمة والخدمات الحرجة، يجب أن تغطي ترتيبات النسخ الاحتياطي جميع معلومات الأنظمة والتطبيقات والبيانات اللازمة لاستعادة النظام الكامل في .حالة وقوع كارثة
341	Translated (100%)	Logging and monitoring	التسجيل والمراقبة
342	Translated (0%)	Al Hammadi Holding logging shall set the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security.	يجب أن تضع شركة الحمادي القابضة للتسجيل الأساس لأنظمة المراقبة الآلية .القادرة على إنشاء تقارير وتنبيهات موحدة حول أمن النظام
343	Translated (0%)	Logging shall be enabled on all systems hosting Al Hammadi Holding data and services.	يجب تمكين التسجيل على جميع الأنظمة التي تستضيف بيانات وخدمات شركة .الحمادي القابضة
344	Translated (0%)	Sufficient resources (e.g., system resources, data storage, and network bandwidth) must be provided to accommodate prescribed logging activities.	يجب توفير موارد كافية (على سبيل المثال، موارد النظام وتخزين البيانات وعرض .النطاق الترددي للشبكة) لاستيعاب أنشطة التسجيل المحددة
345	Translated (0%)	Log storage devices must have sufficient log storage for collecting logs.	يجب أن تحتوي أجهزة تخزين السجلات على مساحة تخزين كافية لجمع .السجلات
346	Translated	Retention period for cybersecurity event logs (must be 12 months	فترة الاحتفاظ بسجلات أحداث الأمن السيبراني (يجب أن تكون 12 شهرًا على

	(0%)	minimum).	.الأقل)
347	Translated (0%)	At least the following events must be logged on all Al Hammadi Holding IT environment:	يجب تسجيل الأحداث التالية على الأقل في جميع بيئة تكنولوجيا المعلومات في شركة الحمادي القابضة:
348	Translated (0%)	Successful login attempts.	.محاولات تسجيل دخول ناجحة
349	Translated (0%)	Unsuccessful login attempts, along with the identification of whether the login attempt involved an invalid password.	محاولات تسجيل الدخول غير الناجحة، إلى جانب تحديد ما إذا كانت محاولة تسجيل الدخول تتضمن كلمة مرور غير صالحة.
350	Translated (0%)	All logoffs.	.جميع عمليات تسجيل الخروج
351	Translated (0%)	Additions, deletions and modifications to user accounts/privileges.	.الإضافات والحذف والتعديلات على حسابات/امتيازات المستخدم
352	Translated (0%)	Users switching IDs during an online session.	.يقوم المستخدمون بتبديل المعرفات أثناء جلسة عبر الإنترنت
353	Translated (0%)	Attempts to perform unauthorized functions.	.محاولات لأداء وظائف غير مصرح بها
354	Translated (0%)	Activities performed by privileged accounts.	.الأنشطة التي تقوم بها الحسابات المميزة
355	Translated (0%)	Modifications to system settings (parameters).	.التعديلات على إعدادات النظام (المعلمات)
356	Translated (0%)	Read or write access to protected information, where there is a potential for theft of that information.	قراءة أو كتابة الوصول إلى المعلومات المحمية، حيث يكون هناك احتمال لسرقة تلك المعلومات.
357	Translated (0%)	Detections in inbound and outbound communications for unusual or unauthorized activities including the detection of malware (such as malicious code, spyware, and adware).	عمليات الكشف في الاتصالات الواردة والصادرة للأنشطة غير العادية أو غير المصرح بها بما في ذلك الكشف عن البرامج الضارة (مثل التعليمات البرمجية الضارة وبرامج التجسس والبرامج الإعلانية).
358	Translated (0%)	Additions, deletions and modifications to security/audit log parameters.	.الإضافات والحذف والتعديلات على معلمات سجل الأمان/التدقيق
359	Translated (0%)	Faults (technical problems in information and technology assets) that could potentially be attributed to a security event.	أخطاء (مشاكل فنية في أصول المعلومات والتكنولوجيا) يمكن أن تعزى إلى حدث أمني.
360	Translated (0%)	Activation or deactivation of activities by a specific service.	.تفعيل أو تعطيل الأنشطة من قبل خدمة معينة
361	Translated (0%)	System crashes or restarts.	.تعطل النظام أو إعادة تشغيله
362	Translated (0%)	Password changes.	.تم تغيير كلمة المرور
363	Translated (0%)	Logs shall be periodically reviewed by Al Hammadi Holding cybersecurity department on a regular basis.	يجب مراجعة السجلات بشكل دوري من قبل إدارة الأمن السيبراني بالحمادي القابضة على أساس منتظم.
364	Translated (0%)	Activities shall be logged in accordance with the regulatory, audit and risk management objectives.	.يجب تسجيل الأنشطة وفقًا للأهداف التنظيمية والتدقيق وإدارة المخاطر
365	Translated	Successful and failed access activities for authentication and	.يجب تسجيل أنشطة الوصول الناجحة والفاشلة للمصادقة والتفويضات

	(0%)	authorizations shall be logged.	
366	Translated (0%)	Activities on system or application privileged accounts shall be logged and reviewed.	.يجب تسجيل الأنشطة على الحسابات المميزة للنظام أو التطبيق ومراجعتها
367	Translated (0%)	The event log sources, and logging systems must be configured to transport logs over reliable and commonly used event log transport protocols such as syslog, Windows Instrumentation Interface (WMI), SNMP traps, etc.	يجب تكوين مصادر سجل الأحداث وأنظمة التسجيل لنقل السجلات عبر بروتوكولات نقل سجل الأحداث الموثوقة والشائعة الاستخدام مثل سجل النظام .وما إلى ذلك SNMP ومصائد Windows (WMI) وواجهة أجهزة
368	Translated (0%)	All event logs must be collected from the sources specified under this requirement:	:يجب جمع جميع سجلات الأحداث من المصادر المحددة بموجب هذا الشرط
369	Translated (0%)	Systems, including Operating Systems, Databases, Storage, Networks, Applications, etc., covering system events and security/audit logs.	الأنظمة، بما في ذلك أنظمة التشغيل وقواعد البيانات والتخزين والشبكات .والتطبيقات وما إلى ذلك، التي تغطي أحداث النظام وسجلات الأمان/التدقيق
370	Translated (0%)	Critical Systems, including Operating Systems, Databases, Storage, Networks, Applications, etc., covering system events and security/audit logs.	الأنظمة الحيوية، بما في ذلك أنظمة التشغيل وقواعد البيانات والتخزين والشبكات .والتطبيقات وما إلى ذلك، والتي تغطي أحداث النظام وسجلات الأمان/التدقيق
371	Translated (0%)	Events of sensitive and privileged accounts.	.أحداث الحسابات الحساسة والمميزة
372	Translated (0%)	Operating System Events (e.g., Linux)	(Linux ،على سبيل المثال) أحداث نظام التشغيل
373	Translated (0%)	Database Events	أحداث قاعدة البيانات
374	Translated (0%)	Security solution events (e.g., Web application Firewall (WAF), Data Loss Prevention (DLP), Multifactor Authentication (MFA), etc.)	منع ،(WAF) أحداث الحلول الأمنية (على سبيل المثال، جدار حماية تطبيق الويب .(إلخ ،(MFA) المصادقة متعددة العوامل ،(DLP) فقدان البيانات
375	Translated (0%)	Logs generated in the events of Internet browsing, Internet connections and Wi-Fi connections.	السجلات التي تم إنشاؤها في أحداث تصفح الإنترنت واتصالات الإنترنت .Wi - Fi واتصالات
376	Translated (0%)	Events generating from data transfer to external storage.	.الأحداث الناتجة عن نقل البيانات إلى التخزين الخارجي
377	Translated (0%)	File Integrity Monitoring (FIM) event logs.	.(FIM) سجلات أحداث مراقبة سلامة الملفات
378	Translated (0%)	Event logs generated from system configuration changes, system updates and patches, and application changes.	سجلات الأحداث الناتجة عن تغييرات تكوين النظام وتحديثات النظام .والتصحيحات وتغييرات التطبيق
379	Translated (0%)	Abnormal activities such as those detected by Intrusion Prevention System (IPS).	.(IPS) الأنشطة غير الطبيعية مثل تلك التي اكتشفها نظام منع التسلل
380	Translated (0%)	Events generated by security solutions including Antimalware, Remote-Access Technologies (such as Virtual Private Network VPN), Web Proxies, Vulnerability Management Software, Host Intrusion Prevention System (HIPS), Authentication Servers, etc.	الأحداث الناتجة عن الحلول الأمنية بما في ذلك مكافحة البرامج الضارة، وتقنيات ووكلاء الويب، وبرامج ،(للشبكة الخاصة الافتراضية VPN مثل) الوصول عن بعد وخوادم المصادقة، وما ،(HIPS) إدارة الثغرات الأمنية، ونظام منع تسلل المضيفين .إلى ذلك
381	Translated	Events generated by perimeter devices including firewalls, routers,	الأحداث الناتجة عن الأجهزة المحيطة بما في ذلك جدران الحماية وأجهزة

	(0%)	traffic managers, etc.	.التوجيه ومديري حركة المرور وما إلى ذلك
382	Translated (0%)	Sysmon Event Logs (SEL), a Microsoft tool that records events that the operating system does not log and is very important and useful in security monitoring and incident response.	وهي أداة من مايكروسوفت تسجل الأحداث ،(SEL) سجلات أحداث سيسمون التي لا يسجلها نظام التشغيل وهي مهمة جدًا ومفيدة في المراقبة الأمنية .والاستجابة للحوادث
383	Translated (0%)	Events generated by virtualization environments and their underlying tools and infrastructure.	.الأحداث الناتجة عن بيئات المحاكاة الافتراضية وأدواتها وبنيتها التحتية الأساسية
384	Translated (0%)	Enable Domain Name System (DNS) query logging wherever technically applicable.	.حيثما ينطبق ذلك تقنيًا (DNS) تمكين تسجيل استعلام نظام أسماء النطاقات
385	Translated (0%)	Event logs generated by Industrial Control Systems (ICS).	.(ICS) سجلات الأحداث التي تم إنشاؤها بواسطة أنظمة التحكم الصناعية
386	Translated (0%)	Event logs shall include, when relevant:	:يجب أن تتضمن سجلات الأحداث، عند الاقتضاء
387	Translated (0%)	user IDs.	.معرّفات المستخدم
388	Translated (0%)	system activities.	.أنشطة النظام
389	Translated (0%)	dates, times and details of key events, e.g., log-on and log-off.	تواريخ وأوقات وتفاصيل الأحداث الرئيسية، على سبيل المثال، تسجيل الدخول .وتسجيل الخروج
390	Translated (0%)	device identity or location if possible and system identifier.	.هوية الجهاز أو موقعه إن أمكن ومعرف النظام
391	Translated (0%)	records of successful and rejected system access attempts.	.سجلات محاولات الوصول إلى النظام الناجحة والمرفوضة
392	Translated (0%)	records of successful and rejected data	سجلات البيانات الناجحة والمرفوضة
393	Translated (0%)	resource access attempts.	.محاولات الوصول إلى الموارد
394	Translated (0%)	changes to system configuration.	.تغييرات في تكوين النظام
395	Translated (0%)	use of privileges.	.استخدام الامتيازات
396	Translated (0%)	use of system utilities and applications.	.استخدام أدوات النظام وتطبيقاته
397	Translated (0%)	files accessed and the kind of access.	.الملفات التي تم الوصول إليها ونوع الوصول
398	Translated (0%)	network addresses and protocols.	.عناوين الشبكة والبروتوكولات
399	Translated (0%)	alarms raised by the access control system.	.الإنذارات الصادرة عن نظام التحكم في الوصول
400	Translated	activation and de-activation of protection systems, such as anti-	تفعيل أنظمة الحماية وإلغاء تنشيطها، مثل أنظمة مكافحة الفيروسات وأنظمة

	(0%)	virus systems and intrusion detection systems.	.الكشف عن التسلل
401	Translated (0%)	records of transactions executed by users in applications.	.سجلات المعاملات التي ينفذها المستخدمون في التطبيقات
402	Translated (0%)	Security event alerts generated from firewalls must be reviewed on a continuing basis to detect any unauthorized access attempts or unusual behavior.	يجب مراجعة تنبيهات الأحداث الأمنية الناتجة عن جدران الحماية بشكل مستمر .للكشف عن أي محاولات وصول غير مصرح بها أو سلوك غير عادي
403	Translated (0%)	Al Hammadi Holding can monitor alerts from firewalls, for example, by observing logs daily or by observing other system aspects such as access attempt patterns, characteristics of access, etc.	يمكن لشركة الحمادي القابضة مراقبة التنبيهات من جدران الحماية، على سبيل المثال، من خلال مراقبة السجلات يوميًا أو من خلال مراقبة جوانب النظام .الأخرى مثل أنماط محاولات الوصول وخصائص الوصول وما إلى ذلك
404	Translated (0%)	Monitoring devices must be deployed to monitor communications at the external boundary of the system (e.g., system perimeter) and at key internal boundaries (e.g., logical/physical interfaces within the information and technology asset) to discover anomalies, detect covert exfiltration of information and track specific types of transactions of interest to Al Hammadi Holding.	يجب نشر أجهزة المراقبة لمراقبة الاتصالات على الحدود الخارجية للنظام (على ،سبيل المثال، محيط النظام) وعلى الحدود الداخلية الرئيسية (على سبيل المثال الواجهات المنطقية/المادية داخل أصول المعلومات والتكنولوجيا) لاكتشاف الحالات الشاذة، واكتشاف التسريب السري للمعلومات وتتبع أنواع محددة من .المعاملات التي تهم شركة الحمادي القابضة
405	Translated (0%)	For example, Network segments where systems that are accessible from the Internet are located.	على سبيل المثال، شرائح الشبكة حيث توجد الأنظمة التي يمكن الوصول إليها من .الإنترنت
406	Translated (0%)	Monitoring tools must be employed to detect indicators of denial-of-service attacks against Al Hammadi Holding’s information and technology assets and infrastructure.	يجب استخدام أدوات المراقبة للكشف عن مؤشرات هجمات الحرمان من الخدمة .ضد أصول المعلومات والتكنولوجيا والبنية التحتية لشركة الحمادي القابضة
407	Translated (0%)	Alerts for information and technology assets must be generated when previously defined security monitoring events occur and/or thresholds for indications of potentially malicious activity are met.	يجب إنشاء تنبيهات لأصول المعلومات والتكنولوجيا عند حدوث أحداث مراقبة .أمنية محددة مسبقًا و/أو استيفاء عتبات مؤشرات النشاط الضار المحتمل
408	Translated (0%)	Specific thresholds for alerting on security monitoring events must be identified and documented.	.يجب تحديد عتبات محددة للتنبيه بشأن أحداث المراقبة الأمنية وتوثيقها
409	Translated (0%)	Thresholds must be periodically revised and updated to stay current with trending security attacks.	يجب مراجعة العتبات وتحديثها بشكل دوري للبقاء محدثة مع الهجمات الأمنية .الشائعة
410	Translated (0%)	Al Hammadi Holding shall implement appropriate privacy protection measures for logs which may contain sensitive data and personally identifiable information.	يجب على شركة الحمادي القابضة تنفيذ تدابير حماية الخصوصية المناسبة .للسجلات التي قد تحتوي على بيانات حساسة ومعلومات تعريف شخصية
411	Translated (0%)	Where possible, Al Hammadi Holding system administrators shall not have permission to erase or de-activate logs of their own activities.	حيثما أمكن، لن يكون لمسؤولي نظام الحمادي القابضة إذن بمسح أو إلغاء تنشيط .سجلات أنشطتهم الخاصة
412	Translated (0%)	Logs and audit trails shall be protected against unauthorized modification and the retention period shall be defined by Al Hammadi Holding.	يجب حماية السجلات ومسارات التدقيق من التعديل غير المصرح به ويجب .تحديد فترة الاحتفاظ من قبل شركة الحمادي القابضة
413	Translated (0%)	Access to log data shall only be allowed for:	:لا يُسمح بالوصول إلى بيانات السجل إلا في الحالات التالية

414	Translated (0%)	Technical and operational reasons.	.الأسباب الفنية والتشغيلية
415	Translated (0%)	When required to assist in investigations.	.عند الحاجة للمساعدة في التحقيقات
416	Translated (0%)	To comply with legal obligations or requests.	.الامتثال للالتزامات أو الطلبات القانونية
417	Translated (0%)	Al Hammadi Holding shall closely monitor and report on the following:	:تراقب شركة الحمادي القابضة عن كثب ما يلي وتقدم تقارير عنه
418	Translated (0%)	alterations to the message types that are recorded.	.التعديلات على أنواع الرسائل المسجلة
419	Translated (0%)	log files being edited or deleted.	.ملفات السجل التي يتم تحريرها أو حذفها
420	Translated (0%)	storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.	تجاوز سعة تخزين وسائط ملف السجل، مما يؤدي إما إلى الفشل في تسجيل .الأحداث أو الإفراط في كتابة الأحداث المسجلة السابقة
421	Translated (0%)	All event logs must be forwarded to a centralized log analytics or Security Information and Event Management (SIEM) system for log correlation, analysis and alerting.	يجب إعادة توجيه جميع سجلات الأحداث إلى تحليلات السجل المركزية أو نظام .لربط السجل وتحليله وتنبيهه (SIEM) إدارة المعلومات الأمنية والأحداث
422	Translated (0%)	Regular review on SIEM must be performed to monitor and detect abnormal behavior and anomalies.	لمراقبة واكتشاف السلوك غير الطبيعي SIEM يجب إجراء مراجعة منتظمة على .والشذوذ
423	Translated (0%)	SIEM system must be tuned on a regular basis to better identify actionable events and decrease event noise.	على أساس منتظم لتحديد الأحداث القابلة للتنفيذ بشكل SIEM يجب ضبط نظام .أفضل وتقليل ضوضاء الحدث
424	Translated (0%)	Event logs and alerts must be periodically reviewed, using manual and automated techniques.	يجب مراجعة سجلات الأحداث والتنبيهات بشكل دوري، باستخدام التقنيات .اليدوية والآلية
425	Translated (0%)	Significant unauthorized activity related to information and technology assets must be detected.	.يجب اكتشاف نشاط كبير غير مصرح به يتعلق بأصول المعلومات والتكنولوجيا
426	Translated (0%)	Misuse of privileged user accounts must be detected.	.يجب الكشف عن إساءة استخدام حسابات المستخدمين المتميزة
427	Translated (0%)	Centralized logging solutions must be treated as if they contain, at a minimum, Al Hammadi Holding's Secret and Confidential data, and as if they comply with all relevant confidentiality controls.	يجب التعامل مع حلول التسجيل المركزية كما لو أنها تحتوي، كحد أدنى، على البيانات السرية والسرية لشركة الحمادي القابضة، وكما لو أنها تمتثل لجميع .ضوابط السرية ذات الصلة
428	Translated (0%)	The use of monitoring and scanning devices or tools must be limited to authorized users.	يجب أن يقتصر استخدام أجهزة أو أدوات المراقبة والمسح الضوئي على .المستخدمين المصرح لهم
429	Translated (0%)	The results of all monitoring and scanning activities must be classified as Confidential, at minimum.	.يجب تصنيف نتائج جميع أنشطة المراقبة والمسح على أنها سرية، على الأقل
430	Translated (0%)	Al Hammadi Holding shall archive critical audit logs to retain evidence to incidents.	يجب على شركة الحمادي القابضة أرشفة سجلات التدقيق الحرجة للاحتفاظ .بالأدلة على الحوادث
431	Translated (100%)	Clock synchronization	مزامنة الساعة

432	Translated (0%)	Clock synchronization shall be implemented on all networking devices with agreed reference.	.يجب تنفيذ مزامنة الساعة على جميع أجهزة الشبكات مع الإشارة المتفق عليها
433	Translated (0%)	Al Hammadi Holding shall ensure that the date and time stamp of the audit trails for all system components are synchronized to facilitate the tracking of user's identity activities, and accuracy and consistency of audit logs.	تضمن شركة الحمادي القابضة مزامنة تاريخ ووقت مسارات التدقيق لجميع مكونات النظام لتسهيل تتبع أنشطة هوية المستخدم، ودقة واتساق سجلات التدقيق.
434	Translated (0%)	Al Hammadi Holding systems shall be linked to a national atomic clock as the master clock for logging systems.	يجب ربط أنظمة الحمادي القابضة بساعة ذرية وطنية كساعة رئيسية لأنظمة قطع الأشجار.
435	Translated (0%)	Al Hammadi Holding shall use a network time protocol to keep all of the servers in synchronization with the master clock.	يجب على شركة الحمادي القابضة استخدام بروتوكول وقت الشبكة للحفاظ على تزامن جميع الخوادم مع الساعة الرئيسية.
436	Translated (100%)	Control of operational software	التحكم في البرمجيات التشغيلية
437	Translated (0%)	Al Hammadi Holding shall control all software installations to ensure the integrity of operational systems.	تتحكم شركة الحمادي القابضة في جميع تركيبات البرامج لضمان سلامة الأنظمة التشغيلية.
438	Translated (0%)	Installation of software on operational systems	تثبيت البرامج على الأنظمة التشغيلية
439	Translated (0%)	All Al Hammadi Holding updates of the operational software, applications and program libraries shall only be performed by trained administrators upon appropriate management authorization.	يجب ألا يتم تنفيذ جميع تحديثات شركة الحمادي القابضة للبرمجيات التشغيلية والتطبيقات ومكتبات البرامج إلا من قبل إداريين مدربين بناءً على إذن إداري مناسب.
440	Translated (0%)	Al Hammadi Holding operational systems shall only hold approved executable code and not development code or compilers.	يجب أن تحتوي الأنظمة التشغيلية لشركة الحمادي القابضة فقط على رمز قابل للتنفيذ معتمد وليس رمز تطوير أو مجمعين.
441	Translated (0%)	Al Hammadi Holding applications and operating system software shall only be implemented after extensive and successful testing.	يجب ألا يتم تنفيذ تطبيقات الحمادي القابضة وبرامج نظام التشغيل إلا بعد إجراء اختبارات مكثفة وناجحة.
442	Translated (0%)	Tests shall cover usability, security, effects on other systems and user-friendliness and shall be carried out on separate systems.	يجب أن تغطي الاختبارات قابلية الاستخدام والأمان والتأثيرات على الأنظمة الأخرى وسهولة الاستخدام ويجب إجراؤها على أنظمة منفصلة.
443	Translated (0%)	Al Hammadi Holding shall use a configuration control system to keep control of all implemented software as well as the system documentation.	يجب أن تستخدم شركة الحمادي القابضة نظام التحكم في التكوين للحفاظ على التحكم في جميع البرامج المنفذة بالإضافة إلى وثائق النظام.
444	Translated (0%)	A rollback strategy shall be in place before changes are implemented.	.يجب وضع استراتيجية التراجع قبل تنفيذ التغييرات
445	Translated (0%)	An audit log shall be maintained of all updates.	.يجب الاحتفاظ بسجل تدقيق لجميع التحديثات
446	Translated (0%)	Al Hammadi Holding previous versions of application software shall be retained as a contingency measure.	يجب الاحتفاظ بالإصدارات السابقة من برمجيات التطبيق لشركة الحمادي القابضة كإجراء طارئ.
447	Translated (0%)	Al Hammadi Holding old versions of software shall be archived, together with all required information and parameters, procedures, configuration details and supporting software for as long as the data are retained in archive.	يجب أرشفة الإصدارات القديمة من برامج شركة الحمادي القابضة، جنبًا إلى جنب مع جميع المعلومات والمعلمات والإجراءات وتفاصيل التكوين والبرامج الداعمة المطلوبة طالما يتم الاحتفاظ بالبيانات في الأرشيف.

448	Translated (0%)	Vendor supplied software used in operational systems shall be maintained at a level supported by the supplier.	يجب الحفاظ على البرامج التي يوفرها البائع والمستخدمة في الأنظمة التشغيلية عند مستوى يدعمه المورد.
449	Translated (100%)	Technical vulnerability management	إدارة الثغرات التقنية
450	Translated (0%)	The Al Hammadi Holding must perform a Vulnerabilities Assessment periodically, to discover and evaluate gaps and flaws in a timely manner and remediate them effectively.	يجب على شركة الحمادي القابضة إجراء تقييم نقاط الضعف بشكل دوري، لاكتشاف وتقييم الثغرات والعيوب في الوقت المناسب ومعالجتها بشكل فعال.
451	Translated (0%)	The Cyber Security Department shall define the systems, services, and technical components on which vulnerabilities are going to be assessed, in accordance with relevant legislative and regulatory requirements.	تحدد إدارة الأمن السيبراني الأنظمة والخدمات والمكونات الفنية التي سيتم تقييم نقاط الضعف عليها، وفقًا للمتطلبات التشريعية والتنظيمية ذات الصلة.
452	Translated (0%)	The Cybersecurity Department must ensure that uses qualified and trusted tools to discover the vulnerabilities.	يجب على إدارة الأمن السيبراني التأكد من استخدام أدوات مؤهلة وموثوقة لاكتشاف نقاط الضعف.
453	Translated (0%)	If the vulnerabilities assessment is carried out by external service providers or a third party on behalf of the Al Hammadi Holding, it must be verified that all cybersecurity requirements relevant to third parties are applied in accordance with the third-party policy approved in the Al Hammadi Holding.	إذا تم إجراء تقييم نقاط الضعف من قبل مقدمي الخدمات الخارجيين أو طرف ثالث نيابة عن شركة الحمادي القابضة، فيجب التحقق من أن جميع متطلبات الأمن السيبراني ذات الصلة بأطراف ثالثة يتم تطبيقها وفقًا لسياسة الطرف الثالث المعتمدة في شركة الحمادي القابضة.
454	Translated (0%)	Appropriate informative communication channels shall be maintained and established to obtain latest details of technical vulnerabilities.	يجب الحفاظ على قنوات الاتصال الإعلامية المناسبة وإنشاءها للحصول على أحدث تفاصيل نقاط الضعف الفنية.
455	Translated (0%)	Al Hammadi Holding shall implement a controlled environment in order to safeguard systems against technical vulnerabilities.	يجب على شركة الحمادي القابضة تنفيذ بيئة خاضعة للرقابة من أجل حماية الأنظمة من الثغرات الفنية.
456	Translated (0%)	Al Hammadi Holding shall establish procedures for periodic security testing of IT systems and services.	يجب على شركة الحمادي القابضة وضع إجراءات للاختبار الأمني الدوري لأنظمة وخدمات تكنولوجيا المعلومات.
457	Translated (0%)	Al Hammadi Holding shall develop vulnerability management program including its associated procedures and processes to cover the following activities at a minimum:	يجب على شركة الحمادي القابضة تطوير برنامج إدارة الثغرات الأمنية بما في ذلك الإجراءات والعمليات المرتبطة به لتغطية الأنشطة التالية كحد أدنى:
458	Translated (100%)	Roles and responsibilities	الأدوار والمسؤوليات
459	Translated (0%)	Vulnerability scanning, patching and monitoring	مسح الثغرات الأمنية وتصحيحها ومراقبتها
460	Translated (0%)	Vulnerability risk assessment and assigning risk ratings	تقييم مخاطر الضعف وتعيين تصنيفات المخاطر
461	Translated (0%)	Risk treatment and any coordination responsibilities required.	معالجة المخاطر وأي مسؤوليات تنسيقية مطلوبة.
462	Translated (0%)	Periodic configuration and logs reviews shall be performed to identify potential weaknesses.	يجب إجراء مراجعات دورية للتكوين والسجلات لتحديد نقاط الضعف المحتملة.
463	Translated	A current and complete inventory of IT assets shall be maintained	يجب الاحتفاظ بجرد حالي وكامل لأصول تكنولوجيا المعلومات لإدارة الثغرات

	(0%)	for vulnerability management.	.الأمنية
464	Translated (0%)	Patching mechanism shall be established so that security patches are deployed periodically as addressed in the information system acquisition, development and management policy.	يجب إنشاء آلية التصحيح بحيث يتم نشر التصحيحات الأمنية بشكل دوري كما .هو موضح في سياسة الحصول على نظام المعلومات وتطويره وإدارته
465	Translated (0%)	Vulnerability scanners shall reference up-to-date vulnerability databases.	يجب أن تشير ماسحات الثغرات الأمنية إلى قواعد بيانات الثغرات الأمنية .المحدثة
466	Translated (0%)	Issues identified by vulnerability scanning shall be regularly reviewed and addressed with appropriate urgency.	يجب مراجعة المشكلات التي يتم تحديدها عن طريق فحص الثغرات الأمنية .بانتظام ومعالجتها على وجه السرعة المناسبة
467	Translated (0%)	External vendors shall be considered for security assessments.	.يجب النظر في البائعين الخارجيين للتقييمات الأمنية
468	Translated (0%)	Public-facing web applications shall be periodically tested, at least annually and after any changes.	يجب اختبار تطبيقات الويب العامة بشكل دوري، على الأقل سنويًا وبعد أي .تغييرات
469	Translated (0%)	Periodic code reviews shall be performed on information systems and applications developed in-house or by an external party.	يجب إجراء مراجعات دورية للأكواد على أنظمة المعلومات والتطبيقات التي تم .تطويرها داخليًا أو من قبل طرف خارجي
470	Translated (0%)	A process to detect the presence of authorized and unauthorized wireless access points shall be defined.	يجب تحديد عملية للكشف عن وجود نقاط وصول لاسلكية مصرح بها وغير .مصرح بها
471	Translated (0%)	For service and systems that are hosted on the cloud, the vulnerability management requirements of the cloud security policy shall be addressed.	بالنسبة للخدمة والأنظمة المستضافة على السحابة، يجب معالجة متطلبات إدارة .الثغرات الأمنية لسياسة الأمن السحابي
472	Translated (0%)	The Al Hammadi Holding shall subscribe to cybersecurity threat intelligence solutions that provide proactive feeds and engage with cybersecurity groups and external experts on the topics relevant, to learn the new threats, and proactively reduce existing vulnerabilities risks.	يجب على شركة الحمادي القابضة الاشتراك في حلول استخبارات تهديدات الأمن السيبراني التي توفر خلاصات استباقية والمشاركة مع مجموعات الأمن السيبراني ،والخبراء الخارجيين في الموضوعات ذات الصلة، لمعرفة التهديدات الجديدة .والحد بشكل استباقي من مخاطر نقاط الضعف الحالية
473	Translated (0%)	Vulnerability management requirements shall be reviewed periodically to manage the vulnerabilities of the Al Hammadi Holding	يجب مراجعة متطلبات إدارة الثغرات الأمنية بشكل دوري لإدارة ثغرات شركة الحمادي القابضة
474	Translated (0%)	Vulnerabilities Assessments Requirements	متطلبات تقييم نقاط الضعف
475	Translated (0%)	Vulnerability assessment shall be conducted before go-live on the Internet or after making any changes to critical systems in accordance with the change management policy.	يجب إجراء تقييم نقاط الضعف قبل بدء التشغيل على الإنترنت أو بعد إجراء أي .تغييرات على الأنظمة الحيوية وفقًا لسياسة إدارة التغيير
476	Translated (0%)	Vulnerabilities must be rated based on associated risk levels.	.يجب تصنيف نقاط الضعف بناءً على مستويات المخاطر المرتبطة بها
477	Translated (0%)	Vulnerabilities remediation must be rated based on classification and associated risk levels.	يجب تصنيف معالجة نقاط الضعف بناءً على التصنيف ومستويات المخاطر .المرتبطة به
478	Translated (0%)	Al Hammadi Holding shall periodically perform a vulnerability assessment on all technical assets along with the remediation.	يجب على شركة الحمادي القابضة إجراء تقييم دوري للضعف على جميع الأصول .الفنية إلى جانب المعالجة
479	Translated	Al Hammadi Holding shall perform a vulnerability assessment on	يجب على شركة الحمادي القابضة إجراء تقييم للضعف على الأصول الحيوية

	(0%)	the technical and internal critical assets every year, and along with the remediation.	.الفنية والداخلية كل عام، جنبًا إلى جنب مع المعالجة
480	Translated (0%)	Vulnerability scanning shall be performed on IT systems yearly or in case of a significant change in the network.	يجب إجراء مسح الثغرات الأمنية على أنظمة تكنولوجيا المعلومات سنويًا أو في .حالة حدوث تغيير كبير في الشبكة
481	Translated (0%)	Al Hammadi Holding shall perform a vulnerability assessment on the technical and external critical assets publicly facing the Internet once a year.	يجب على شركة الحمادي القابضة إجراء تقييم للضعف على الأصول الفنية .والخارجية الهامة التي تواجه الإنترنت علنًا مرة واحدة في السنة
482	Translated (0%)	For systems that are storing and processing card holder data, vulnerability scanning shall be performed by qualified personnel independent from.	بالنسبة للأنظمة التي تقوم بتخزين ومعالجة بيانات حامل البطاقة، يجب إجراء .فحص الثغرات الأمنية بواسطة موظفين مؤهلين مستقلين عن
483	Translated (0%)	Vulnerabilities Remediation Requirements	متطلبات معالجة الثغرات الأمنية
484	Translated (0%)	Vulnerability assessment reports shall be prepared after assessment completion to contain identified vulnerabilities and the recommendations proposed for remediation.	يجب إعداد تقارير تقييم الضعف بعد الانتهاء من التقييم لاحتواء نقاط الضعف .المحددة والتوصيات المقترحة للمعالجة
485	Translated (0%)	After the remediation of the vulnerabilities by the mandated departments, it is necessary to re-assess the vulnerabilities again to ensure that they are properly fixed.	بعد معالجة نقاط الضعف من قبل الإدارات المكلفة، من الضروري إعادة تقييم .نقاط الضعف مرة أخرى لضمان إصلاحها بشكل صحيح
486	Translated (0%)	Updates and patches shall be acquired from trusted and secure sources and in accordance with the patch management policy.	يجب الحصول على التحديثات والتصحيحات من مصادر موثوقة وآمنة ووفقًا .لسياسة إدارة التصحيح
487	Translated (0%)	Critical Vulnerabilities shall be fixed and closed, following the change management policy of the Al Hammadi Holding.	يجب إصلاح نقاط الضعف الحرجة وإغلاقها، باتباع سياسة إدارة التغيير الخاصة .بشركة الحمادي القابضة
488	Translated (0%)	If a vulnerability cannot be repaired and closed for any reason or limitations, alternative security controls shall be applied such as stopping the service causing the vulnerability.	إذا تعذر إصلاح الثغرة الأمنية وإغلاقها لأي سبب أو قيود، فيجب تطبيق ضوابط .أمنية بديلة مثل إيقاف الخدمة التي تسبب الثغرة الأمنية
489	Translated (0%)	Or providing a compensating control such as blocking access via firewalls, monitor the vulnerability through monitoring tools, and inform the incident response team of this vulnerability and the possibility of exploiting it.	أو توفير تحكم تعويضي مثل منع الوصول عبر جدران الحماية، ومراقبة الثغرة الأمنية من خلال أدوات المراقبة، وإبلاغ فريق الاستجابة للحوادث بهذه الثغرة .وإمكانية استغلالها
490	Translated (0%)	Penetration Test	اختبار الاختراق
491	Translated (0%)	Rules of engagement document must be developed prior to <2743>2743/>>the Penetration <2749>2749/>>Testing process, <2755>2755/>>which must cover the scope of testing, <2761> </2761>privileges, duration<2767>2767/>>, target systems, testing mechanism, general conditions and requirements, etc.	،يجب وضع وثيقة قواعد الاشتباك قبل عملية <2743><2743/>اختبار الاختراق ،والتي يجب أن <2755><2755/>تغطي نطاق الاختبار<2749></2749> ،<والامتيازات، والمدة<2761><2761/>، والأنظمة المستهدفة<2767><2767/ .وآلية الاختبار، والشروط والمتطلبات العامة، وما إلى ذلك
492	Translated (0%)	<2773>2773/>>The scope of penetration testing must include all technology components including: infrastructure, websites, web applications, smart phones and tablets applications, emails, and	يجب أن يشمل نطاق اختبار الاختراق جميع مكونات<2773></2773> التكنولوجيا بما في ذلك: البنية التحتية ومواقع الويب وتطبيقات الويب وتطبيقات الهواتف الذكية والأجهزة اللوحية ورسائل البريد الإلكتروني والوصول عن بُعد

		remote access, OT/ICS network environment in accordance with the relevant legal and regulatory requirements.	.وفقًا للمتطلبات القانونية والتنظيمية ذات الصلة OT/ICS وبيئة شبكة
493	Translated (0%)	<2779>2779/>>Penetration Testing must be conducted <2785> </2785>to evaluate and test the efficiency of cybersecurity capabilities regularly.	<2779/> يجب إجراء اختبار <2785/><2785>الاختراق لتقييم<2779> .واختبار كفاءة قدرات الأمن السيبراني بانتظام
494	Translated (0%)	Penetration testing must be conducted on critical systems, their technology components and all their internal and external services at least every six months.	يجب إجراء اختبار الاختراق على الأنظمة الحيوية ومكوناتها التكنولوجية وجميع .خدماتها الداخلية والخارجية كل ستة أشهر على الأقل
495	Translated (0%)	<2794>2794/>>Penetration testing <2800>2800/>>must be conducted on <2806>2806/>>telework systems and all externally provided services (through the internet) and their technology components at least once a year.	<2794/>يجب إجراء اختبار <2800/><2800>الاختراق على أنظمة<2794> العمل <2806/><2806>عن بعد وجميع الخدمات المقدمة من الخارج (عبر .الإنترنت) ومكوناتها التكنولوجية مرة واحدة على الأقل في السنة
496	Translated (0%)	<2812>2812/>>Ensure <2818>2818/>>that the testing effect is limited on <2824>2824/>>the production environment (operating environment<2830>2830/>>) or <2836>2836/>>conduct penetration testing <2842>2842/>>in an identical separate environment.	تأكد <2818/><2818>من أن تأثير الاختبار يقتصر على<2812></2812> بيئة الإنتاج (بيئة التشغيل<2830>)<2830/> أو قم<2824></2824> بإجراء اختبار الاختراق <2842/><2842>في بيئة منفصلة<2836></2836> .متطابقة
497	Translated (0%)	Passive testing must be conducted to review and examine systems, applications, networks, policies and procedures, and detect security vulnerabilities.	يجب إجراء اختبار سلبي لمراجعة وفحص الأنظمة والتطبيقات والشبكات .والسياسات والإجراءات واكتشاف الثغرات الأمنية
498	Translated (0%)	A plan for penetration testing that covers scope of work, start date, end date, methodology, and real-world attack scenarios must be developed and approved.	يجب وضع خطة لاختبار الاختراق تغطي نطاق العمل وتاريخ البدء وتاريخ .الانتهاء والمنهجية وسيناريوهات الهجوم في العالم الحقيقي والموافقة عليها
499	Translated (0%)	Ensure that the penetration testing does not impact systems and provided services in Al Hammadi Holding<2866>2866/>>.	التأكد من أن اختبار الاختراق لا يؤثر على الأنظمة والخدمات المقدمة في شركة .الحمادي<2866/><2866> القابضة
500	Translated (0%)	<2872>2872/>>A qualified team with relevant certificates and experience must be appointed to ensure <2878>2878/>>effective <2884>2884/>>penetration testing <2890>2890/>>.	<2872/> يجب تعيين فريق مؤهل يتمتع بالشهادات والخبرة ذات الصلة<2872> لضمان <2878/><2878>اختبار <2884/><2884>الاختراق الفعال. <2890> </2890>
501	Translated (0%)	Penetration testing team must coordinate with stakeholders from Al Hammadi Holding to follow the approved procedures and penetration testing plans, conduct the necessary analysis in order to define the false positive indicators, classify vulnerabilities and determine their causes.	يجب على فريق اختبار الاختراق التنسيق مع أصحاب المصلحة من شركة الحمادي القابضة لمتابعة الإجراءات المعتمدة وخطط اختبار الاختراق وإجراء التحليل اللازم من أجل تحديد المؤشرات الإيجابية الخاطئة وتصنيف نقاط .الضعف وتحديد أسبابها
502	Translated (0%)	<2905>2905/>>Penetration testing data must be processed in a secure manner and must be collected, stored, transferred<2911> </2911>, and removed <2917>2917/>>when it becomes unnecessary according to Al Hammadi Holding Information Protection Policy.	يجب معالجة بيانات اختبار الاختراق بطريقة آمنة ويجب<2905></2905> جمعها وتخزينها ونقلها وإزالتها<2911/><2911> عندما تصبح غير ضرورية وفقًا لسياسة حماية معلومات شركة الحمادي<2917></2917> .القابضة
503	Translated	Penetration testing must be conducted to discover <2932>	يجب إجراء اختبار الاختراق لاكتشاف نقاط <2932/><2932>الضعف بجميع

	(0%)	</2932>vulnerabilities of all forms, including vulnerabilities <2938>2938/>>that usually result from <2944>2944/>>application development errors without taking into account the <2950> </2950>Secure Code Development <2956>2956/>>and Misconfigurations <2962>2962/>>standard as well as the Exploitability of Identified Vulnerability.	أشكالها، بما في <2938><2938/>ذلك نقاط الضعف التي تنتج عادة عن أخطاء تطوير<2944/>التطبيقات دون <2950><2950/>مراعاة معيار<2944> <2956>تطوير/> التعليمات البرمجية الآمنة <2962><2962/> والتكوينات الخاطئة وكذلك قابلية استغلال نقاط الضعف المحددة.
504	Translated (0%)	<2968>2968/>>If a third party is assigned to conduct penetration testing on behalf of Al Hammadi Holding <2980>2980/>>, third party cybersecurity requirements must be verified <2986> </2986>as per Al Hammadi Holding's <2998>2998/>>Supplier Relationship Security Policy.	إذا تم تعيين طرف ثالث لإجراء اختبار الاختراق نيابة عن<2968></2968> شركة الحمادي القابضة، <2980><2980/>فيجب التحقق من متطلبات الأمن السيبراني للطرف <2986><2986/>الثالث وفقًا لسياسة أمن علاقات الموردين الخاصة بشركة الحمادي القابضة<2998></2998>.
505	Translated (0%)	A report must be developed stating the testing results, recommendations must be made after completion of the penetration testing process.	يجب وضع تقرير يوضح نتائج الاختبار، ويجب تقديم التوصيات بعد الانتهاء من عملية اختبار الاختراق.
506	Translated (0%)	Penetration testing results must be classified based on their sensitivity, and remediated according to their cyber risks <3019> </3019>as per Al Hammadi Holding risk management methodology	يجب تصنيف نتائج اختبار الاختراق بناءً على حساسيتها، ومعالجتها وفقًا لمخاطرها السيبرانية <3019><3019/>وفقًا لمنهجية إدارة مخاطر شركة الحمادي القابضة
507	Translated (0%)	An action plan must be developed to remediate penetration testing results and illustrate risk impacts, treatment mechanism, implementation owner, <3034>3034/>>duration and monitoring<3040>3040/>>.	يجب وضع خطة عمل لمعالجة نتائج اختبار الاختراق وتوضيح آثار المخاطر وآلية المعالجة ومسؤول <3034><3034/>التنفيذ والمدة والمراقبة <3040></3040>.
508	Translated (0%)	User accounts <3049>3049/>>used to conduct penetration testing must be managed <3055>3055/>>and monitored to ensure that they are only used for legitimate purposes and removed after testing.	يجب <3049>إدارة/> حسابات المستخدمين المستخدمة لإجراء اختبار الاختراق ومراقبتها للتأكد من استخدامها فقط لأغراض<3055></3055> مشروعة وإزالتها بعد الاختبار.
509	Translated (0%)	<3064>3064/>>Procedures <3070>3070/>>and standards <3076> </3076>for penetration <3082>3082/>>testing <3088> </3088>must be developed <3094>3094/>>based <3100> </3100>on <3106>3106/>>business need<3112>3112/>>.	يجب <3070><3070/><3064>تطوير/><3076><3076/>إجراءات ومعايير <3082><3082/>اختبار <3088><3088/>الاختراق بناءً على <3100><3100/>حاجة <3106><3106/>العمل<3094></3094> <3112>.</3112>
510	Translated (0%)	<3118>Key performance indicators must be used to </3118><3124><3122>ensure the continuous improvement and effective and efficient use of</3122></3124><3127> Penetration Testing <3130>3130/>>requirements.</3127>	يجب استخدام مؤشرات الأداء الرئيسية لضمان<3118> التحسين المستمر والاستخدام الفعال والفعال<3122></3118><3124> لمتطلبات اختبار <3130><3130/>الاختراق <3127></3122></3124> </3127>.
511	Translated (0%)	Al Hammadi Holding IT departments is responsible for the managing and implementing the Penetration testing with a supervision by the Cybersecurity department	أقسام تكنولوجيا المعلومات في شركة الحمادي القابضة مسؤولة عن إدارة وتنفيذ اختبار الاختراق تحت إشراف قسم الأمن السيبراني
512	Translated (0%)	Restrictions on software installation	القيود المفروضة على تثبيت البرامج

513	Translated (0%)	Rules governing the installation of software by users shall be established and implemented.	.يجب وضع وتنفيذ القواعد التي تحكم تثبيت البرامج من قبل المستخدمين
514	Translated (0%)	Users shall not be given administrative rights, users to have the ability to install software.	لا يجوز منح المستخدمين حقوقًا إدارية، ويجب أن يتمتع المستخدمون بالقدرة .على تثبيت البرامج
515	Translated (0%)	Al Hammadi Holding shall define and enforce strict policy on which types of software users may install.	يجب على شركة الحمادي القابضة تحديد وإنفاذ سياسة صارمة بشأن أنواع .البرامج التي يمكن للمستخدمين تثبيتها
516	Translated (0%)	The principle of least privilege shall be applied.	.يطبق مبدأ الحد الأدنى من الامتيازات
517	Translated (0%)	Al Hammadi Holding shall identify what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software that is only for personal use and software whose pedigree regarding being potentially malicious is unknown or suspect).	يجب أن تحدد شركة الحمادي القابضة أنواع تثبيتات البرامج المسموح بها (على سبيل المثال، التحديثات والتصحيحات الأمنية للبرامج الحالية) وأنواع التثبيتات المحظورة (على سبيل المثال، البرامج المخصصة للاستخدام الشخصي فقط والبرامج التي تكون نسبها فيما يتعلق باحتمال كونها ضارة غير معروفة أو .(مشبوهة
518	Translated (0%)	Any given privileges shall be granted having regard to the roles of the users concerned.	.تُمنح أي امتيازات معينة مع مراعاة أدوار المستخدمين المعنيين
519	Translated (0%)	Al Hammadi Holding shall prepare a whitelist of the allowed applications to be installed at Al Hammadi Holding's information assets including but not limited to workstations, application servers, database servers and other operating servers at Al Hammadi Holding work environment.	تقوم شركة الحمادي القابضة بإعداد قائمة بيضاء بالتطبيقات المسموح بتثبيتها في أصول معلومات شركة الحمادي القابضة بما في ذلك على سبيل المثال لا الحصر محطات العمل وخوادم التطبيقات وخوادم قواعد البيانات وخوادم التشغيل .الأخرى في بيئة عمل شركة الحمادي القابضة
520	Translated (0%)	Al Hammadi Holding shall restrict installation of any non-allowed applications or software's either at clients or servers and the list of the allowed applications shall be documented.	يجب على شركة الحمادي القابضة تقييد تثبيت أي تطبيقات أو برامج غير مسموح بها إما على العملاء أو الخوادم ويجب توثيق قائمة التطبيقات المسموح .بها
521	Translated (0%)	The anti-malware solution shall also publish the whitelist of the allowed applications and in case of any suspicious attempt for any not allowed application to be installed the anti-malware solution can block this attempt.	يجب أن ينشر حل مكافحة البرامج الضارة أيضًا القائمة البيضاء للتطبيقات المسموح بها وفي حالة وجود أي محاولة مشبوهة لتثبيت أي تطبيق غير مسموح .به، يمكن لحل مكافحة البرامج الضارة منع هذه المحاولة
522	Translated (100%)	Information systems audit considerations	اعتبارات تدقيق أنظمة المعلومات
523	Translated (0%)	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.	يجب التخطيط بعناية لمتطلبات وأنشطة التدقيق التي تنطوي على التحقق من .الأنظمة التشغيلية والاتفاق عليها لتقليل الاضطرابات في العمليات التجارية
524	Translated (0%)	Audit requirements for access to Al Hammadi Holding systems and data shall be agreed with appropriate management.	يجب الاتفاق على متطلبات التدقيق للوصول إلى أنظمة وبيانات شركة الحمادي .القابضة مع الإدارة المناسبة
525	Translated (0%)	Scope of technical audit tests and the required access shall be agreed and controlled.	.يجب الاتفاق على نطاق اختبارات التدقيق الفني والوصول المطلوب والتحكم فيه
526	Translated (0%)	Audit tests shall be limited to read-only access to software and data.	.يجب أن تقتصر اختبارات التدقيق على الوصول للقراءة فقط إلى البرامج والبيانات

527	Translated (0%)	Access, other than read-only, shall only be allowed for copies of systems.	.يجب السماح بالوصول، بخلاف القراءة فقط، فقط لنسخ الأنظمة
528	Translated (0%)	Access shall be erased when the audit is completed or given appropriate protection if there is an approved obligation.	يجب محو الوصول عند اكتمال التدقيق أو منح الحماية المناسبة إذا كان هناك .التزام معتمد
529	Translated (0%)	Audit tests that could affect system availability shall be run outside business hours.	.يجب إجراء اختبارات التدقيق التي قد تؤثر على توفر النظام خارج ساعات العمل
530	Translated (0%)	A periodic audit of the Cybersecurity practices and processes shall be conducted to determine whether the control objectives, processes and procedures of the Cybersecurity team:	يجب إجراء تدقيق دوري لممارسات وعمليات الأمن السيبراني لتحديد ما إذا كانت :أهداف وعمليات وإجراءات الرقابة لفريق الأمن السيبراني
531	Translated (0%)	meet the requirements of applicable standards and industry good practices	تلبية متطلبات المعايير المعمول بها والممارسات الجيدة في الصناعة
532	Translated (0%)	meet regulatory, legislative and contractual requirements	تلبية المتطلبات التنظيمية والتشريعية والتعاقدية
533	Translated (0%)	meet the Information Security requirements defined in the Information Security policy and associated policies.	تلبية متطلبات أمن المعلومات المحددة في سياسة أمن المعلومات والسياسات .ذات الصلة
534	Translated (0%)	are effectively implemented and maintained as designed.	.تُنفذ وتُحفظ بالكامل كما هو مخطط لها
535	Translated (0%)	Information systems must be regularly reviewed for compliance with the Al Hammadi Holding's Cybersecurity policies and standards.	يجب مراجعة أنظمة المعلومات بانتظام للتأكد من امتثالها لسياسات ومعايير الأمن .السيبراني لشركة الحمادي القابضة
536	Translated (0%)	All relevant legislative, statutory, regulatory and contractual requirements shall be identified, documented and kept up to date.	يجب تحديد جميع المتطلبات التشريعية والقانونية والتنظيمية والتعاقدية ذات .الصلة وتوثيقها وتحديثها
537	Translated (0%)	Al Hammadi Holding's information systems must be reviewed immediately following any implementation of a new system or a change to existing one to verify that they are compliant with Cybersecurity Standards.	يجب مراجعة أنظمة معلومات شركة الحمادي القابضة فورًا بعد أي تنفيذ لنظام .جديد أو تغيير في النظام الحالي للتحقق من امتثالها لمعايير الأمن السيبراني
538	Translated (0%)	Whilst such a compliance review shall be performed by appropriately qualified personnel, there shall be adequate segregation of duties between the personnel performing System Administrators', System Operators', and System Auditors' functions within the organization.	في حين يجب إجراء مراجعة الامتثال هذه من قبل موظفين مؤهلين بشكل مناسب، يجب أن يكون هناك فصل كافٍ للواجبات بين الموظفين الذين يؤدون .وظائف مسؤولي النظام ومشغلي النظام ومراجعي النظام داخل المنظمة
539	Translated (0%)	For more details, refer to AHH-CS-ISMS-000 ISMS Internal Audit Policy	سياسة التدقيق الداخلي AHH - CS - ISMS -000 لمزيد من التفاصيل، راجع لنظام إدارة أمن المعلومات
540	Translated (0%)	Compliance and Adherence	الامتثال والالتزام
541	Translated (0%)	Al Hammadi Holding CEO shall ensure compliance with the cybersecurity policies and standards.	يضمن الرئيس التنفيذي لشركة الحمادي القابضة الامتثال لسياسات ومعايير الأمن .السيبراني
542	Translated (0%)	To ensure compliance, the Cybersecurity department will establish regular reporting by the Cybersecurity Manager, conduct periodic	لضمان الامتثال، سينشئ قسم الأمن السيبراني نظامًا لتقديم تقارير منتظمة يُعدّها مدير الأمن السيبراني، ويجري عمليات تدقيق دورية، أو يشكل لجنة للأمن

		audits, or form a Cybersecurity Committee for oversight.	.السيبراني للإشراف
543	Translated (0%)	The CS manager shall ensure adherence to this policy.	.يتعين على مدير الأمن السيبراني ضمان الالتزام بهذه السياسة
544	Translated (0%)	All employees of Al Hammadi Holding must adhere to this policy.	.على جميع موظفي شركة الحمادي القابضة الالتزام بهذه السياسة
545	Translated (0%)	Violations of this policy may result in legal action in any jurisdiction or other measures as deemed appropriate by the Al Hammadi Holding.	قد تؤدي انتهاكات هذه السياسة إلى اتخاذ إجراءات قانونية في أي ولاية قضائية أو .غيرها من التدابير التي تراها شركة الحمادي القابضة مناسبة
546	Translated (100%)	Exceptions	الاستثناءات
547	Translated (0%)	Violation of cybersecurity policies and standards is prohibited unless a prior justified exception is obtained from the Cybersecurity Department or the Cybersecurity Steering Committee.	يُحظر انتهاك سياسات ومعايير الأمن السيبراني ما لم يتم الحصول على استثناء .مبرر مسبق من إدارة الأمن السيبراني أو اللجنة التوجيهية للأمن السيبراني
548	Translated (0%)	In case of a conflict, applicable legislative and regulatory requirements overrule Al Hammadi Holding policies and standards.	في حالة وجود تعارض، فإن المتطلبات التشريعية والتنظيمية المعمول بها تسود .على سياسات ومعايير شركة الحمادي القابضة
549	Translated (100%)	Revision	المراجعة
550	Translated (0%)	This policy is reviewed annually, after major changes in Al Hammadi Holding's organizational chart or infrastructure, and more frequently whenever required, to ensure it remains appropriate and current for Al Hammadi Holding, ISO 27001, and NCA requirements.	تخضع هذه السياسة لمراجعة سنوية، ولإعادة التقييم بعد أي تغييرات جوهرية في الهيكل التنظيمي أو البنية التحتية لشركة الحمادي القابضة، إضافة إلى مراجعات دورية إضافية عند الضرورة، وذلك لضمان توافقها المستمر مع متطلبات شركة الحمادي القابضة، ومعيار آيزو ISO 27001:2022، وإرشادات .الهيئة الوطنية للأمن السيبراني
551	Translated (0%)	Approval Section	قسم الاعتماد
552	Translated (100%)	Prepared by:	:إعداد
553	Translated (0%)	Mr. Mohammed Alamer	السيد/ محمد العامر
554	Translated (0%)	GRC Cybersecurity Specialist	أخصائي حوكمة ومخاطر وامتثال في الأمن السيبراني
555	Translated (100%)	Name	الاسم
556	Translated (100%)	Designation	المسمى الوظيفي
557	Translated (100%)	Signature	التوقيع
558	Translated	Date	التاريخ

	(100%)		
559	Translated (100%)	Reviewed by:	:راجعها
560	Translated (0%)	Mr. Deepak Dasan	السيد/ ديباك داسان
561	Translated (100%)	IT Manager	مدير تكنولوجيا المعلومات
562	Translated (100%)	Name	الاسم
563	Translated (100%)	Designation	المسمى الوظيفي
564	Translated (100%)	Signature	التوقيع
565	Translated (100%)	Date	التاريخ
566	Translated (100%)	Reviewed by:	:راجعها
567	Translated (0%)	Mr. Majid Al Nahdi	السيد/ ماجد النهدي
568	Translated (100%)	HR Manager	مدير الموارد البشرية
569	Translated (100%)	Name	الاسم
570	Translated (100%)	Designation	المسمى الوظيفي
571	Translated (100%)	Signature	التوقيع
572	Translated (100%)	Date	التاريخ
573	Translated (100%)	Reviewed by:	:راجعها
574	Translated (0%)	Ms. Mashael Alotaibi	السيدة/ مشاعل العتيبي
575	Translated (0%)	<3453>Cybersecurity </3453>Manager	<مدير <3453>الأمن السيبراني</3453/>
576	Translated (100%)	Name	الاسم
577	Translated (100%)	Designation	المسمى الوظيفي

578	Translated (100%)	Signature	التوقيع
579	Translated (100%)	Date	التاريخ
580	Translated (100%)	Approved by:	:اعتمدها
581	Translated (0%)	Dr. Abdulaziz Al Hammadi	الحمادي<Bold><Bold></Bold></Bold></Bold> د./ عبد العزيز<Bold><Bold><Bold><Bold></Bold></Bold></Bold></Bold>
582	Translated (100%)	Chief Operating Officer	الرئيس التنفيذي للعمليات
583	Translated (100%)	Name	الاسم
584	Translated (100%)	Designation	المسمى الوظيفي
585	Translated (100%)	Signature	التوقيع
586	Translated (100%)	Date	التاريخ
587	Translated (100%)	Approved by:	:اعتمدها
588	Translated (0%)	Mr. Mohammad AlHammadi	السيد/ محمد الحمادي
589	Translated (100%)	Chief Executive Officer	الرئيس التنفيذي
590	Translated (100%)	Name	الاسم
591	Translated (100%)	Designation	المسمى الوظيفي
592	Translated (100%)	Signature	التوقيع
593	Translated (100%)	Date	التاريخ

Segment ID	Segment status	Source segment	Target segment
1	Translated (0%)	<3/><32><6>Information Security Internal Policy <22/><26/> </6></32>	<3/><32><6><26></22> السياسة الداخلية لأمن المعلومات /> </6></32>
2	Translated (100%)	Page <43><34/> of <42/></43>	<43><34/> صفحة <42/></43> من 43/>
3	Translated (100%)	Al Hammadi Holding	شركة الحمادي القابضة
4	Translated (0%)	Information Security Internal Policy	السياسة الداخلية لأمن المعلومات
5	Translated (100%)	CYBERSECURITY DEPARTMENT	إدارة الأمن السيبراني
6	Translated (100%)	Policy ID	معرّف السياسة
7	Translated (100%)	AHH-CS-ISMS-009	AHH-CS-ISMS-009
8	Translated (100%)	Class	الفئة
9	Translated (100%)	Internal Release	إصدار داخلي
10	Not Translated (0%)		
11	Translated (100%)	V3.1	V3.1
12	Translated (100%)	Published at	نُشرت في
13	Translated (100%)	April 2025	أبريل 2025
14	Translated (100%)	Document Owner	المسؤول عن المستند
15	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
16	Translated (100%)	Disclaimer	تنويه
17	Translated (100%)	The information contained in this document is the property of Hammadi Holding and must not be copied or communicated to a third party or used for any purpose other than that for which it is supplied, without the written consent of Al Hammadi Holding.	المعلومات الواردة في هذا المستند هي ملك لشركة الحمادي القابضة ولا يجوز نسخها أو إبلاغها إلى طرف ثالث أو استخدامها لأي غرض آخر غير الغرض الذي تم توفيرها من أجله، دون موافقة خطية من شركة الحمادي القابضة.

18	Translated (100%)	Contents	جدول المحتويات
19	Translated (100%)	Document Control	ضبط المستندات
20	Translated (100%)	Document Information	معلومات المستند
21	Translated (100%)	Synopsis	الملخص
22	Translated (100%)	Document Title:	:عنوان المستند
23	Translated (100%)	Information Security Internal Policy	السياسة الداخلية لأمن المعلومات
24	Translated (100%)	Document Status:	:حالة المستند
25	Translated (100%)	Approved	معتمد
26	Translated (100%)	Document Effective Date:	:تاريخ سريان المستند
27	Translated (100%)	April 2025	أبريل 2025
28	Translated (100%)	Document Issue Date:	:تاريخ إصدار المستند
29	Translated (100%)	April 2025	أبريل 2025
30	Translated (100%)	Document Next Revision Date:	:تاريخ المراجعة التالية للمستند
31	Translated (100%)	April <227>2026</227>	<أبريل <227>2026<227/>
32	Translated (100%)	Key contacts	جهات التواصل الرئيسية
33	Translated (100%)	Document Owner:	:المسؤول عن المستند
34	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
35	Translated (100%)	Approval Authority	جهة الاعتماد
36	Translated (100%)	Document Created by:	:مُنشئ المستند
37	Translated	Cybersecurity Department	إدارة الأمن السيبراني

	(100%)		
38	Translated (100%)	Document Reviewed by:	:راجع المستند
39	Translated (100%)	Al Hammadi Holding CS Manager	مدير الأمن السيبراني في شركة الحمادي القابضة
40	Translated (100%)	Document Approved by:	:اعتمد المستند
41	Translated (100%)	Al Hammadi Holding COO & CEO	الرئيس التنفيذي للعمليات والرئيس التنفيذي في شركة الحمادي القابضة
42	Translated (100%)	Note:	:ملاحظة
43	Translated (100%)	Any additional approval will be added in the document annex	تُضاف أي اعتمادات إضافية في ملحق المستند
44	Translated (100%)	Classification	التصنيف
45	Translated (100%)	Company Internal – to be shared with 3rd parties after consent of CS Manager	داخلي لاستخدام للشركة – يُسمح بمشاركته مع جهات خارجية بعد موافقة مدير إدارة الأمن السيبراني
46	Translated (100%)	Version / Dates	الإصدار / التواريخ
47	Translated (100%)	Current Version:	:الإصدار الحالي
48	Translated (100%)	V 3.1	V 3.1
49	Translated (100%)	Date Published:	:تاريخ النشر
50	Translated (100%)	April 2025	أبريل 2025
51	Translated (100%)	Date of Next Review:	:تاريخ المراجعة التالية
52	Translated (100%)	April 2026	أبريل 2026
53	Translated (100%)	Prior Version:	:الإصدار السابق
54	Translated (100%)	V 3.0	V 3.0
55	Translated (100%)	Prior Published:	:تاريخ النشر السابق
56	Translated (100%)	December 2023	ديسمبر 2023

57	Translated (100%)	Document Changes	التغييرات على المستند
58	Translated (100%)	Date	التاريخ
59	Translated (100%)	Version	الإصدار
60	Translated (100%)	Document Owner	المسؤول عن المستند
61	Translated (100%)	Change Description	وصف التغيير
62	Translated (100%)	April <383>2025</383>	<أبريل <383>2025<383/>
63	Translated (100%)	3.1	3.1
64	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
65	Translated (100%)	Document reviewed and updated based on NCA ECC-2:2024 and ISO27001:2022 requirements	تمت مراجعة المستند وتحديثه استنادًا إلى متطلبات الهيئة الوطنية للأمن السيبراني (NCA) المعيار ECC-2:2024 ومعيار آيزو ISO 27001:2022.
66	Translated (100%)	Document Circulation	تعميم المستند
67	Translated (100%)	To	إلى
68	Translated (100%)	Method	الطريقة
69	Translated (100%)	IT Staff	موظفو تكنولوجيا المعلومات
70	Translated (100%)	Intranet Portal	بوابة الإنترانت
71	Translated (100%)	All Al Hammadi Staff	جميع موظفي شركة الحمادي
72	Translated (100%)	Intranet Portal	بوابة الإنترانت
73	Translated (100%)	Objectives	الأهداف
74	Translated (0%)	The purpose of this document to set the principles and procedural implementation guidelines, which by Al Hammadi Holding shall select and deploy the suitable and applicable information security policies and controls, to provide management direction and support for information security in	الغرض من هذا المستند هو وضع المبادئ وإرشادات التنفيذ الإجرائية، والتي يجب على شركة الحمادي القابضة اختيار ونشر ،سياسات وضوابط أمن المعلومات المناسبة والقابلة للتطبيق لتوفير التوجيه الإداري والدعم لأمن المعلومات وفقًا لمتطلبات

		accordance with business requirements and relevant laws and regulations, and in compliance with the requirements specified in	العمل والقوانين واللوائح ذات الصلة، وبما يتوافق مع المتطلبات المحددة في
75	Translated (0%)	ISO/IEC 27001 Annex-A:A.5.1 Policies for Information Security, A.5.2 Information security roles and responsibilities, A.5.3 Segregation of duties, A.5.4 Management responsibilities, A.5.5 Contact with authorities, A.5.6 Contact with special interest groups, A.5.8 Information security in project management	الملحق أ: أ .5.1 سياسات أمن المعلومات، أ .5.2 ISO/IEC 27001 أدوار ومسؤوليات أمن المعلومات، أ .5.3 الفصل بين الواجبات، أ مسؤوليات الإدارة، أ .5.5 الاتصال بالسلطات، أ .5.6 الاتصال 5.4. بمجموعات المصالح الخاصة، أ .5.8 أمن المعلومات في إدارة المشاريع
76	Translated (100%)	NCA ECC-2:2024:	ECC-2:2024: معيار الهيئة الوطنية للأمن السيبراني رقم
77	Translated (0%)	1-3 Cybersecurity Policies and Procedures, 1-6 Cybersecurity in Information and Technology Project Management	سياسات وإجراءات الأمن السيبراني، 1-6 الأمن السيبراني في 1-3 إدارة مشاريع المعلومات والتكنولوجيا
78	Translated (100%)	Scope	النطاق
79	Translated (0%)	This document is applicable to all Al Hammadi Holding ISMS information assets, security operations, healthcare systems, and all persons doing work under Al Hammadi Holding control.	تنطبق هذا المستند على جميع أصول معلومات نظام إدارة أمن المعلومات في شركة الحمادي القابضة والعمليات الأمنية وأنظمة الرعاية الصحية وجميع الأشخاص الذين يعملون تحت سيطرة شركة الحمادي القابضة.
80	Translated (100%)	This includes employees, contractors, suppliers, and 3rd Parties.	وتشمل السياسة الموظفين والمتعاقدين والموردين والجهات الخارجية.
81	Translated (100%)	Roles and Responsibilities	الأدوار والمسؤوليات
82	Translated (0%)	Al Hammadi Holding Management and Cybersecurity Department are responsible for implementing, maintaining, and updating this policy with all its contents, in accordance with any changes in the applicable legislative, regulatory requirements or related standards.	تتولى إدارة الحمادي القابضة والأمن السيبراني مسؤولية تنفيذ هذه السياسة وصيانتها وتحديثها بجميع محتوياتها، وفقًا لأي تغييرات في المتطلبات التشريعية أو التنظيمية المعمول بها أو المعايير ذات الصلة.
83	Translated (100%)	Principles	المبادئ
84	Translated (0%)	Policies for Information Security	سياسات أمن المعلومات
85	Translated (0%)	Al Hammadi Holding Cybersecurity management shall define a set of information security policies and procedures which shall be approved by Cybersecurity Steering Committee, published and communicated to employees and relevant external parties.	يجب على إدارة الأمن السيبراني في شركة الحمادي القابضة تحديد مجموعة من سياسات وإجراءات أمن المعلومات التي يجب أن توافق عليها اللجنة التوجيهية للأمن السيبراني ونشرها وإبلاغها للموظفين والأطراف الخارجية ذات الصلة.
86	Translated (0%)	Policies should be communicated to all employees and relevant external parties in a form that is relevant, accessible and understandable, e.g., in the context of an information security awareness, education and training program.	يجب إبلاغ السياسات إلى جميع الموظفين والأطراف الخارجية ذات الصلة في شكل ذي صلة ويمكن الوصول إليه وفهمه، على سبيل المثال، في سياق برنامج التوعية بأمن المعلومات والتعليم والتدريب.
87	Translated (0%)	Information security policies should address requirements created by:	يجب أن تتناول سياسات أمن المعلومات المتطلبات التي أنشأها:

88	Translated (0%)	business strategy.	.استراتيجية العمل
89	Translated (0%)	Risk assessment.	.تقييم المخاطر
90	Translated (0%)	Applicable Saudi law, regulations, legislation and contracts.	.القوانين واللوائح والتشريعات والعقود السعودية المعمول بها
91	Translated (0%)	current and projected information security threat environment including threat intelligence platforms .	بيئة تهديد أمن المعلومات الحالية والمتوقعة بما في ذلك منصات .استخبارات التهديدات
92	Translated (0%)	The information security policy should contain statements concerning:	:يجب أن تحتوي سياسة أمن المعلومات على بيانات تتعلق بما يلي
93	Translated (0%)	definition of information security, objectives and principles.	.تعريف أمن المعلومات والأهداف والمبادئ
94	Translated (0%)	assignment of general and specific roles and responsibilities.	.تعيين الأدوار والمسؤوليات العامة والمحددة
95	Translated (0%)	Information security policy should be supported by topic-specific policies, e.g.:	يجب أن تكون سياسة أمن المعلومات مدعومة بسياسات خاصة :بالموضوع، على سبيل المثال
96	Translated (0%)	access control.	.التحكم في الوصول
97	Translated (0%)	information classification.	.تصنيف المعلومات
98	Translated (0%)	physical and environmental security.	.الأمن المادي والبيئي
99	Translated (0%)	The cybersecurity policies and procedures must be supported by technical security standards (e.g., operating systems, databases and firewall technical security standards)	يجب أن تكون سياسات وإجراءات الأمن السيبراني مدعومة بمعايير الأمن التقني (على سبيل المثال، أنظمة التشغيل وقواعد (البيانات ومعايير الأمن التقني لجدار الحماية
100	Translated (0%)	Each policy should have an owner who has approved management responsibility for the development, review and evaluation of the policies.	يجب أن يكون لكل سياسة مسؤول وافق على مسؤولية الإدارة عن .تطوير السياسات ومراجعتها وتقييمها
101	Translated (0%)	The review should include assessing opportunities for improvement of the organization’s policies and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions or technical environment.	يجب أن تتضمن المراجعة تقييم فرص تحسين سياسات المنظمة ونهجها لإدارة أمن المعلومات استجابة للتغيرات في البيئة .التنظيمية أو ظروف العمل أو الظروف القانونية أو البيئة التقنية
102	Translated (0%)	The review of policies for information security should take the results of management reviews into account.	يجب أن تأخذ مراجعة سياسات أمن المعلومات في الاعتبار نتائج .مراجعات الإدارة
103	Translated (0%)	Management approval for a revised policy should be obtained.	.يجب الحصول على موافقة الإدارة على سياسة منقحة
104	Translated (0%)	Cybersecurity Manager shall ensure the implementation of the information security policies and procedures and the adherence to these policies by, at least, performing periodical audit, review, vulnerability assessment, penetration test…etc.	يجب على مدير الأمن السيبراني ضمان تنفيذ سياسات وإجراءات أمن المعلومات والالتزام بهذه السياسات، على الأقل، من خلال إجراء تدقيق دوري ومراجعة وتقييم الثغرات الأمنية واختبار .الاختراق...إلخ

105	Translated (0%)	Review of the Policies for Information Security	مراجعة سياسات أمن المعلومات
106	Translated (0%)	Information security policies shall be reviewed at least annually or when significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	يجب مراجعة سياسات أمن المعلومات سنويًا على الأقل أو عند حدوث تغييرات كبيرة لضمان استمرار ملاءمتها وكفايتها وفعاليتها.
107	Translated (0%)	Segregation of duties	الفصل بين الواجبات
108	Translated (0%)	Al Hammadi Holding shall segregate conflicting duties and areas of responsibility to minimize risks and/or opportunities for undesired modification or misuse of its critical assets.	تقوم شركة الحمادي القابضة بفصل الواجبات ومجالات المسؤولية المتضاربة لتقليل المخاطر و/أو فرص التعديل أو سوء الاستخدام غير المرغوب فيه لأصولها الحيوية.
109	Translated (0%)	All persons who shall access, modify or use Al Hammadi Holding assets shall be authorized.	يجب تفويض جميع الأشخاص الذين يجب عليهم الوصول إلى أصول شركة الحمادي القابضة أو تعديلها أو استخدامها.
110	Translated (0%)	Al Hammadi Holding management shall ensure that initiation of an event will be separated from its authorization.	يجب على إدارة شركة الحمادي القابضة التأكد من فصل بدء الحدث عن تفويضها.
111	Translated (0%)	Al Hammadi Holding management shall consider the possibility of collusion while designing the necessary controls.	يجب على إدارة شركة الحمادي القابضة النظر في إمكانية التواطؤ أثناء تصميم الضوابط اللازمة.
112	Translated (0%)	Contact with authorities	الاتصال بالسلطات
113	Translated (0%)	Al Hammadi Holding management shall define appropriate persons for contacting with relevant authorities.	يجب على إدارة شركة الحمادي القابضة تحديد الأشخاص المناسبين للاتصال بالسلطات ذات الصلة.
114	Translated (0%)	(e.g., law enforcement, regulatory bodies, supervisory authorities)	على سبيل المثال، إنفاذ القانون والهيئات التنظيمية والسلطات الإشرافية)
115	Translated (0%)	Al Hammadi Holding management shall specify when and how authorities will be contacted.	يجب على إدارة شركة الحمادي القابضة تحديد متى وكيف سيتم الاتصال بالسلطات.
116	Translated (0%)	Al Hammadi Holding management shall define which internal, external, or international authorities shall be reported to in a timely manner with major information security incidents.	يجب على إدارة شركة الحمادي القابضة تحديد السلطات الداخلية أو الخارجية أو الدولية التي يجب الإبلاغ عنها في الوقت المناسب مع حوادث أمن المعلومات الرئيسية.
117	Translated (0%)	Contact with special interest groups	الاتصال بمجموعات الاهتمامات الخاصة
118	Translated (0%)	Al Hammadi Holding management shall define appropriate persons for contacting with relevant security forums and professional associations.	يجب على إدارة شركة الحمادي القابضة تحديد الأشخاص المناسبين للاتصال بالمنتديات الأمنية والجمعيات المهنية ذات الصلة.
119	Translated (0%)	<782><780>Appointed persons shall receive early warnings of alerts, advisories, and patches pertaining to attacks and vulnerabilities</780></782><783/><786>.</786>	يجب أن يتلقى الأشخاص المعينون تحذيرات مبكرة<782><780> من التنبيهات والتحذيرات والتصحيحات المتعلقة بالهجمات ونقاط الضعف</780/><782/><783></783><786>.</786/>
120	Translated (0%)	Information security in project management	أمن المعلومات في إدارة المشاريع
121	Translated (0%)	All IT projects must incorporate cybersecurity planning, risk management, and compliance measures throughout the project lifecycle—from initiation and	يجب أن تتضمن جميع مشاريع تكنولوجيا المعلومات تخطيط الأمن السيبراني وإدارة المخاطر وتدابير الامتثال طوال دورة حياة

		planning to execution, monitoring, and closure.	.المشروع - من البدء والتخطيط إلى التنفيذ والمراقبة والإغلاق
122	Translated (0%)	Al Hammadi Holding management shall address information security in project management, regardless of the type of the project.	يجب على إدارة شركة الحمادي القابضة معالجة أمن المعلومات .في إدارة المشروع، بغض النظر عن نوع المشروع
123	Translated (0%)	Information security objectives shall be included in projects' objectives.	.يجب تضمين أهداف أمن المعلومات في أهداف المشاريع
124	Translated (0%)	Information security risk assessments shall be conducted at early stages of Al Hammadi Holding projects to identify necessary controls.	يجب إجراء تقييمات مخاطر أمن المعلومات في المراحل المبكرة .من مشاريع شركة الحمادي القابضة لتحديد الضوابط اللازمة
125	Translated (0%)	Information security shall be integrated with Al Hammadi Holding applied project methodology.	يجب دمج أمن المعلومات مع منهجية المشروع التطبيقي لشركة .الحمادي القابضة
126	Translated (0%)	Cybersecurity Requirements in Project Lifecycle	متطلبات الأمن السيبراني في دورة حياة المشروع
127	Translated (0%)	Initiation Phase	مرحلة البدء
128	Translated (0%)	Al Hammadi Holding CS team shall conduct a preliminary cybersecurity impact assessment.	يجب على فريق الأمن السيبراني في شركة الحمادي القابضة إجراء .تقييم أولي لأثر الأمن السيبراني
129	Translated (0%)	Al Hammadi Holding shall identify sensitive data or critical systems involved.	يجب على شركة الحمادي القابضة تحديد البيانات الحساسة أو .الأنظمة الحيوية المعنية
130	Translated (0%)	Al Hammadi Holding shall assign cybersecurity roles within the project team.	تقوم شركة الحمادي القابضة بتعيين أدوار الأمن السيبراني داخل .فريق المشروع
131	Translated (100%)	Planning Phase	مرحلة التخطيط
132	Translated (0%)	Al Hammadi Holding CS team shall develop a cybersecurity plan aligned with organizational policies and standards (e.g., NCA ECC, ISO/IEC 27001).	يجب على فريق الأمن السيبراني في شركة الحمادي القابضة وضع خطة للأمن السيبراني تتماشى مع السياسات والمعايير التنظيمية .(على سبيل المثال، NCA ECC، ISO/IEC 27001)
133	Translated (0%)	Al Hammadi Holding CS team shall conduct a detailed threat and risk assessment.	يجب على فريق الأمن السيبراني في شركة الحمادي القابضة إجراء .تقييم مفصل للتهديد والمخاطر
134	Translated (0%)	Al Hammadi Holding CS team shall define security controls and mitigation strategies.	يجب على فريق الأمن السيبراني في شركة الحمادي القابضة .تحديد الضوابط الأمنية واستراتيجيات التخفيف
135	Translated (0%)	Al Hammadi Holding shall include cybersecurity milestones in the project schedule.	يجب أن تدرج شركة الحمادي القابضة مراحل الأمن السيبراني في .الجدول الزمني للمشروع
136	Translated (0%)	Execution Phase	مرحلة التنفيذ
137	Translated (0%)	Al Hammadi Holding shall ensure secure configurations and system hardening.	يجب أن تضمن شركة الحمادي القابضة تكوينات آمنة وتصلب .النظام
138	Translated (0%)	Al Hammadi Holding shall enforce access control measures (least privilege principle).	يجب على شركة الحمادي القابضة فرض تدابير التحكم في .الوصول (مبدأ الامتياز الأقل)
139	Translated (0%)	Al Hammadi Holding shall perform code reviews and vulnerability scanning.	يجب على شركة الحمادي القابضة إجراء مراجعات التعليمات .البرمجية ومسح الثغرات الأمنية
140	Translated	Al Hammadi Holding shall implement encryption for data at rest and in transit.	تقوم شركة الحمادي القابضة بتنفيذ تشفير البيانات أثناء الراحة

	(0%)		والنقل.
141	Translated (0%)	Al Hammadi Holding shall ensure preforming a PT testing before go-live for any published product.	قبل بدء PT يجب أن تضمن شركة الحمادي القابضة إجراء اختبار التشغيل لأي منتج منشور.
142	Translated (0%)	Monitoring and Controlling Phase	مرحلة المراقبة والتحكم
143	Translated (0%)	Al Hammadi Holding shall track cybersecurity metrics and incidents.	يجب على شركة الحمادي القابضة تتبع مقاييس الأمن السيبراني والحوادث.
144	Translated (0%)	Al Hammadi Holding shall conduct periodic security testing (e.g., penetration testing).	يجب على شركة الحمادي القابضة إجراء اختبار أمني دوري (على سبيل المثال، اختبار الاختراق).
145	Translated (0%)	Al Hammadi Holding shall update the risk register with new or emerging threats.	يجب على شركة الحمادي القابضة تحديث سجل المخاطر بالتهديدات الجديدة أو الناشئة.
146	Translated (0%)	Al Hammadi Holding shall review third-party security compliance if applicable.	تقوم شركة الحمادي القابضة بمراجعة الامتثال الأمني من طرف ثالث إذا كان ذلك ممكنًا.
147	Translated (100%)	Compliance and Adherence	الامتثال والالتزام
148	Translated (100%)	Al Hammadi Holding CEO shall ensure compliance with the cybersecurity policies and standards.	يضمن الرئيس التنفيذي لشركة الحمادي القابضة الامتثال لسياسات ومعايير الأمن السيبراني.
149	Translated (100%)	To ensure compliance, the Cybersecurity department will establish regular reporting by the Cybersecurity Manager, conduct periodic audits, or form a Cybersecurity Steering Committee for oversight.	لضمان الامتثال، سينشئ قسم الأمن السيبراني نظامًا لتقديم تقارير منتظمة يُعدّها مدير الأمن السيبراني، ويجري عمليات تدقيق دورية، أو يشكل لجنة توجيهية للأمن السيبراني للإشراف.
150	Translated (100%)	The CS Manager shall ensure adherence to this policy.	يتعين على مدير الأمن السيبراني ضمان الالتزام بهذه السياسة.
151	Translated (100%)	All employees of Al Hammadi Holding must adhere to this policy.	على جميع موظفي شركة الحمادي القابضة الالتزام بهذه السياسة.
152	Translated (0%)	Violations of this policy may result in legal action in any jurisdiction or other measures deemed appropriate by the Al Hammadi Holding.	قد تؤدي انتهاكات هذه السياسة إلى اتخاذ إجراءات قانونية في أي ولاية قضائية أو غيرها من التدابير التي تراها شركة الحمادي القابضة مناسبة.
153	Translated (100%)	Exceptions	الاستثناءات
154	Translated (100%)	Violation of cybersecurity policies and standards is prohibited unless a prior justified exception is obtained from the Cybersecurity Department or the Cybersecurity Steering Committee.	يُحظر انتهاك سياسات ومعايير الأمن السيبراني ما لم يتم الحصول على استثناء مبرر مسبق من إدارة الأمن السيبراني أو اللجنة التوجيهية للأمن السيبراني.
155	Translated (100%)	In case of a conflict, applicable legislative and regulatory requirements overrule Al Hammadi Holding policies and standards.	في حالة وجود تعارض، فإن المتطلبات التشريعية والتنظيمية المعمول بها تسود على سياسات ومعايير شركة الحمادي القابضة.
156	Translated (100%)	Revision	المراجعة
157	Translated (100%)	This policy is reviewed annually, or after major changes in Al Hammadi Holding’s organizational chart or infrastructure, and more frequently whenever required, to ensure it remains appropriate and current for Al	تخضع هذه السياسة لمراجعة سنوية، أو لإعادة التقييم بعد أي تغييرات جوهرية في الهيكل التنظيمي أو البنية التحتية لشركة الحمادي القابضة، إضافة إلى مراجعات دورية إضافية عند

		Hammadi Holding, ISO 27001, and NCA requirements.	الضرورة، وذلك لضمان توافقها المستمر مع متطلبات شركة وإرشادات ISO 27001:2022، الحمادي القابضة، ومعيار آيزو .الهيئة الوطنية للأمن السيبراني
158	Translated (100%)	Approval Section	قسم الاعتماد
159	Translated (100%)	Prepared by:	:إعداد
160	Translated (100%)	Mr. Mohammed Alamer	السيد/ محمد العامر
161	Translated (100%)	GRC Cybersecurity Specialist	أخصائي حوكمة ومخاطر وامتثال في الأمن السيبراني
162	Translated (100%)	Name	الاسم
163	Translated (100%)	Designation	المسمى الوظيفي
164	Translated (100%)	Signature	التوقيع
165	Translated (100%)	Date	التاريخ
166	Translated (100%)	Reviewed by:	:راجعها
167	Translated (100%)	Mr. Deepak Dasan	السيد/ ديباك داسان
168	Translated (100%)	IT Manager	مدير تكنولوجيا المعلومات
169	Translated (100%)	Name	الاسم
170	Translated (100%)	Designation	المسمى الوظيفي
171	Translated (100%)	Signature	التوقيع
172	Translated (100%)	Date	التاريخ
173	Translated (100%)	Reviewed by:	:راجعها
174	Translated (100%)	Ms. Mashael Alotaibi	السيدة/ مشاعل العتيبي
175	Translated (100%)	<1149>Cybersecurity </1149>Manager	<مدير <1149>الأمن السيبراني</1149/>

176	Translated (100%)	Name	الاسم
177	Translated (100%)	Designation	المسمى الوظيفي
178	Translated (100%)	Signature	التوقيع
179	Translated (100%)	Date	التاريخ
180	Translated (100%)	Approved by:	:اعتمدها
181	Translated (100%)	Dr. Abdulaziz Al Hammadi	الحمادي<Bold><Bold></Bold></Bold> د./ عبد العزيز<Bold><Bold></Bold></Bold>
182	Translated (100%)	Chief Operating Officer	الرئيس التنفيذي للعمليات
183	Translated (100%)	Name	الاسم
184	Translated (100%)	Designation	المسمى الوظيفي
185	Translated (100%)	Signature	التوقيع
186	Translated (100%)	Date	التاريخ
187	Translated (100%)	Approved by:	:اعتمدها
188	Translated (100%)	Mr. Mohammad Al Hammadi	السيد/ محمد الحمادي
189	Translated (100%)	Chief Executive Officer	الرئيس التنفيذي
190	Translated (100%)	Name	الاسم
191	Translated (100%)	Designation	المسمى الوظيفي
192	Translated (100%)	Signature	التوقيع
193	Translated (100%)	Date	التاريخ

Segment ID	Segment status	Source segment	Target segment
1	Translated (100%)	Sample Copy	نسخة نموذجية
2	Translated (0%)	<7/><32><14><10> </10><13>Information Security Network & Communication Management Policy <21/><25/></13><28> </28></14></32>	سياسة أمن المعلومات وإدارة الشبكات<7/><32><14><10> </10><13>والاتصالات <21></25><13/><28/><14/><32>
3	Translated (100%)	Sample Copy	نسخة نموذجية
4	Translated (100%)	Page <47><38/> of <46/></47>	صفحة <47><38/></47> من <46/></47>
5	Translated (100%)	Al Hammadi Holding	شركة الحمادي القابضة
6	Translated (0%)	Information Security Network &	شبكة أمن المعلومات و
7	Translated (0%)	Communication Management Policy	سياسة إدارة الاتصالات
8	Translated (100%)	CYBERSECURITY DEPARTMENT	إدارة الأمن السيبراني
9	Translated (100%)	Policy ID	معرّف السياسة
10	Translated (100%)	AHH-CS-ISMS-010	AHH-CS-ISMS-010
11	Translated (100%)	Class	الفئة
12	Translated (100%)	Internal Release	إصدار داخلي
13	Not Translated (0%)		
14	Translated (100%)	V3.1	V3.1
15	Translated (100%)	Published at	نُشرت في
16	Translated (100%)	April 2025	أبريل 2025
17	Translated (100%)	Document Owner	المسؤول عن المستند
18	Translated	Cybersecurity Department	إدارة الأمن السيبراني

	(100%)		
19	Translated (100%)	Disclaimer	تنويه
20	Translated (99%)	The information contained in this document is the property of Al Hammadi Holding and must not be copied or communicated to a third party or used for any purpose other than that for which it is supplied, without the written consent of Al Hammadi Holding.	المعلومات الواردة في هذا المستند هي ملك لشركة الحمادي القابضة ولا يجوز نسخها أو إبلاغها إلى طرف ثالث أو استخدامها لأي غرض آخر غير الغرض الذي تم توفيرها من أجله، دون موافقة خطية من شركة الحمادي القابضة.
21	Translated (100%)	Contents	جدول المحتويات
22	Translated (100%)	Document Control	ضبط المستندات
23	Translated (100%)	Document Information	معلومات المستند
24	Translated (100%)	Synopsis	الملخص
25	Translated (100%)	Document Title:	:عنوان المستند
26	Translated (0%)	Information Security Network and Communication Management Policy	سياسة إدارة شبكة أمن المعلومات والاتصالات
27	Translated (100%)	Document Status:	:حالة المستند
28	Translated (100%)	Approved	معتمد
29	Translated (100%)	Document Effective Date:	:تاريخ سريان المستند
30	Translated (100%)	April 2025	أبريل 2025
31	Translated (0%)	<321>Document Issue Date</321>:	:<تاريخ إصدار المستند<321>321/>
32	Translated (100%)	April 2025	أبريل 2025
33	Translated (0%)	<336>Document Next Revision Date</336>:	:<تاريخ المراجعة التالية للوثيقة<336>336/>
34	Translated (100%)	April 2026	أبريل 2026
35	Translated (100%)	Key contacts	جهات التواصل الرئيسية
36	Translated (100%)	Document Owner:	:المسؤول عن المستند

37	Translated (100%)	Cybersecurity Management	إدارة الأمن السيبراني
38	Translated (100%)	Approval Authority	جهة الاعتماد
39	Translated (100%)	Document Created by:	مُنشئ المستند:
40	Translated (100%)	IT Management	إدارة تكنولوجيا المعلومات
41	Translated (100%)	Document Reviewed by:	راجع المستند:
42	Translated (100%)	Al Hammadi Holding CS&IT Managers	مديرو الأمن السيبراني وتكنولوجيا المعلومات في شركة الحمادي القابضة
43	Translated (100%)	Document Approved by:	اعتمد المستند:
44	Translated (100%)	Al Hammadi Holding COO & CEO	الرئيس التنفيذي للعمليات والرئيس التنفيذي في شركة الحمادي القابضة
45	Translated (100%)	Note:	ملاحظة:
46	Translated (100%)	Any additional approval will be added in the document annex	تُضاف أي اعتمادات إضافية في ملحق المستند
47	Translated (100%)	Classification	التصنيف
48	Translated (100%)	Company Internal – to be shared with 3rd parties after consent of CS Manager	داخلي لاستخدام للشركة – يُسمح بمشاركته مع جهات خارجية بعد موافقة مدير إدارة الأمن السيبراني
49	Translated (100%)	Version / Dates	الإصدار / التواريخ
50	Translated (100%)	Current Version:	الإصدار الحالي:
51	Translated (100%)	V 3.1	V 3.1
52	Translated (100%)	Date Published:	تاريخ النشر:
53	Translated (100%)	April 2025	أبريل 2025
54	Translated (100%)	Date of Next Review:	تاريخ المراجعة التالية:
55	Translated (100%)	April 2026	أبريل 2026
56	Translated	Prior Version:	الإصدار السابق:

	(100%)		
57	Translated (100%)	V 3.0	V 3.0
58	Translated (100%)	Prior Published:	تاريخ النشر السابق:
59	Translated (100%)	December 2023	ديسمبر 2023
60	Translated (100%)	Document Changes	التغييرات على المستند
61	Translated (100%)	Date	التاريخ
62	Translated (100%)	Version	الإصدار
63	Translated (100%)	Document Owner	المسؤول عن المستند
64	Translated (100%)	Change Description	وصف التغيير
65	Translated (100%)	December 2024	ديسمبر 2024
66	Translated (100%)	3.0	3.0
67	Translated (100%)	IT Management	إدارة تكنولوجيا المعلومات
68	Translated (100%)	Updated policy number to	تحديث رقم السياسة إلى
69	Translated (100%)	AHH-IT-ISMS-010	AHH-IT-ISMS-010
70	Translated (100%)	April 2025	أبريل 2025
71	Translated (100%)	3.1	3.1
72	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
73	Translated (100%)	Document reviewed and updated based on NCA ECC-2:2024 and ISO27001:2022 requirements	تمت مراجعة المستند وتحديثه استنادًا إلى متطلبات الهيئة الوطنية للأمن السيبراني (NCA) المعيار ECC-2:2024 ومعيار آيزو ISO 27001:2022.
74	Translated (100%)	Document Circulation	تعميم المستند
75	Translated (100%)	To	إلى

76	Translated (100%)	Date	التاريخ
77	Translated (100%)	Method	الطريقة
78	Translated (100%)	IT Staff	موظفو تكنولوجيا المعلومات
79	Translated (100%)	April 2025	أبريل 2025
80	Translated (100%)	Intranet Portal	بوابة الإنترانت
81	Translated (100%)	Objectives	الأهداف
82	Translated (0%)	The purpose of this policy is to set the principles and procedural implementation guidelines, by which Al Hammadi Holding shall manage and control its critical communication and network assets to ensure its protection and continuous availability against possible threats, unauthorized use, and unplanned outages, in compliance with the requirements specified in:	الغرض من هذه السياسة هو وضع المبادئ وإرشادات التنفيذ الإجرائية، والتي بموجبها تقوم شركة الحمادي القابضة بإدارة ومراقبة اتصالاتها الحرجة وأصول شبكتها لضمان حمايتها وتوافرها المستمر ضد التهديدات المحتملة والاستخدام غير المصرح به والانقطاعات غير المخطط لها، وفقًا للمتطلبات المحددة في:
83	Translated (100%)	ISO/IEC 27001 Annex-A:	الملحق أ ISO 27001:2022/معيار آيزو:
84	Translated (0%)	A.8.20 Networks security, A.8.21 Security of network services, A.8.22 Segregation of networks, A.8.23 Web filtering, A.5.14 Information transfer, A.6.6 Confidentiality or non-disclosure agreements.	أ .8.20 أمن الشبكات، أ .8.21 أمن خدمات الشبكة، أ .8.22 فصل الشبكات، أ تصفية الويب، أ .5.14 نقل المعلومات، أ .6.6 اتفاقيات السرية أو عدم الإفصاح.
85	Translated (100%)	NCA ECC-2:2024:	ECC-2:2024: معيار الهيئة الوطنية للأمن السيبراني رقم
86	Translated (0%)	2-5 Network Security Management.	2-5 إدارة أمن الشبكات.
87	Translated (100%)	Scope	النطاق
88	Translated (95%)	This policy is applicable to all Al Hammadi Holding ISMS information assets, security operations, Healthcare systems, and all persons doing work under Al Hammadi Holding control.	تنطبق هذه السياسة على جميع أصول معلومات نظام إدارة أمن المعلومات في شركة الحمادي القابضة والعمليات الأمنية والأنظمة الصحية وجميع الأشخاص الذين يعملون تحت إشراف شركة الحمادي القابضة.
89	Translated (100%)	This includes employees and contractors, suppliers, and 3rd Parties.	تشمل السياسة الموظفين والمتعاقدين والموردين والجهات الخارجية.
90	Translated (100%)	Roles and Responsibilities	الأدوار والمسؤوليات
91	Translated (100%)	Al Hammadi Holding Cybersecurity and IT Departments are responsible for maintaining this policy with all its contents, in accordance with any changes in the applicable regulations and	تتولى إدارات الأمن السيبراني وتكنولوجيا المعلومات في شركة الحمادي القابضة مسؤولية حفظ هذه السياسة بجميع محتوياتها، وفقًا لأي تغييرات تطرأ على اللوائح والتشريعات المعمول بها، وذلك وفقًا لما يلي:

		legislation, where:	
92	Translated (0%)	<701>701/>>Policy Review and Update:	:<701/> مراجعة السياسة وتحديثها<701>
93	Translated (100%)	Cybersecurity Manager	مدير الأمن السيبراني
94	Translated (0%)	<707>707/>>Policy Implementation and Execution:	:<707/> تنفيذ السياسة وتنفيذها<707>
95	Translated (100%)	IT Manager	مدير تكنولوجيا المعلومات
96	Translated (100%)	Policy Compliance Measurement:	:قياس الامتثال للسياسة
97	Translated (100%)	Cybersecurity Manager	مدير الأمن السيبراني
98	Translated (100%)	Principles	المبادئ
99	Translated (0%)	Network controls	عناصر تحكم الشبكة
100	Translated (0%)	Al Hammadi Holding shall ensure the protection of information in networks and its IT facilities.	تضمن شركة الحمادي القابضة حماية المعلومات في الشبكات ومرافق تكنولوجيا المعلومات التابعة لها.
101	Translated (0%)	Al Hammadi Holding Cybersecurity Department shall identify and document all network devices within Al Hammadi Holding and ensure that all devices are up to date and approved.	يجب على إدارة الأمن السيبراني في شركة الحمادي القابضة تحديد وتوثيق جميع أجهزة الشبكة داخل شركة الحمادي القابضة والتأكد من أن جميع الأجهزة محدثة ومعتمدة.
102	Translated (0%)	Al Hammadi Holding Cybersecurity department shall document technical security standards for all network devices used within Al Hammadi Holding.	يجب على إدارة الأمن السيبراني في شركة الحمادي القابضة توثيق معايير الأمن الفني لجميع أجهزة الشبكة المستخدمة داخل شركة الحمادي القابضة.
103	Translated (0%)	Al Hammadi Holding Networks shall be managed and controlled to protect information in systems and applications from unauthorized access.	يجب إدارة ومراقبة شبكات الحمادي القابضة لحماية المعلومات في الأنظمة والتطبيقات من الوصول غير المصرح به.
104	Translated (0%)	Al Hammadi Holding responsibilities for the management of networking equipment shall be established.	يتم تحديد مسؤوليات شركة الحمادي القابضة لإدارة معدات الشبكات.
105	Translated (0%)	Operational responsibility for networks shall be separated from computer operations where appropriate.	يجب فصل المسؤولية التشغيلية للشبكات عن عمليات الكمبيوتر عند الاقتضاء.
106	Translated (0%)	Special controls shall be established to safeguard the confidentiality and integrity of data passing over public or wireless networks.	يجب وضع ضوابط خاصة لحماية سرية وسلامة البيانات التي تمر عبر الشبكات العامة أو اللاسلكية.
107	Translated (0%)	Special controls shall also be required to maintain the availability of the network services and connected computers.	كما يلزم وجود ضوابط خاصة للحفاظ على توافر خدمات الشبكة وأجهزة الكمبيوتر المتصلة.
108	Translated (0%)	Logging and monitoring shall be applied to enable recording and detection of actions that may affect information security.	يجب تطبيق التسجيل والمراقبة لتمكين تسجيل واكتشاف الإجراءات التي قد تؤثر على أمن المعلومات.
109	Translated	Systems on the network shall be authenticated.	يجب المصادقة على الأنظمة الموجودة على الشبكة.

	(0%)		
110	Translated (0%)	Security of network services	أمن خدمات الشبكة
111	Translated (0%)	Service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	يجب تحديد مستويات الخدمة ومتطلبات الإدارة لجميع خدمات الشبكة وإدراجها في اتفاقيات خدمات الشبكة، سواء كانت هذه الخدمات مقدمة داخليًا أو الاستعانة بمصادر خارجية.
112	Translated (0%)	The ability of the network service provider to manage agreed services in a secure way shall be determined and regularly monitored, and the right to audit shall be agreed.	يتم تحديد قدرة مزود خدمة الشبكة على إدارة الخدمات المتفق عليها بطريقة آمنة ومراقبتها بانتظام، ويتم الاتفاق على الحق في التدقيق.
113	Translated (0%)	Security for network services shall include the provision of connections, private network services and value-added networks and managed network security solutions such as firewalls and intrusion detection systems.	يجب أن يشمل أمن خدمات الشبكة توفير الاتصالات وخدمات الشبكات الخاصة والشبكات ذات القيمة المضافة وحلول أمن الشبكات المدارة مثل جدران الحماية وأنظمة الكشف عن التسلل.
114	Translated (0%)	Manage access permissions to Al Hammadi Holding networks in accordance with the identity and access management policy to be granted only to authorized users, and the connection must be available.	إدارة أذونات الوصول إلى شبكات الحمادي القابضة وفقًا لسياسة إدارة الهوية والوصول التي يتم منحها فقط للمستخدمين المصرح لهم، ويجب أن يكون الاتصال متاحًا.
115	Translated (0%)	Networks shall be isolated and segmented physically and logically using the firewall and Defense-in-Depth.	يجب عزل الشبكات وتقسيمها ماديًا ومنطقيًا باستخدام جدار الحماية والدفاع المتعمق.
116	Translated (0%)	Apply the VLAN logical isolation.	تطبيق العزل المنطقي للشبكة المحلية الافتراضية.
117	Translated (0%)	Logical isolation shall be applied between the production environment network and the test environment network and other networks.	يجب تطبيق العزل المنطقي بين شبكة بيئة الإنتاج وشبكة بيئة الاختبار والشبكات الأخرى.
118	Translated (0%)	Prevent the connection of critical systems to the Internet if these systems provide an internal service for Al Hammadi Holding and there is no business demand to be accessible outside Al Hammadi Holding.	منع اتصال الأنظمة الحيوية بالإنترنت إذا كانت هذه الأنظمة توفر خدمة داخلية لشركة الحمادي القابضة ولا يوجد طلب تجاري يمكن الوصول إليه خارج شركة الحمادي القابضة.
119	Translated (0%)	Logical isolation shall be applied between the Voice Over IP “VOIP” network and the data network.	يجب تطبيق العزل المنطقي بين شبكة الصوت عبر بروتوكول الإنترنت "VOIP" وشبكة البيانات.
120	Translated (0%)	Restricting the use of logical network ports in all Al Hammadi Holding facilities by using Port Security or Port-Based Authentication to prevent unauthorized access to the detection of suspicious devices.	تقييد استخدام منافذ الشبكة المنطقية في جميع مرافق شركة الحمادي القابضة باستخدام أمن الموانئ أو المصادقة القائمة على الموانئ لمنع الوصول غير المصرح به للكشف عن الأجهزة المشبوهة.
121	Translated (0%)	Advanced continuous threats (APT Protection) shall be applied to the internet gateway used for Zero-Day Malware.	على بوابة الإنترنت (APT حماية) يجب تطبيق التهديدات المستمرة المتقدمة Zero - Day المستخدمة للبرامج الضارة.
122	Translated (0%)	Prevent internal network connection to the Internet directly, and it must be through a proxy to analyze and filter the data transferred to and from Al Hammadi Holding.	منع اتصال الشبكة الداخلية بالإنترنت مباشرة، ويجب أن يكون من خلال وكيل لتحليل وتصفية البيانات المنقولة من وإلى شركة الحمادي القابضة.
123	Translated	Configure firewalls access rules to deny access automatically and	تكوين قواعد الوصول إلى جدران الحماية لرفض الوصول تلقائيًا وبشكل

	(0%)	explicitly to all unspecified segments or devices, and accept rules are only added based on the raised business demand.	صريح إلى جميع الشرائح أو الأجهزة غير المحددة، ويتم إضافة قواعد القبول فقط بناءً على طلب العمل المتزايد.
124	Translated (0%)	DNS security shall be provided.	يجب توفير أمن نظام أسماء النطاقات.
125	Translated (0%)	Intrusion Prevention Systems (IPS) shall be provided in all segments of the network and updated periodically.	في جميع قطاعات الشبكة وتحديثها (IPS) يجب توفير أنظمة منع التسلل بشكل دوري.
126	Translated (0%)	Network APT systems shall be provided on critical systems.	يجب توفير أنظمة ملائمة للشبكة على الأنظمة الحيوية.
127	Translated (0%)	Mechanisms to protect the Internet browsing channel from advanced threats (APT) and previously unknown malware shall be applied and safely managed.	(APT) يجب تطبيق آليات حماية قناة تصفح الإنترنت من التهديدات المتقدمة والبرامج الضارة غير المعروفة سابقًا وإدارتها بأمان.
128	Translated (0%)	Protection of the Distributed Denial of Service Attack “DDoS” shall be provided on critical external systems.	على "DDoS" يجب توفير الحماية لهجوم الحرمان من الخدمة الموزع الأنظمة الخارجية الهامة.
129	Translated (0%)	Segregation in networks	الفصل في الشبكات
130	Translated (0%)	Al Hammadi Holding groups of information services, users, and information systems shall be segregated into separate network domains.	يجب فصل مجموعات الحمادي القابضة من خدمات المعلومات والمستخدمين وأنظمة المعلومات إلى نطاقات شبكة منفصلة.
131	Translated (0%)	Al Hammadi Holding domains shall be chosen based on trust levels (e.g., public access domain, desktop domain, server domain), departments (e.g., human resources, finance, marketing) or a combination (e.g., server domain connecting to multiple organizational units).	يجب اختيار نطاقات الحمادي القابضة بناءً على مستويات الثقة (على سبيل المثال، مجال الوصول العام، مجال سطح المكتب، مجال الخادم)، الإدارات أو مزيج (على سبيل (على سبيل المثال، الموارد البشرية، المالية، التسويق) (المثال، مجال الخادم المتصل بوحدات تنظيمية متعددة.
132	Translated (0%)	The segregation shall be done using physically different networks or by using logical networks (e.g., virtual private networking).	يجب أن يتم الفصل باستخدام شبكات مختلفة ماديًا أو باستخدام شبكات منطقية (على سبيل المثال، الشبكات الخاصة الافتراضية).
133	Translated (0%)	The perimeter of each domain shall be well defined.	يجب أن يكون محيط كل مجال محددًا جيدًا.
134	Translated (0%)	Access between network domains shall be controlled by a perimeter gateway (e.g., firewall, filtering router).	يجب التحكم في الوصول بين نطاقات الشبكة بواسطة بوابة محيط (على سبيل المثال، جدار الحماية، جهاز توجيه التصفية).
135	Translated (0%)	Criteria for segregation of networks into domains, and the access allowed through the gateways, shall be based on an assessment of the security requirements of each domain, in accordance with the access control policy.	يجب أن تستند معايير فصل الشبكات إلى نطاقات، والوصول المسموح به من خلال البوابات، إلى تقييم للمتطلبات الأمنية لكل نطاق، وفقًا لسياسة التحكم في الوصول.
136	Translated (0%)	Authentication, encryption, and user level network access control technologies shall be used with wireless networks to connect to Al Hammadi Holding internal network.	يجب استخدام تقنيات المصادقة والتشفير والتحكم في الوصول إلى الشبكة على مستوى المستخدم مع الشبكات اللاسلكية للاتصال بالشبكة الداخلية لشركة الحمادي القابضة.
137	Translated (0%)	Accessibility to the Network Requirements	إمكانية الوصول إلى متطلبات الشبكة
138	Translated	Al Hammadi Holding cybersecurity department shall adopt	يجب على إدارة الأمن السيبراني في شركة الحمادي القابضة اعتماد إجراءات

	(0%)	procedures for granting and revoking access permissions to the network, in accordance with the identity and access management policy.	.منح وإلغاء تصاريح الوصول إلى الشبكة، وفقًا لسياسة إدارة الهوية والوصول
139	Translated (0%)	To permit user access to the network, the user shall raise access requests to the Information Technology Department stating its validity period and the justifications.	للسماح للمستخدم بالوصول إلى الشبكة، يجب على المستخدم رفع طلبات .الوصول إلى إدارة تكنولوجيا المعلومات مع ذكر فترة صلاحيتها والمبررات
140	Translated (0%)	In case of modifying firewall lists/rules, the network administrator shall document the business requirements and the request information.	في حالة تعديل قوائم/قواعد جدار الحماية، يجب على مسؤول الشبكة توثيق .متطلبات العمل ومعلومات الطلب
141	Translated (0%)	Username and password shall be used to log in to Al Hammadi Holding network in accordance with the identity and access management policy.	يجب استخدام اسم المستخدم وكلمة المرور لتسجيل الدخول إلى شبكة .الحمادي القابضة وفقًا لسياسة إدارة الهوية والوصول
142	Translated (0%)	Firewall Rules shall be reviewed periodically, and at least every six months for critical systems.	يجب مراجعة قواعد جدار الحماية بشكل دوري، وكل ستة أشهر على الأقل .للأنظمة الحرجة
143	Translated (0%)	Secure browsing and restricting access to suspicious websites, file sharing sites, and remote access sites.	التصفح الآمن وتقييد الوصول إلى مواقع الويب المشبوهة ومواقع مشاركة .الملفات ومواقع الوصول عن بُعد
144	Translated (0%)	The wireless network is connected to the internal network of Al Hammadi Holding allowance and is based on risk analysis and guarantees the protection, confidentiality, and integrity of internal technical assets of Al Hammadi Holding.	تتصل الشبكة اللاسلكية بالشبكة الداخلية لبدل شركة الحمادي القابضة وتستند إلى تحليل المخاطر وتضمن حماية وسرية وسلامة الأصول الفنية .الداخلية لشركة الحمادي القابضة
145	Translated (0%)	It is forbidden to connect the critical systems to the wireless network for Al Hammadi Holding.	.يحظر توصيل الأنظمة الحرجة بالشبكة اللاسلكية لشركة الحمادي القابضة
146	Translated (0%)	Restriction techniques are required to manage network ports, protocols, and services.	.تقنيات التقييد مطلوبة لإدارة منافذ الشبكة والبروتوكولات والخدمات
147	Translated (0%)	Al Hammadi Holding IT shall prevent direct connection of internal devices to critical systems prior to checking security requirements and ensure protection measures are applied that match the security acceptable level of critical systems.	يجب على شركة الحمادي القابضة لتقنية المعلومات منع الاتصال المباشر للأجهزة الداخلية بالأنظمة الحيوية قبل التحقق من متطلبات الأمان والتأكد من تطبيق تدابير الحماية التي تتطابق مع المستوى الأمني المقبول للأنظمة .الحيوية
148	Translated (0%)	Third Party Accessibility to the Network Requirements	إمكانية وصول الطرف الثالث إلى متطلبات الشبكة
149	Translated (0%)	Granting access to external parties to Al Hammadi Holding network is subject to the cybersecurity third party policy.	يخضع منح الوصول إلى الأطراف الخارجية لشبكة الحمادي القابضة لسياسة .الطرف الثالث للأمن السيبراني
150	Translated (0%)	Encryption and authentication are required to transfer data to and from third parties.	.التشفير والمصادقة مطلوبان لنقل البيانات من وإلى أطراف ثالثة
151	Translated (0%)	Specify a limited period for external parties to access Al Hammadi Holding network.	.تحديد فترة محدودة للأطراف الخارجية للوصول إلى شبكة الحمادي القابضة
152	Translated (0%)	Periodically review the user access permissions of external parties, in accordance with the cybersecurity policies adopted in Al Hammadi Holding.	المراجعة الدورية لأذونات وصول المستخدمين من الأطراف الخارجية، وفقًا .لسياسات الأمن السيبراني المعتمدة في شركة الحمادي القابضة

153	Translated (0%)	Wireless Protection	الحماية اللاسلكية
154	Translated (0%)	A logically and/or physically segmented wireless network must be designed and implemented, taking into consideration business needs and enterprise architecture, and based on the principles of Defense-in-Depth and multi-tier architecture.	يجب تصميم وتنفيذ شبكة لاسلكية مجزأة منطقيًا و/أو ماديًا، مع مراعاة احتياجات العمل وبنية المؤسسة، واستنادًا إلى مبادئ الدفاع المتعمق والبنية متعددة المستويات.
155	Translated (0%)	Appropriate level of security controls must be applied to different network segments based on the value and classification of information processed in the wireless network, levels of trust, business impact and associated risks.	يجب تطبيق مستوى مناسب من الضوابط الأمنية على قطاعات الشبكة المختلفة بناءً على قيمة وتصنيف المعلومات التي تتم معالجتها في الشبكة اللاسلكية ومستويات الثقة وتأثير الأعمال والمخاطر المرتبطة بها.
156	Translated (0%)	Wireless networks traffic must be logged and designed and configured to filter traffic between different segments and block any unauthorized access.	يجب تسجيل حركة مرور الشبكات اللاسلكية وتصميمها وتكوينها لتصفية حركة المرور بين القطاعات المختلفة ومنع أي وصول غير مصرح به.
157	Translated (0%)	Wireless networks traffic logs must be stored in a secure location as required by the local regulations and standards.	يجب تخزين سجلات حركة مرور الشبكات اللاسلكية في مكان آمن كما هو مطلوب بموجب اللوائح والمعايير المحلية.
158	Translated (0%)	Adjust firewall and routers settings to prevent unauthorized connections between untrusted wireless networks.	اضبط إعدادات جدار الحماية والموجهات لمنع الاتصالات غير المصرح بها بين الشبكات اللاسلكية غير الموثوقة.
159	Translated (0%)	Security configurations, rules, policies and profiles for firewalls and routers must be reviewed on a regular basis in accordance with an approved plan.	يجب مراجعة تكوينات الأمان والقواعد والسياسات والملفات التعريفية لجدران الحماية وأجهزة التوجيه بشكل منتظم وفقًا لخطة معتمدة.
160	Translated (0%)	Critical systems must be prevented from connecting to the wireless network.	يجب منع الأنظمة الحيوية من الاتصال بالشبكة اللاسلكية.
161	Translated (0%)	An up-to-date inventory of all of Al Hammadi Holding's wireless network boundaries must be maintained.	يجب الحفاظ على جرد محدث لجميع حدود الشبكة اللاسلكية لشركة الحمادي القابضة.
162	Translated (0%)	Communications with known malicious or unused Internet IP addresses must be denied, and access must be limited to trusted and necessary IP address ranges at each of Al Hammadi Holding's wireless network boundaries.	يجب رفض الاتصالات بعناوين IP الإنترنت على مستخدمة غير أو ضارة، ويجب أن يقتصر الوصول على نطاقات عناوين IP الموثوقة والضرورية في كل من حدود الشبكة اللاسلكية لشركة الحمادي القابضة.
163	Translated (0%)	Communication over unauthorized TCP or UDP ports or application traffic must be denied to ensure that only authorized protocols are allowed to cross the network boundary in or out of the wireless network at each of Al Hammadi Holding's network boundaries.	يجب رفض الاتصال عبر منافذ TCP أو UDP غير المصرح بها أو حركة مرور التطبيق لضمان السماح للبروتوكولات المصرح بها فقط بعبور حدود الشبكة داخل أو خارج الشبكة اللاسلكية في كل من حدود شبكة الحمادي القابضة.
164	Translated (0%)	Monitoring systems must be configured to record network packets passing through the boundary at each of Al Hammadi Holding's wireless network boundaries.	يجب تكوين أنظمة المراقبة لتسجيل حزم الشبكة التي تمر عبر الحدود في كل من حدود الشبكة اللاسلكية لشركة الحمادي القابضة.
165	Translated (0%)	Network-based Intrusion Prevention Systems (IPS) must be deployed to block malicious network traffic at each of Al Hammadi Holding's wireless network boundaries.	يجب نشر أنظمة منع التسلل القائمة على الشبكة (IPS) لمنع حركة مرور الشبكة الضارة في كل من حدود الشبكة اللاسلكية لشركة الحمادي القابضة.
166	Translated	Network-based Advanced Persistent Threat (APT)	يجب نشر أنظمة الكشف عن التهديدات المستمرة المتقدمة (APT) القائمة

	(0%)	detection/prevention systems must be deployed to detect or block malicious network attacks and Zero-Day attacks at each of Al Hammadi Holding's network boundaries.	على الشبكة للكشف عن هجمات الشبكة الخبيثة وهجمات يوم الصفر أو منعها في كل من حدود شبكة شركة الحمادي القابضة.
167	Translated (0%)	The collection of NetFlow and event logging must be enabled on all wireless network boundary devices.	وتسجيل الأحداث على جميع أجهزة حدود NetFlow يجب تمكين جمع الشبكة اللاسلكية.
168	Translated (0%)	All wireless network traffic to/from the Internet must pass through an authenticated application layer proxy that is configured to filter unauthorized connections.	يجب أن تمر جميع حركة مرور الشبكة اللاسلكية من/إلى الإنترنت عبر وكيل طبقة تطبيق مصادق عليه تم تكوينه لتصفية الاتصالات غير المصرح بها.
169	Translated (0%)	Domain Name System (DNS) query logging must be enabled to detect hostname lookups for known malicious domains.	للكشف عن (DNS) يجب تمكين تسجيل استعلام نظام أسماء النطاقات عمليات البحث عن اسم المضيف للنطاقات الضارة المعروفة.
170	Translated (0%)	All subscription services, URL categories, threat feeds, blacklists, and signatures must be up-to-date and updated regularly.	وموجزات URL يجب تحديث جميع خدمات الاشتراك وفئات عناوين التهديدات والقوائم السوداء والتوقيعات وتحديثها بانتظام.
171	Translated (0%)	A separate wireless network must be created for personal or untrusted devices.	يجب إنشاء شبكة لاسلكية منفصلة للأجهزة الشخصية أو غير الموثوقة.
172	Translated (0%)	Enterprise access from this network must be treated as untrusted and must be filtered and audited accordingly.	يجب التعامل مع وصول المؤسسة من هذه الشبكة على أنه غير موثوق به ويجب تصفيته وتدقيقه وفقًا لذلك.
173	Translated (0%)	All physical wireless network devices must be scanned for signs of tampering upon installation.	يجب فحص جميع أجهزة الشبكة اللاسلكية المادية بحثًا عن علامات العبث عند التثبيت.
174	Translated (0%)	Software, updates, patches, and upgrades to wireless network components must be obtained from validated sources.	يجب الحصول على البرامج والتحديثات والتصحيحات والترقيات لمكونات الشبكة اللاسلكية من مصادر تم التحقق من صحتها.
175	Translated (0%)	A comprehensive risk assessment exercise must be conducted to evaluate the risks of connecting wireless networks to the internal network.	يجب إجراء تمرين شامل لتقييم المخاطر لتقييم مخاطر توصيل الشبكات اللاسلكية بالشبكة الداخلية.
176	Translated (0%)	Protection Against DDOS	الحماية من حجب الخدمة الموزعة
177	Translated (0%)	DDoS protection solution must protect both IPv4 and IPv6 stack of Al Hammadi Holding's network.	لشبكة الحمادي IPv6 و IPv4 كلًا من حزمة DDoS يجب أن يحمي حل حماية القابضة.
178	Translated (0%)	DDoS protection solution must have consistent application uptime and availability.	على وقت تشغيل وتوافر متسق للتطبيق DDoS يجب أن يحتوي حل حماية.
179	Translated (0%)	DDoS protection solution must protect networks, DNS servers, publicly accessible & hosted websites within Al Hammadi Holding IT environment and individual IPs.	ومواقع الويب التي DNS الشبكات وخوادم DDoS يجب أن يحمي حل حماية يمكن الوصول إليها بشكل عام والمستضافة داخل بيئة تكنولوجيا المعلومات الفردية IP في شركة الحمادي القابضة وعناوين.
180	Translated (0%)	DDoS protection solution must have a multi-layered protection from DDoS attacks on the network and application layers, volumetric and non-volumetric attacks, as well as full coverage of SSL/TLS-based DDoS attacks.	على حماية متعددة الطبقات من هجمات DDoS يجب أن يحتوي حل حماية DDoS على الشبكة وطبقات التطبيق والهجمات الحجمية وغير الحجمية، المستندة إلى SSL/TLS بالإضافة إلى التغطية الكاملة لهجمات DDoS.
181	Translated (0%)	All Al Hammadi Holding's IT administrators defined in Access Management Principles that need access to the DDoS attacks logs must have configured access to the logs database.	يجب أن يكون جميع مسؤولي تكنولوجيا المعلومات في شركة الحمادي القابضة المحددين في مبادئ إدارة الوصول الذين يحتاجون إلى الوصول إلى سجلات هجمات حجب الخدمة الموزعة قد قاموا بتكوين الوصول إلى قاعدة

			.بيانات السجلات
182	Translated (0%)	All security updates to the DDoS protection solution must be installed in accordance to patch management process.	وفقًا لعملية DDoS يجب تثبيت جميع التحديثات الأمنية على حل حماية .إدارة التصحيح
183	Translated (0%)	All management communication channels must be using a dedicated management network or the management network communications which are authenticated and encrypted using cryptographic modules validated in line with National Cryptography Standard and internal Al Hammadi Holding's cryptography standards.	يجب أن تستخدم جميع قنوات الاتصال الإداري شبكة إدارة مخصصة أو اتصالات شبكة الإدارة التي يتم مصادقتها وتشفيرها باستخدام وحدات تشفير تم التحقق من صحتها بما يتماشى مع معيار التشفير الوطني ومعايير التشفير .الداخلية لشركة الحمادي القابضة
184	Translated (0%)	There must be protection in case of access to the managing console in DDoS as a Service deployment method.	يجب أن تكون هناك حماية في حالة الوصول إلى وحدة التحكم الإدارية في .كطريقة لنشر الخدمة DDoS
185	Translated (0%)	DDoS Response and mitigation plan should be established in accordance with the relevant legislative and regulatory requirements.	يجب وضع خطة الاستجابة لحجب الخدمة الموزعة والتخفيف من حدتها .وفقًا للمتطلبات التشريعية والتنظيمية ذات الصلة
186	Translated (0%)	Al Hammadi Holding must perform periodic training for employees to ensure that they know how to choose the right mitigation service and measure training effectiveness based on reviewing the KPIs annually.	يجب على شركة الحمادي القابضة إجراء تدريب دوري للموظفين للتأكد من معرفتهم بكيفية اختيار خدمة التخفيف المناسبة وقياس فعالية التدريب بناءً .على مراجعة مؤشرات الأداء الرئيسية سنويًا
187	Translated (0%)	DDoS protection solution must provide reports and dashboards of prevented attacks and actions.	تقارير ولوحات معلومات للهجمات DDoS يجب أن يوفر حل حماية .والإجراءات التي تم منعها
188	Translated (0%)	Al Hammadi Holding must define key performance indicators to track effectiveness and trends related to DDoS protection solution.	يجب على شركة الحمادي القابضة تحديد مؤشرات الأداء الرئيسية لتتبع .الفعالية والاتجاهات المتعلقة بحل حماية حجب الخدمة الموزعة
189	Translated (0%)	DDoS protection solution must use automation to quickly mitigate arising attacks.	الأتمتة للتخفيف بسرعة من الهجمات DDoS يجب أن يستخدم حل حماية .الناشئة
190	Translated (0%)	DDoS protection solution should use machine learning and artificial intelligence in order to prevent new threats.	التعلم الآلي والذكاء الاصطناعي من أجل DDoS يجب أن يستخدم حل حماية .منع التهديدات الجديدة
191	Translated (100%)	Information transfer	نقل المعلومات
192	Translated (0%)	Al Hammadi Holding shall maintain the security of information transferred within the organization and with any external entity.	تحافظ شركة الحمادي القابضة على أمن المعلومات المنقولة داخل المؤسسة .ومع أي جهة خارجية
193	Translated (0%)	Information transfer may occur using several types of communication facilities, including electronic mail, voice, facsimile, and video.	قد يحدث نقل المعلومات باستخدام عدة أنواع من مرافق الاتصال، بما في .ذلك البريد الإلكتروني والصوت والفاكس والفيديو
194	Translated (0%)	Software transfer may occur through several mediums, including downloading from the Internet and acquiring from vendors.	قد يتم نقل البرامج من خلال عدة وسائل، بما في ذلك التنزيل من الإنترنت .والاستحواذ من البائعين
195	Translated (0%)	Al Hammadi Holding business, legal and security implications associated with electronic data interchange, electronic commerce and electronic communications and the requirements for controls shall be considered.	يجب مراعاة الآثار التجارية والقانونية والأمنية المرتبطة بالتبادل الإلكتروني .للبيانات والتجارة الإلكترونية والاتصالات الإلكترونية ومتطلبات الضوابط
196	Translated (0%)	Al Hammadi Holding shall protect transferred information from interception, copying, modification, misrouting, and destruction.	يجب على شركة الحمادي القابضة حماية المعلومات المنقولة من الاعتراض .والنسخ والتعديل وسوء التوجيه والتدمير
197	Translated (0%)	Al Hammadi Holding shall detect and protect against malware transmitted through electronic communications.	تقوم شركة الحمادي القابضة بالكشف والحماية من البرامج الضارة التي .تنتقل عبر الاتصالات الإلكترونية

198	Translated (0%)	Al Hammadi Holding shall protect communicated sensitive electronic information that is in the form of an attachment.	يجب على شركة الحمادي القابضة حماية المعلومات الإلكترونية الحساسة التي يتم توصيلها في شكل مرفق.
199	Translated (0%)	Al Hammadi Holding shall ensure that employees and external parties will not compromise the organization through defamation, harassment, impersonation, forwarding of chain letters, unauthorized purchasing, etc.	تضمن شركة الحمادي القابضة عدم تعريض الموظفين والأطراف الخارجية المنظمة للخطر من خلال التشهير والمضايقة وانتحال الشخصية وإعادة توجيه الرسائل المتسلسلة والشراء غير المصرح به وما إلى ذلك.
200	Translated (0%)	Al Hammadi Holding shall use cryptographic techniques to protect the confidentiality, integrity, and authenticity of information.	يجب على شركة الحمادي القابضة استخدام تقنيات التشفير لحماية سرية وسلامة وصحة المعلومات.
201	Translated (0%)	Al Hammadi Holding shall comply with retention and disposal guidelines for all business correspondence, including messages, in accordance with relevant national and local legislation and regulations.	تلتزم شركة الحمادي القابضة بإرشادات الاحتفاظ والتخلص من جميع مراسلات الأعمال، بما في ذلك الرسائل، وفقًا للتشريعات واللوائح الوطنية والمحلية ذات الصلة.
202	Translated (0%)	Al Hammadi Holding shall implement controls and restrictions to prevent using communications for automatic forwarding of electronic mail to external mail addresses.	يجب على شركة الحمادي القابضة تنفيذ الضوابط والقيود لمنع استخدام الاتصالات لإعادة التوجيه التلقائي للبريد الإلكتروني إلى عناوين البريد الخارجي.
203	Translated (0%)	Al Hammadi Holding shall implement controls and restrictions to prevent deliberate programming of sending messages to specific phone numbers.	يجب على شركة الحمادي القابضة تنفيذ الضوابط والقيود لمنع البرمجة المتعمدة لإرسال الرسائل إلى أرقام هواتف محددة.
204	Translated (0%)	Al Hammadi Holding shall implement controls to prevent sending documents and messages to the wrong number/s either by misdialing or using the wrong stored number.	يجب على شركة الحمادي القابضة تنفيذ ضوابط لمنع إرسال المستندات والرسائل إلى الرقم/الأرقام الخاطئة إما عن طريق الاتصال الخاطئ أو استخدام الرقم المخزن الخاطئ.
205	Translated (0%)	Al Hammadi Holding personnel shall be reminded that they shall not have confidential conversations in public places or over insecure communication channels, open offices, and meeting places.	يجب تذكير موظفي شركة الحمادي القابضة بأنه لا يجوز لهم إجراء محادثات سرية في الأماكن العامة أو عبر قنوات الاتصال غير الآمنة والمكاتب المفتوحة وأماكن الاجتماعات.
206	Translated (0%)	Agreements on information transfer	اتفاقيات نقل المعلومات
207	Translated (0%)	Agreements shall address the secure transfer of business information between Al Hammadi Holding and external parties.	يجب أن تتناول الاتفاقيات النقل الآمن لمعلومات العمل بين شركة الحمادي القابضة والأطراف الخارجية.
208	Translated (0%)	Information transfer agreements shall safeguard the following:	يجب أن تحمي اتفاقيات نقل المعلومات ما يلي:
209	Translated (0%)	controlling and notifying transmission, dispatch, and receipt.	مراقبة وإخطار الإرسال والإرسال والاستلام.
210	Translated (0%)	traceability and non-repudiation.	التتبع وعدم الإنكار.
211	Translated (0%)	escrow agreements.	اتفاقيات الضمان.
212	Translated (0%)	courier identification standards.	معايير تحديد هوية البريد السريع.
213	Translated	responsibilities and liabilities in the event of information security	المسؤوليات والمسؤوليات في حالة حوادث أمن المعلومات، مثل فقدان

	(0%)	incidents, such as loss of data.	.البيانات
214	Translated (0%)	special controls that are required to protect sensitive items, such as cryptography.	.الضوابط الخاصة المطلوبة لحماية العناصر الحساسة، مثل التشفير
215	Translated (0%)	maintaining a chain of custody for information while in transit.	.الحفاظ على سلسلة الحراسة للحصول على المعلومات أثناء النقل
216	Translated (0%)	acceptable levels of access control	مستويات مقبولة من التحكم في الوصول
217	Translated (0%)	Electronic messaging	المراسلة الإلكترونية
218	Translated (0%)	Information involved in electronic messaging shall be appropriately protected.	.يجب حماية المعلومات المتعلقة بالرسائل الإلكترونية بشكل مناسب
219	Translated (0%)	Al Hammadi Holding shall implement controls to protect messages from unauthorized access, modification, or denial of service, commensurate with Al Hammadi Holding classification scheme.	يجب على شركة الحمادي القابضة تنفيذ ضوابط لحماية الرسائل من الوصول غير المصرح به أو التعديل أو رفض الخدمة، بما يتناسب مع مخطط تصنيف .شركة الحمادي القابضة
220	Translated (0%)	Al Hammadi Holding shall ensure correct addressing and transportation of the message.	.تضمن شركة الحمادي القابضة العناوين الصحيحة ونقل الرسالة
221	Translated (0%)	Al Hammadi Holding shall ensure the reliability and availability of the service.	.تضمن شركة الحمادي القابضة موثوقية الخدمة وتوافرها
222	Translated (0%)	Al Hammadi Holding shall ensure address legal requirements for electronic and digital signatures.	تضمن شركة الحمادي القابضة تلبية المتطلبات القانونية للتوقيعات .الإلكترونية والرقمية
223	Translated (0%)	Al Hammadi Holding employees shall obtain approval prior to using external public services such as instant messaging, social networking, or file sharing	يجب على موظفي شركة الحمادي القابضة الحصول على موافقة قبل استخدام الخدمات العامة الخارجية مثل المراسلة الفورية أو الشبكات الاجتماعية أو مشاركة الملفات
224	Translated (100%)	Web Filtering	تصفية الويب
225	Translated (0%)	Al Hammadi Holding shall use a centralized web filtering solution to monitor and control outbound and inbound internet traffic.	يجب على شركة الحمادي القابضة استخدام حل تصفية ويب مركزي لمراقبة .ومراقبة حركة المرور على الإنترنت الصادرة والواردة
226	Translated (0%)	Al Hammadi Holding shall implement a combination of URL filtering, DNS filtering, content filtering, and real-time scanning for malicious threats.	URL، يجب على شركة الحمادي القابضة تنفيذ مزيج من تصفية عناوين وتصفية المحتوى، والمسح في الوقت الفعلي للتهديدات ،DNS وتصفية .الضارة
227	Translated (0%)	Restrict access to high-risk or unauthorized sites by default, with exceptions based on role or necessity for specific job functions	،تقييد الوصول إلى المواقع عالية المخاطر أو غير المصرح بها بشكل افتراضي مع استثناءات بناءً على الدور أو الضرورة لوظائف وظيفية محددة
228	Translated (0%)	Exceptions to the filtering policy can be made by authorized personnel for specific business needs.	يمكن إجراء استثناءات لسياسة التصفية من قبل الموظفين المعتمدين لتلبية .احتياجات عمل محددة
229	Translated (0%)	These exceptions should be documented, monitored, and reviewed periodically.	.يجب توثيق هذه الاستثناءات ومراقبتها ومراجعتها بشكل دوري
230	Translated (0%)	Web traffic logs must be captured and stored securely, detailing which sites were accessed, the time of access, and the user responsible.	يجب تسجيل سجلات حركة مرور الويب وتخزينها بشكل آمن، مع تفصيل .المواقع التي تم الوصول إليها ووقت الوصول والمستخدم المسؤول

231	Translated (0%)	Regular reviews of logs should be conducted to identify unusual or unauthorized activity.	يجب إجراء مراجعات منتظمة للسجلات لتحديد النشاط غير العادي أو غير المصرح به.
232	Translated (0%)	Incident reports should be generated if suspicious or non-compliant web activity is detected, and corrective actions should be implemented immediately.	يجب إنشاء تقارير الحوادث إذا تم اكتشاف نشاط ويب مشبوه أو غير متوافق، ويجب تنفيذ الإجراءات التصحيحية على الفور.
233	Translated (0%)	Confidentiality or nondisclosure agreements	اتفاقيات السرية أو عدم الإفصاح
234	Translated (0%)	Confidentiality or non-disclosure agreements shall address the requirement to protect confidential information using legally enforceable terms.	يجب أن تتناول اتفاقيات السرية أو عدم الإفصاح متطلبات حماية المعلومات السرية باستخدام شروط قابلة للتنفيذ قانونًا.
235	Translated (0%)	Confidentiality or non-disclosure agreements are applicable to external parties and Al Hammadi Holding employees.	تنطبق اتفاقيات السرية أو عدم الإفصاح على الأطراف الخارجية وموظفي شركة الحمادي القابضة.
236	Translated (0%)	Elements shall be selected or added in consideration of the type of the other party and its permissible access or handling of confidential information.	يتم اختيار العناصر أو إضافتها مع مراعاة نوع الطرف الآخر والوصول المسموح به أو التعامل مع المعلومات السرية.
237	Translated (0%)	To identify requirements for confidentiality or non-disclosure agreements, Al Hammadi Holding shall identify the following elements:	لتحديد متطلبات اتفاقيات السرية أو عدم الإفصاح، يجب على شركة الحمادي القابضة تحديد العناصر التالية:
238	Translated (0%)	a definition of the information to be protected.	تعريف المعلومات المراد حمايتها.
239	Translated (0%)	expected duration of the agreement.	المدة المتوقعة للاتفاقية.
240	Translated (0%)	cases where confidentiality might need to be maintained indefinitely.	الحالات التي قد يلزم فيها الحفاظ على السرية إلى أجل غير مسمى.
241	Translated (0%)	required actions when an agreement is terminated.	الإجراءات المطلوبة عند إنهاء الاتفاقية.
242	Translated (0%)	responsibilities and actions of signatories to avoid unauthorized information disclosure.	مسؤوليات وإجراءات الموقعين لتجنب الكشف عن المعلومات غير المصرح به.
243	Translated (0%)	ownership of information, trade secrets, and intellectual property.	ملكية المعلومات والأسرار التجارية والملكية الفكرية.
244	Translated (0%)	the permitted use of confidential information and rights of the signatory to use information.	الاستخدام المسموح به للمعلومات السرية وحقوق الموقع في استخدام المعلومات.
245	Translated (0%)	the right to audit and monitor activities that involve confidential information.	الحق في تدقيق ومراقبة الأنشطة التي تنطوي على معلومات سرية.
246	Translated (0%)	process for notification and reporting of unauthorized disclosure or confidential information leakage.	عملية الإخطار والإبلاغ عن الكشف غير المصرح به أو تسرب المعلومات السرية.
247	Translated (0%)	terms for information to be returned or destroyed at agreement cessation.	شروط إعادة المعلومات أو إتلافها عند انتهاء الاتفاقية.
248	Translated	expected actions to be taken in case of a breach of the agreement.	الإجراءات المتوقع اتخاذها في حالة خرق الاتفاقية.

	(0%)		
249	Translated (100%)	Physical and Environmental Security	الأمن الفيزيائي والبيئي
250	Translated (0%)	Network devices shall be kept in a safe and secure environment, and ensure that the temperature and humidity are adjusted, as well as the presence of backup power sources such as (Uninterruptible Power Supply “UPS”).	يجب الاحتفاظ بأجهزة الشبكة في بيئة آمنة ومأمونة، والتأكد من ضبط درجة الحرارة والرطوبة، وكذلك وجود مصادر طاقة احتياطية مثل (مزود الطاقة غير المنقطع "UPS ")..
251	Translated (0%)	Physical access to the network devices shall be restricted to authorized personnel only to protect them from theft or tampering.	يقتصر الوصول المادي إلى أجهزة الشبكة على الموظفين المصرح لهم فقط لحمايتهم من السرقة أو العبث.
252	Translated (0%)	Log records shall be maintained, and CCTV placed in devices areas for monitoring and periodically review logs.	يجب الاحتفاظ بسجلات السجل، ووضع كاميرات المراقبة في مناطق الأجهزة لمراقبة السجلات ومراجعتها بشكل دوري.
253	Translated (0%)	Other Requirements	متطلبات أخرى
254	Translated (0%)	Cybersecurity network security requirements shall be reviewed annually, or if legislative or regulatory requirements or related standards change.	يجب مراجعة متطلبات أمن شبكة الأمن السيبراني سنويًا، أو إذا تغيرت المتطلبات التشريعية أو التنظيمية أو المعايير ذات الصلة.
255	Translated (100%)	Compliance and Adherence	الامتثال والالتزام
256	Translated (100%)	Al Hammadi Holding CEO shall ensure compliance with the cybersecurity policies and standards.	يضمن الرئيس التنفيذي لشركة الحمادي القابضة الامتثال لسياسات ومعايير الأمن السيبراني.
257	Translated (98%)	To ensure compliance, the Cybersecurity department will establish regular reporting by the Cybersecurity Manager, conduct periodic audits, or form a Cybersecurity Steering Committee for oversight.	لضمان الامتثال، سينشئ قسم الأمن السيبراني نظامًا لتقديم تقارير منتظمة يُعدّها مدير الأمن السيبراني، ويجري عمليات تدقيق دورية، أو يشكل لجنة توجيهية للأمن السيبراني للإشراف.
258	Translated (99%)	The CS Manager shall ensure adherence to this policy.	يتعين على مدير الأمن السيبراني ضمان الالتزام بهذه السياسة.
259	Translated (100%)	All employees of Al Hammadi Holding must adhere to this policy.	على جميع موظفي شركة الحمادي القابضة الالتزام بهذه السياسة.
260	Translated (100%)	Violations of this policy may result in legal action in any jurisdiction or other measures as deemed appropriate by the Al Hammadi Holding.	قد تؤدي انتهاكات هذه السياسة إلى اتخاذ إجراءات قانونية في أي ولاية قضائية أو غيرها من التدابير التي تراها شركة الحمادي القابضة مناسبة.
261	Translated (100%)	Exceptions	الاستثناءات
262	Translated (100%)	Violation of cybersecurity policies and standards is prohibited unless a prior justified exception is obtained from the Cybersecurity Department or the Cybersecurity Steering Committee.	يُحظر انتهاك سياسات ومعايير الأمن السيبراني ما لم يتم الحصول على استثناء مبرر مسبق من إدارة الأمن السيبراني أو اللجنة التوجيهية للأمن السيبراني.
263	Translated (100%)	In case of a conflict, applicable legislative and regulatory requirements overrule Al Hammadi Holding policies and standards.	في حالة وجود تعارض، فإن المتطلبات التشريعية والتنظيمية المعمول بها تسود على سياسات ومعايير شركة الحمادي القابضة.
264	Translated (100%)	Revision	المراجعة
265	Translated	This policy is reviewed annually, after major changes in Al Hammadi	تخضع هذه السياسة لمراجعة سنوية، ولإعادة التقييم بعد أي تغييرات

	(100%)	Holding’s organizational chart or infrastructure, and more frequently whenever required, to ensure it remains appropriate and current for Al Hammadi Holding, ISO 27001, and NCA requirements.	،جوهرية في الهيكل التنظيمي أو البنية التحتية لشركة الحمادي القابضة إضافة إلى مراجعات دورية إضافية عند الضرورة، وذلك لضمان توافقها ISO المستمر مع متطلبات شركة الحمادي القابضة، ومعيار آيزو .وإرشادات الهيئة الوطنية للأمن السيبراني ،27001:2022
266	Translated (0%)	9.	9.
267	Translated (100%)	Approval Section	قسم الاعتماد
268	Translated (100%)	Prepared by:	:إعداد
269	Translated (100%)	Mr. Mohammed Alamer	السيد/ محمد العامر
270	Translated (100%)	GRC Cybersecurity Specialist	أخصائي حوكمة ومخاطر وامتثال في الأمن السيبراني
271	Translated (100%)	Name	الاسم
272	Translated (100%)	Designation	المسمى الوظيفي
273	Translated (100%)	Signature	التوقيع
274	Translated (100%)	Date	التاريخ
275	Translated (100%)	Reviewed by:	:راجعها
276	Translated (100%)	Mr. Deepak Dasan	السيد/ ديباك داسان
277	Translated (100%)	IT Manager	مدير تكنولوجيا المعلومات
278	Translated (100%)	Name	الاسم
279	Translated (100%)	Designation	المسمى الوظيفي
280	Translated (100%)	Signature	التوقيع
281	Translated (100%)	Date	التاريخ
282	Translated (100%)	Reviewed by:	:راجعها
283	Translated	Ms. Mashael Alotaibi	السيدة/ مشاعل العتيبي

	(100%)		
284	Translated (100%)	<1711>Cybersecurity </1711>Manager	<مدير <1711>الأمن السيبراني</1711/>
285	Translated (100%)	Name	الاسم
286	Translated (100%)	Designation	المسمى الوظيفي
287	Translated (100%)	Signature	التوقيع
288	Translated (100%)	Date	التاريخ
289	Translated (100%)	Approved by:	:اعتمدها
290	Translated (100%)	Dr. Abdulaziz Al Hammadi	<Bold><Bold>د./ عبد العزيز</Bold></Bold>الحمادي <Bold><Bold></Bold></Bold>
291	Translated (100%)	Chief Operating Officer	الرئيس التنفيذي للعمليات
292	Translated (100%)	Name	الاسم
293	Translated (100%)	Designation	المسمى الوظيفي
294	Translated (100%)	Signature	التوقيع
295	Translated (100%)	Date	التاريخ
296	Translated (100%)	Approved by:	:اعتمدها
297	Translated (0%)	Mr. Mohammad Al Hammadi	السيد/ محمد الحمادي
298	Translated (100%)	Chief Executive Officer	الرئيس التنفيذي
299	Translated (100%)	Name	الاسم
300	Translated (100%)	Designation	المسمى الوظيفي
301	Translated (100%)	Signature	التوقيع
302	Translated (100%)	Date	التاريخ

Segment ID	Segment status	Source segment	Target segment
1	Translated (0%)	<3/><7/> <23><10>Information Security Compliance Management Policy<17/> </10></23>	<3/><7/> <23><10>17>سياسة إدارة الامتثال لأمن المعلومات/> </10></23>
2	Translated (100%)	Page <34><25/> of <33/></34>	34/></33> من </25><34>صفحة
3	Translated (100%)	Al Hammadi Holding	شركة الحمادي القابضة
4	Translated (100%)	Information Security Compliance	الامتثال لأمن المعلومات
5	Translated (100%)	Management Policy	سياسة الإدارة
6	Translated (100%)	CYBERSECURITY DEPARTMENT	إدارة الأمن السيبراني
7	Translated (100%)	Policy ID	معرّف السياسة
8	Translated (100%)	AHH-CS-ISMS-011	AHH-CS-ISMS-011
9	Translated (100%)	Class	الفئة
10	Translated (100%)	Internal Release	إصدار داخلي
11	Not Translated (0%)		
12	Translated (100%)	V3.1	V3.1
13	Translated (100%)	Published at	نُشرت في
14	Translated (100%)	April 2025	أبريل 2025
15	Translated (100%)	Document Owner	المسؤول عن المستند
16	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
17	Translated (100%)	Disclaimer	تنويه
18	Translated (100%)	The information contained in this document is the property of Hammadi Holding and must not be copied or communicated to a third party or used	المعلومات الواردة في هذا المستند هي ملك لشركة الحمادي القابضة ولا يجوز نسخها أو إبلاغها إلى طرف ثالث أو استخدامها لأي غرض آخر غير

		for any purpose other than that for which it is supplied, without the written consent of Al Hammadi Holding.	الغرض الذي تم توفيرها من أجله، دون موافقة خطية من شركة الحمادي القابضة.
19	Translated (100%)	Contents	جدول المحتويات
20	Translated (100%)	Document Information	معلومات المستند
21	Translated (100%)	Synopsis	الملخص
22	Translated (100%)	Document Title:	عنوان المستند:
23	Translated (0%)	Information Security Compliance Management Policy	سياسة إدارة الامتثال لأمن المعلومات
24	Translated (100%)	Document Status:	حالة المستند:
25	Translated (100%)	Approved	معتمد
26	Translated (100%)	Document Effective Date:	تاريخ سريان المستند:
27	Translated (100%)	April 2025	أبريل 2025
28	Translated (100%)	Document Issue Date:	تاريخ إصدار المستند:
29	Translated (100%)	April 2025	أبريل 2025
30	Translated (100%)	Document Next Revision Date:	تاريخ المراجعة التالية للمستند:
31	Translated (100%)	April 2026	أبريل 2026
32	Translated (100%)	Key contacts	جهات التواصل الرئيسية
33	Translated (100%)	Document Owner:	المسؤول عن المستند:
34	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
35	Translated (100%)	Approval Authority	جهة الاعتماد
36	Translated (100%)	Document Created by:	مُنشئ المستند:
37	Translated	IT Management	إدارة تكنولوجيا المعلومات

	(100%)		
38	Translated (100%)	Document Reviewed by:	:راجع المستند
39	Translated (100%)	Al Hammadi Holding CS&IT Managers	مديرو الأمن السيبراني وتكنولوجيا المعلومات في شركة الحمادي القابضة
40	Translated (100%)	Document Approved by:	:اعتمد المستند
41	Translated (100%)	Al Hammadi Holding COO & CEO	الرئيس التنفيذي للعمليات والرئيس التنفيذي في شركة الحمادي القابضة
42	Translated (100%)	Note:	:ملاحظة
43	Translated (100%)	Any additional approval will be added in the document annex	تُضاف أي اعتمادات إضافية في ملحق المستند
44	Translated (100%)	Classification	التصنيف
45	Translated (100%)	Company Internal – to be shared with 3rd parties after consent of CS Manager	داخلي لاستخدام للشركة – يُسمح بمشاركته مع جهات خارجية بعد موافقة مدير إدارة الأمن السيبراني
46	Translated (100%)	Version / Dates	الإصدار / التواريخ
47	Translated (100%)	Current Version:	:الإصدار الحالي
48	Translated (100%)	V3.1	V3.1
49	Translated (100%)	Date Published:	:تاريخ النشر
50	Translated (100%)	April 2025	أبريل 2025
51	Translated (100%)	Date of Next Review:	:تاريخ المراجعة التالية
52	Translated (0%)	April*<315>* 2026*</315>*	*315/>*2026 *<315>*أبريل*<*
53	Translated (100%)	Prior Version:	:الإصدار السابق
54	Translated (100%)	3.0	3.0
55	Translated (100%)	Prior Published:	:تاريخ النشر السابق
56	Translated (100%)	December 2023	ديسمبر 2023

57	Translated (100%)	Document Control	ضبط المستندات
58	Translated (100%)	Document Changes	التغييرات على المستند
59	Translated (100%)	Date	التاريخ
60	Translated (100%)	Version	الإصدار
61	Translated (100%)	Document Owner	المسؤول عن المستند
62	Translated (100%)	Change Description	وصف التغيير
63	Translated (100%)	December 2024	ديسمبر 2024
64	Translated (100%)	3.0	3.0
65	Translated (100%)	IT Management	إدارة تكنولوجيا المعلومات
66	Translated (100%)	Updated policy number to	تحديث رقم السياسة إلى
67	Translated (100%)	April 2025	أبريل 2025
68	Translated (100%)	3.1	3.1
69	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
70	Translated (100%)	Document reviewed and updated based on NCA ECC-2:2024 and ISO27001:2022 requirements	تمت مراجعة المستند وتحديثه استنادًا إلى متطلبات الهيئة الوطنية للأمن السيبراني (NCA) المعيار ECC-2:2024 ومعيار آيزو ISO 27001:2022.
71	Translated (100%)	Document Circulation	تعميم المستند
72	Translated (100%)	To	إلى
73	Translated (100%)	Date	التاريخ
74	Translated (100%)	Method	الطريقة
75	Translated (0%)	IT Security Function	وظيفة أمن تكنولوجيا المعلومات
76	Translated	December 2024	ديسمبر 2024

	(100%)		
77	Translated (0%)	Email/ Employee Intranet Portal	البريد الإلكتروني/ بوابة الإنترانت للموظف
78	Translated (0%)	Application and Development Function	وظيفة التطبيق والتطوير
79	Translated (100%)	December 2024	ديسمبر 2024
80	Translated (100%)	Email/ Employee Intranet Portal	البريد الإلكتروني/ بوابة الإنترانت للموظف
81	Translated (0%)	Change Management Function	وظيفة إدارة التغيير
82	Translated (100%)	December 2024	ديسمبر 2024
83	Translated (100%)	Email/ Employee Intranet Portal	البريد الإلكتروني/ بوابة الإنترانت للموظف
84	Translated (0%)	Business Support Function	وظيفة دعم الأعمال
85	Translated (100%)	December 2024	ديسمبر 2024
86	Translated (100%)	Email/ Employee Intranet Portal	البريد الإلكتروني/ بوابة الإنترانت للموظف
87	Translated (0%)	Information Technology Department	إدارة تقنية المعلومات
88	Translated (100%)	December 2024	ديسمبر 2024
89	Translated (100%)	Email/ Employee Intranet Portal	البريد الإلكتروني/ بوابة الإنترانت للموظف
90	Translated (0%)	Objective<484/>s	الأهداف<484/>
91	Translated (0%)	The purpose of this policy is to set the principles and procedural implementation guidelines, by which Al Hammadi Holding shall comply with the applicable national and international legal, statutory, regulatory, and contractual obligations related to information security, in compliance with the requirements specified in:	،الغرض من هذه السياسة هو وضع المبادئ وإرشادات التنفيذ الإجرائية والتي بموجبها تلتزم شركة الحمادي القابضة بالالتزامات القانونية والقانونية والتنظيمية والتعاقدية الوطنية والدولية المعمول بها المتعلقة بأمن المعلومات، وفقًا للمتطلبات المحددة في:
92	Translated (100%)	ISO/IEC 27001:2022 Annex-A:	الملحق أ IEC 27001:2022/معيار آيزو:
93	Translated (0%)	A.5.31 Legal, statutory, regulatory and contractual requirements, A.5.32 Intellectual property rights, A.5.33 Protection of records, A.5.34 Privacy and protection of PII.	أ .5.31 المتطلبات القانونية والقانونية والتنظيمية والتعاقدية، أ .5.32 حقوق الملكية الفكرية، أ .5.33 حماية السجلات، أ .5.34 الخصوصية وحماية معلومات التعريف الشخصية.

94	Translated (100%)	NCA ECC-2:2024:	ECC-2:2024: معيار الهيئة الوطنية للأمن السيبراني رقم
95	Translated (0%)	1-7 Compliance with Cybersecurity Standards, Laws and Regulations, 2-7 Data and Information Protection	1-7 الامتثال لمعايير وقوانين ولوائح الأمن السيبراني، 2-7 حماية البيانات والمعلومات
96	Translated (100%)	Scope	النطاق
97	Translated (100%)	This policy is applicable to all Al Hammadi Holding ISMS information assets, security operations, Healthcare systems, and all persons doing work under Al Hammadi Holding control.	تنطبق هذه السياسة على جميع أصول معلومات نظام إدارة أمن المعلومات في شركة الحمادي القابضة والعمليات الأمنية والأنظمة الصحية وجميع الأشخاص الذين يعملون تحت إشراف شركة الحمادي القابضة.
98	Translated (100%)	This includes employees, contractors, suppliers, and 3rd Parties.	وتشمل السياسة الموظفين والمتعاقدين والموردين والجهات الخارجية.
99	Translated (100%)	Roles and Responsibilities	الأدوار والمسؤوليات
100	Translated (0%)	Al Hammadi Holding Legal Department, Cybersecurity and IT Departments are responsible for maintaining this policy with all its contents, in accordance with any changes in the applicable regulations and legislation, where:	تتحمل الإدارة القانونية بالحمادي القابضة وإدارات الأمن السيبراني وتكنولوجيا المعلومات مسؤولية الحفاظ على هذه السياسة بجميع محتوياتها، وفقًا لأي تغييرات في اللوائح والتشريعات المعمول بها، حيث:
101	Translated (100%)	Policy Review and Update:	مراجعة السياسة وتحديثها:
102	Translated (100%)	Cybersecurity Department.	إدارة الأمن السيبراني.
103	Translated (100%)	Policy Implementation and Enforcement:	تنفيذ السياسة وإنفاذها:
104	Translated (0%)	Legal and IT Departments.	الإدارات القانونية وتقنية المعلومات.
105	Translated (100%)	Policy Compliance Measurement:	قياس الامتثال للسياسة:
106	Translated (100%)	Cybersecurity Department.	إدارة الأمن السيبراني.
107	Translated (100%)	Compliance with legal and contractual requirements	الامتثال للمتطلبات القانونية والتعاقدية
108	Translated (0%)	Al Hammadi Holding shall avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.	يجب على شركة الحمادي القابضة تجنب انتهاكات الالتزامات القانونية أو القانونية أو التنظيمية أو التعاقدية المتعلقة بأمن المعلومات وأي متطلبات أمنية.
109	Translated (0%)	Identification of applicable legislation and contractual requirements	تحديد التشريعات المعمول بها والمتطلبات التعاقدية
110	Translated (0%)	Al Hammadi Holding shall explicitly identify all relevant and applicable legislative, statutory, regulatory, and contractual information security	تحدد شركة الحمادي القابضة صراحة جميع متطلبات والتزامات أمن المعلومات التشريعية والقانونية والتنظيمية والتعاقدية ذات الصلة

		requirements and obligations, whether local or international.	.والقابلة للتطبيق، سواء كانت محلية أو دولية
111	Translated (0%)	Al Hammadi Holding Internal Audit functiopn shall document the Legal and Compliance Register (LCR) serves as a centralized repository to document and track all applicable legal, regulatory, and contractual obligations relevant to the organization to ensure that all requirements are clearly understood, assigned, and regularly reviewed, forming a foundational component of the organization's compliance and risk management framework.	يجب على وظيفة التدقيق الداخلي لشركة الحمادي القابضة توثيق سجل كمستودع مركزي لتوثيق وتتبع جميع الالتزامات (LCR) الامتثال القانوني القانونية والتنظيمية والتعاقدية المعمول بها ذات الصلة بالمنظمة لضمان فهم جميع المتطلبات بوضوح وتعيينها ومراجعتها بانتظام، مما يشكل .مكونًا أساسيًا لإطار الامتثال وإدارة المخاطر في المنظمة
112	Translated (0%)	The approach to meet these requirements, the specific controls, and the individual responsibilities, shall be documented and kept up to date.	يجب توثيق النهج المتبع لتلبية هذه المتطلبات والضوابط المحددة .والمسؤوليات الفردية وتحديثه باستمرار
113	Translated (0%)	Ensure compliance with requirements related to cybersecurity through the use of appropriate tools, including but not limited to:	ضمان الامتثال للمتطلبات المتعلقة بالأمن السيبراني من خلال استخدام :الأدوات المناسبة، بما في ذلك على سبيل المثال لا الحصر
114	Translated (0%)	Cybersecurity Risk Assessment activities.	.أنشطة تقييم مخاطر الأمن السيبراني
115	Translated (0%)	Vulnerability Management activities.	.أنشطة إدارة الثغرات الأمنية
116	Translated (0%)	Penetration Test activities.	.أنشطة اختبار الاختراق
117	Translated (0%)	Review of cybersecurity standards.	.مراجعة معايير الأمن السيبراني
118	Translated (0%)	Security Source Code Review.	.مراجعة كود مصدر الأمان
119	Translated (0%)	User surveys.	.استبيانات المستخدمين
120	Translated (0%)	Stakeholder interviews.	.المقابلات مع أصحاب المصلحة
121	Translated (0%)	Review of privileges on the system and network.	.مراجعة الامتيازات على النظام والشبكة
122	Translated (0%)	Review of cybersecurity logs and events.	.مراجعة سجلات وأحداث الأمن السيبراني
123	Translated (0%)	Intellectual property rights	حقوق الملكية الفكرية
124	Translated (0%)	The following guidelines shall be considered by Al Hammadi Holding to protect any material that may be considered intellectual property:	يجب على شركة الحمادي القابضة النظر في الإرشادات التالية لحماية أي :مادة يمكن اعتبارها ملكية فكرية
125	Translated (0%)	acquiring software only through known and reputable sources, to ensure that copyright is not violated.	،الحصول على البرامج فقط من خلال مصادر معروفة وذات سمعة طيبة .لضمان عدم انتهاك حقوق الطبع والنشر
126	Translated (0%)	maintaining awareness of policies to protect intellectual property rights and giving notice of the intent to take disciplinary action against personnel breaching them.	الحفاظ على الوعي بسياسات حماية حقوق الملكية الفكرية وإعطاء إشعار .بنية اتخاذ إجراءات تأديبية ضد الموظفين الذين ينتهكونها

127	Translated (0%)	maintaining appropriate asset registers and identifying all assets with requirements to protect intellectual property rights.	الاحتفاظ بسجلات الأصول المناسبة وتحديد جميع الأصول مع متطلبات لحماية حقوق الملكية الفكرية.
128	Translated (0%)	maintaining proof and evidence of ownership of licenses, master disks, manuals, etc.	الاحتفاظ بإثبات وإثبات ملكية التراخيص والأقراص الرئيسية والأدلة وما إلى ذلك.
129	Translated (0%)	implementing controls to ensure that any maximum number of users permitted within the license is not exceeded.	تنفيذ الضوابط لضمان عدم تجاوز الحد الأقصى لعدد المستخدمين المسموح به في الترخيص.
130	Translated (0%)	carrying out reviews that only authorized software and licensed products are installed.	إجراء مراجعات بحيث يتم تثبيت البرامج المصرح بها والمنتجات المرخصة فقط.
131	Translated (0%)	complying with terms and conditions for software and information obtained from public networks.	الامتثال لشروط وأحكام البرامج والمعلومات التي يتم الحصول عليها من الشبكات العامة.
132	Translated (0%)	not duplicating, converting to another format or extracting from commercial recordings (film, audio) other than permitted by copyright law.	عدم التكرار أو التحويل إلى تنسيق آخر أو الاستخراج من التسجيلات التجارية (فيلم أو صوت) بخلاف ما يسمح به قانون حقوق الطبع والنشر.
133	Translated (0%)	not copying in full or in part, patient records, books, articles, reports or other documents, other than permitted by copyright law.	عدم النسخ الكامل أو الجزئي لسجلات المرضى أو الكتب أو المقالات أو التقارير أو المستندات الأخرى، بخلاف ما يسمح به قانون حقوق الطبع والنشر.
134	Translated (0%)	Protection of records	حماية السجلات
135	Translated (0%)	Al Hammadi Holding records shall be protected from loss, destruction, falsification, unauthorized access, and unauthorized release, in accordance with legislatory, regulatory, contractual, and business requirements.	يجب حماية سجلات شركة الحمادي القابضة من الفقدان والتدمير والتزوير والوصول غير المصرح به والإفراج غير المصرح به، وفقًا للمتطلبات التشريعية والتنظيمية والتعاقدية والتجارية.
136	Translated (0%)	The system of storage and handling shall ensure identification of records and their retention period as defined by applicable national or regional legislation or regulations.	يجب أن يضمن نظام التخزين والمناولة تحديد السجلات وفترة الاحتفاظ بها على النحو المحدد في التشريعات أو اللوائح الوطنية أو الإقليمية المعمول بها.
137	Translated (0%)	Records classification shall conform to their corresponding classification in Al Hammadi Holding’s classification scheme.	يجب أن يتوافق تصنيف السجلات مع تصنيفها المقابل في مخطط تصنيف الحمادي القابضة.
138	Translated (0%)	Details of retention periods and type of allowable storage media shall be defined.	يجب تحديد تفاصيل فترات الاحتفاظ ونوع وسائط التخزين المسموح بها.
139	Translated (0%)	Consideration shall be given to the possibility of deterioration of media used for storage of records.	يجب النظر في إمكانية تدهور الوسائط المستخدمة لتخزين السجلات.
140	Translated (0%)	Storage and handling system shall be implemented in accordance with manufacturer’s recommendations.	يجب تنفيذ نظام التخزين والمناولة وفقًا لتوصيات الشركة المصنعة.
141	Translated (0%)	Ability to access Al Hammadi Holding’s data throughout the retention period shall be safeguarded against loss due to future technology change.	يجب حماية القدرة على الوصول إلى بيانات شركة الحمادي القابضة طوال فترة الاحتفاظ من الخسارة بسبب التغيير التكنولوجي في المستقبل.
142	Translated (0%)	Storage and handling system shall permit appropriate destruction of records after the retention period if not needed by Al Hammadi Holding.	يجب أن يسمح نظام التخزين والمناولة بالتدمير المناسب للسجلات بعد فترة الاحتفاظ إذا لم تكن هناك حاجة إليها من قبل شركة الحمادي القابضة.

143	Translated (0%)	Retention of Records	الاحتفاظ بالسجلات
144	Translated (0%)	Al Hammadi Holding IT must retain records of consent given by data owners and must retain records of withdrawal or revocation of consent for the length of time specified by law or regulation.	يجب أن تحتفظ شركة الحمادي القابضة لتقنية المعلومات بسجلات الموافقة المقدمة من مسؤولي إدارة البيانات ويجب أن تحتفظ بسجلات سحب أو إلغاء الموافقة للمدة الزمنية المحددة بموجب القانون أو اللائحة.
145	Translated (0%)	Al Hammadi Holding Cybersecurity Department and IT Department must keep a record of all secure data disposal operations that have been executed.	يجب على إدارة الأمن السيبراني الحمادي القابضة وإدارة تكنولوجيا المعلومات الاحتفاظ بسجل لجميع عمليات التخلص الآمن من البيانات التي تم تنفيذها.
146	Translated (0%)	Al Hammadi Holding must retain data for the length of time specified by law or regulation or until the sensitive information is no longer required for the purpose for which it was collected.	يجب أن تحتفظ شركة الحمادي القابضة بالبيانات للمدة الزمنية المحددة بموجب القانون أو اللائحة أو حتى تصبح المعلومات الحساسة غير مطلوبة للغرض الذي تم جمعها من أجله.
147	Translated (0%)	Al Hammadi Holding IT must create a record of processing activities, update it when required and retain copies for the length of time specified by law or regulation.	يجب على شركة الحمادي القابضة لتقنية المعلومات إنشاء سجل لأنشطة المعالجة وتحديثه عند الاقتضاء والاحتفاظ بنسخ للمدة الزمنية المحددة بموجب القانون أو اللائحة.
148	Translated (0%)	Identifying retention period for all systems-associated data, in accordance with relevant legislations.	تحديد فترة الاحتفاظ لجميع البيانات المرتبطة بالأنظمة، وفقًا للتشريعات ذات الصلة.
149	Translated (0%)	Only required data must be retained in the production environment.	يجب الاحتفاظ بالبيانات المطلوبة فقط في بيئة الإنتاج.
150	Translated (100%)	Document Type	نوع المستند
151	Translated (100%)	Retention Period	فترة الحفظ
152	Translated (100%)	Hard Copy	نسخة ورقية
153	Translated (100%)	Soft Copy	نسخة إلكترونية
154	Translated (100%)	Request Forms	نماذج الطلب
155	Translated (100%)	HIS Access Request	طلب الوصول إلى نظام معلومات المستشفى
156	Translated (100%)	New Procedure Code Request	طلب رمز إجراء جديد
157	Translated (100%)	Modification of Laboratory/Radiology Reports	تعديل تقارير المختبر/الأشعة
158	Translated (100%)	Report Request	طلب التقرير
159	Translated (100%)	IT Work Request	طلب عمل تكنولوجيا المعلومات
160	Translated	Change Request	طلب تغيير

	(100%)		
161	Translated (100%)	Archive	أرشيف
162	Translated (100%)	Hospital Information System (HIS)	(HIS) نظام معلومات المستشفى
163	Translated (100%)	Archive	أرشيف
164	Translated (100%)	Laboratory Information System (LIS)	(LIS) نظام المعلومات المختبرية
165	Translated (99%)	10 years	سنوات 10
166	Translated (100%)	Picture Archiving and Communication System (PACS)	(PACS) نظام أرشفة الصور والاتصالات
167	Translated (100%)	5 years	سنوات 5
168	Translated (100%)	Financial and Accounting Management System	نظام الإدارة المالية والمحاسبية
169	Translated (100%)	10 years	سنوات 10
170	Translated (100%)	Human Resource Management System (HRMS)	(HRMS) نظام إدارة الموارد البشرية
171	Translated (100%)	10 years	سنوات 10
172	Translated (100%)	Network System and Security Records	نظام الشبكة والسجلات الأمنية
173	Translated (100%)	Archive	أرشيف
174	Translated (100%)	Contracts and Purchasing Records	العقود وسجلات المشتريات
175	Translated (100%)	3 years	سنوات 3
176	Translated (0%)	cybersecurity event logs	سجلات أحداث الأمن السيبراني
177	Translated (0%)	<928>24 </928> Months	شهرًا <928>24 </928>
178	Translated (0%)	<942>Privacy and protection of personally identifiable information</942>, PII	PII ،<942>الخصوصية وحماية معلومات التعريف الشخصية942/></942>
179	Translated (0%)	Privacy and protection of Al Hammadi Holding's PII shall be safeguarded in relevance to Al Hammadi Holding applicable legislations and	يجب حماية خصوصية وحماية معلومات تحديد الهوية الشخصية لشركة الحمادي القابضة فيما يتعلق بالتشريعات واللوائح المعمول بها في شركة

		regulations.	.الحمادي القابضة
180	Translated (0%)	Compliance with this policy and all relevant legislation and regulations concerning the protection of the privacy of people and the protection of PII is the responsibility of Al Hammadi Holding senior management.	تقع مسؤولية الامتثال لهذه السياسة وجميع التشريعات واللوائح ذات الصلة المتعلقة بحماية خصوصية الأشخاص وحماية معلومات تحديد .الهوية الشخصية على عاتق الإدارة العليا لشركة الحمادي القابضة
181	Translated (0%)	Al Hammadi Holding adheres to the following core privacy principles:	:تلتزم شركة الحمادي القابضة بمبادئ الخصوصية الأساسية التالية
182	Translated (0%)	Lawful and Fair Processing:	:المعالجة القانونية والعادلة
183	Translated (0%)	Personal data must be collected and processed fairly and only for lawful and specified purposes.	يجب جمع البيانات الشخصية ومعالجتها بشكل عادل وفقط لأغراض .قانونية ومحددة
184	Translated (0%)	Purpose Limitation:	:تحديد الغرض
185	Translated (0%)	Data must only be used for the purposes stated at the time of collection.	.يجب استخدام البيانات فقط للأغراض المذكورة في وقت الجمع
186	Translated (0%)	Data Minimization:	:تقليل البيانات إلى الحد الأدنى
187	Translated (0%)	Only the minimum necessary data will be collected and processed.	.سيتم جمع ومعالجة الحد الأدنى من البيانات اللازمة فقط
188	Translated (100%)	Accuracy:	:الدقة
189	Translated (0%)	Reasonable steps must be taken to ensure data is accurate and up to date.	.يجب اتخاذ خطوات معقولة لضمان دقة البيانات وتحديثها
190	Translated (0%)	Storage Limitation:	:قيود التخزين
191	Translated (0%)	Data shall be retained only for as long as necessary.	.يجب الاحتفاظ بالبيانات فقط طالما كان ذلك ضروريًا
192	Translated (0%)	Integrity and Confidentiality:	:النزاهة والسرية
193	Translated (0%)	Data must be protected against unauthorized access, disclosure, alteration, and destruction.	يجب حماية البيانات من الوصول غير المصرح به والإفصاح والتغيير .والتدمير
194	Translated (0%)	Accountability:	:المساءلة
195	Translated (0%)	The organization must demonstrate compliance with privacy obligation	يجب على المنظمة إثبات الامتثال لالتزام الخصوصية
196	Translated (0%)	Personal and sensitive data must be classified as Restricted or Confidential.	.يجب تصنيف البيانات الشخصية والحساسة على أنها مقيدة أو سرية
197	Translated (0%)	Al Hammadi Holding should appoint a responsible person as a privacy officer.	يجب على شركة الحمادي القابضة تعيين شخص مسؤول كمسؤول عن .الخصوصية
198	Translated	Al Hammadi Holding privacy officer should provide guidance to managers,	يجب على مسؤول الخصوصية في شركة الحمادي القابضة تقديم

	(0%)	users, and service providers on their individual responsibilities and the specific procedures that shall be followed.	التوجيه للمديرين والمستخدمين ومقدمي الخدمات بشأن مسؤولياتهم الفردية والإجراءات المحددة التي يجب اتباعها.
199	Translated (0%)	Al Hammadi Holding privacy officer should implement appropriate technical and organizational measures to protect Al Hammadi Holding's PII.	يجب على مسؤول الخصوصية في شركة الحمادي القابضة تنفيذ التدابير الفنية والتنظيمية المناسبة لحماية معلومات تحديد الهوية الشخصية الخاصة بشركة الحمادي القابضة.
200	Translated (0%)	Al Hammadi Holding must consider privacy at the initial design stages and throughout the complete development process of new systems, applications, databases, products, processes, or services that involve processing personally identifying information (PII).	يجب على شركة الحمادي القابضة مراعاة الخصوصية في مراحل التصميم الأولية وطوال عملية التطوير الكاملة للأنظمة أو التطبيقات أو قواعد البيانات أو المنتجات أو العمليات أو الخدمات الجديدة التي تنطوي على معالجة معلومات التعريف الشخصية (PII).
201	Translated (0%)	Privacy by Design must be embedded into the design and architecture of IT systems processing personally identifying information (PII) to ensure that current, new or changes to the systems that collect, or process personally identifying information (PII) satisfy requirements.	يجب تضمين الخصوصية حسب التصميم في تصميم وبنية أنظمة تكنولوجيا المعلومات التي تعالج معلومات التعريف الشخصية (PII) للتأكد من أن الأنظمة الحالية أو الجديدة أو التغييرات التي تطرأ على الأنظمة التي تجمع أو تعالج معلومات التعريف الشخصية (PII) تفي بالمتطلبات.
202	Translated (0%)	When applicable, Al Hammadi Holding IT must apply suitable data pseudonymization / anonymization techniques to meet the requirements of Privacy by Design principle.	عند الاقتضاء، يجب على شركة الحمادي القابضة لتقنية المعلومات تطبيق تقنيات مناسبة لإخفاء الهوية / إخفاء الهوية لتلبية متطلبات مبدأ الخصوصية حسب التصميم.
203	Translated (0%)	The default system settings must be the most privacy friendly (data minimization principle), if a system or service includes choices for data subjects on how much personally identifying information (PII) is shared.	يجب أن تكون إعدادات النظام الافتراضية هي الأكثر ملاءمة للخصوصية إذا كان النظام أو الخدمة تتضمن خيارات ،(مبدأ تقليل البيانات) التي (PII) لموضوعات البيانات حول مقدار معلومات التعريف الشخصية تتم مشاركتها.
204	Translated (0%)	Al Hammadi Holding IT must implement least privilege access and multi-factor authentication.	يجب على شركة الحمادي القابضة لتقنية المعلومات تنفيذ الحد الأدنى من الوصول إلى الامتيازات والمصادقة متعددة العوامل.
205	Translated (0%)	All access to personal data must be logged and regularly reviewed.	يجب تسجيل جميع عمليات الوصول إلى البيانات الشخصية ومراجعتها بانتظام.
206	Translated (0%)	Al Hammadi Holding IT must put appropriate technical and organizational measures in place to ensure, that only necessary personally identifying information (PII) are processed by default.	يجب على شركة الحمادي القابضة لتقنية المعلومات وضع التدابير الفنية والتنظيمية المناسبة لضمان معالجة معلومات التعريف الشخصية الضرورية فقط بشكل افتراضي.
207	Translated (0%)	Personal data must not be transferred outside Saudi Arabia without compliance with NDMO cross-border data transfer rules.	يجب عدم نقل البيانات الشخصية خارج المملكة العربية السعودية دون الامتثال لقواعد نقل البيانات عبر الحدود الصادرة عن المكتب الوطني لإدارة البيانات.
208	Translated (0%)	Any data breach involving personal data must be reported within 72 hours and investigated with documented outcomes.	يجب الإبلاغ عن أي خرق للبيانات يتضمن بيانات شخصية في غضون 72 ساعة والتحقيق فيه بنتائج موثقة.
209	Translated (0%)	Regulation of cryptographic controls	تنظيم ضوابط التشفير
210	Translated (0%)	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	يجب استخدام ضوابط التشفير وفقًا لجميع الاتفاقيات والتشريعات واللوائح ذات الصلة.
211	Translated (0%)	The following items shall be considered for compliance with the relevant agreements, laws and regulations:	يجب النظر في البنود التالية للامتثال للاتفاقيات والقوانين واللوائح ذات الصلة:

212	Translated (0%)	restrictions on import or export of computer hardware and software for performing cryptographic functions.	القيود المفروضة على استيراد أو تصدير أجهزة وبرامج الكمبيوتر لأداء وظائف التشفير.
213	Translated (0%)	restrictions on import or export of computer hardware and software which is designed to have cryptographic functions added to it.	القيود المفروضة على استيراد أو تصدير أجهزة وبرامج الكمبيوتر المصممة لإضافة وظائف التشفير إليها.
214	Translated (0%)	restrictions on the usage of encryption.	قيود على استخدام التشفير.
215	Translated (0%)	mandatory or discretionary methods of access by the Saudi's authorities to information encrypted by hardware or software to provide confidentiality of content.	الطرق الإلزامية أو التقديرية للوصول من قبل السلطات السعودية إلى المعلومات المشفرة بواسطة الأجهزة أو البرامج لتوفير سرية المحتوى.
216	Translated (0%)	Before encrypted information or cryptographic controls are moved across Saudi jurisdictional borders, legal advice shall be taken.	قبل نقل المعلومات المشفرة أو ضوابط التشفير عبر الحدود القضائية السعودية، يجب أخذ المشورة القانونية.
217	Translated (0%)	Al Hammadi Holding's related cryptographic keys and programs associated with encrypted records' archives or digital signatures, shall be stored to enable decryption of the records for the length of time they are retained.	يجب تخزين مفاتيح وبرامج التشفير ذات الصلة بشركة الحمادي القابضة المرتبطة بأرشيفات السجلات المشفرة أو التوقيعات الرقمية لتمكين فك تشفير السجلات طوال فترة الاحتفاظ بها.
218	Translated (100%)	Information security reviews	مراجعات أمن المعلومات
219	Translated (0%)	Independent review of information security	المراجعة المستقلة لأمن المعلومات
220	Translated (0%)	Al Hammadi Holding's information security and its implementation (i.e., control objectives, controls, policies, processes and procedures for information security) shall be audited independently taking into account the principle of non-conflict of interests, as per the general standards accepted for review and auditing as well as the relevant legal and regulatory requirements, this audit shall be done at planned intervals or when significant changes occur.	يجب تدقيق أمن معلومات شركة الحمادي القابضة وتنفيذه (أي أهداف الرقابة والضوابط والسياسات والعمليات والإجراءات الخاصة بأمن المعلومات) بشكل مستقل مع مراعاة مبدأ عدم تضارب المصالح، وفقًا للمعايير العامة المقبولة للمراجعة والتدقيق بالإضافة إلى المتطلبات القانونية والتنظيمية ذات الصلة، يجب أن يتم هذا التدقيق على فترات مخططة أو عند حدوث تغييرات كبيرة.
221	Translated (0%)	Al Hammadi Holding's independent reviews shall ensure the continuing suitability, adequacy and effectiveness of Al Hammadi Holding's approach to managing information security.	يجب أن تضمن المراجعات المستقلة لشركة الحمادي القابضة استمرار ملاءمة وكفاية وفعالية نهج شركة الحمادي القابضة لإدارة أمن المعلومات.
222	Translated (0%)	A periodic audit of the Information security practices and processes shall be conducted to determine whether the control objectives, processes and procedures of the Cybersecurity team:	يجب إجراء تدقيق دوري لممارسات وعمليات أمن المعلومات لتحديد ما إذا كانت أهداف وعمليات وإجراءات الرقابة لفريق الأمن السيبراني:
223	Translated (0%)	meet the requirements of applicable standards and industry fit practices to meet regulatory, legislative and contractual requirements	تلبية متطلبات المعايير المعمول بها والممارسات الملائمة للصناعة لتلبية المتطلبات التنظيمية والتشريعية والتعاقدية
224	Translated (100%)	meet the Information Security requirements defined in the Information Security policy and associated policies.	تلبية متطلبات أمن المعلومات المحددة في سياسة أمن المعلومات والسياسات ذات الصلة.
225	Translated (100%)	are effectively implemented and maintained as designed.	تُنفذ وتُحفظ بالكامل كما هو مخطط لها.
226	Translated	The reviews shall include assessing opportunities for improvement and	يجب أن تتضمن المراجعات تقييم فرص التحسين والحاجة إلى تغييرات

	(0%)	the need for changes to the approach to security, including the policy and control objectives.	.في نهج الأمن، بما في ذلك أهداف السياسة والرقابة
227	Translated (0%)	Al Hammadi Holding's independent reviews shall be carried out by individuals independent of the area under review, e.g., the internal audit function or an external party organization.	يجب إجراء المراجعات المستقلة لشركة الحمادي القابضة من قبل أفراد مستقلين عن المنطقة قيد المراجعة، على سبيل المثال، وظيفة التدقيق .الداخلي أو منظمة طرف خارجي
228	Translated (0%)	Individuals carrying out reviews shall have the appropriate skills and experience.	يجب أن يتمتع الأفراد الذين يجرون المراجعات بالمهارات والخبرات .المناسبة
229	Translated (0%)	Results from the cybersecurity audits and reviews must be documented and presented to the cybersecurity steering committee and Authorizing Official.	يجب توثيق نتائج عمليات تدقيق ومراجعات الأمن السيبراني وتقديمها .إلى اللجنة التوجيهية للأمن السيبراني والمسؤول المفوض
230	Translated (0%)	Results must include the audit/review scope, observations, recommendations and remediation plans.	يجب أن تتضمن النتائج نطاق التدقيق/المراجعة والملاحظات والتوصيات .وخطط الإصلاح
231	Translated (0%)	Al Hammadi Holding shall conduct management review meetings, appoint suitable staff to find out the root cause of the resulting Non-Conformities, and approve an action plan to implement corrective actions.	تقوم شركة الحمادي القابضة بعقد اجتماعات مراجعة الإدارة، وتعيين ،الموظفين المناسبين لمعرفة السبب الجذري لعدم المطابقة الناتج .والموافقة على خطة عمل لتنفيذ الإجراءات التصحيحية
232	Translated (0%)	Compliance with security policies and standards	الامتثال للسياسات والمعايير الأمنية
233	Translated (0%)	Al Hammadi Holding shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	تقوم شركة الحمادي القابضة بمراجعة منتظمة لامتثال معالجة المعلومات والإجراءات داخل منطقة مسؤوليتها مع السياسات والمعايير .الأمنية المناسبة وأي متطلبات أمنية أخرى
234	Translated (0%)	Cybersecurity reviews must be conducted periodically by the cybersecurity function in the organization to assess the compliance with the cybersecurity controls in the organization.	يجب إجراء مراجعات الأمن السيبراني بشكل دوري من قبل قسم الأمن السيبراني في المؤسسة لتقييم الامتثال لضوابط الأمن السيبراني في .المؤسسة
235	Translated (0%)	Al Hammadi Holding shall identify automatic measurement and reporting tools for efficient regular reviews.	يجب على شركة الحمادي القابضة تحديد أدوات القياس والإبلاغ .التلقائية لإجراء مراجعات منتظمة فعالة
236	Translated (0%)	Al Hammadi Holding's information systems shall be reviewed immediately following any implementation of a new system or a change to existing one to verify that they are compliant with Information Security Standards.	يجب مراجعة أنظمة معلومات شركة الحمادي القابضة فورًا بعد أي تنفيذ لنظام جديد أو تغيير في النظام الحالي للتحقق من امتثالها لمعايير .أمن المعلومات
237	Translated (0%)	If any non-compliance is found as a result of the review, managers or Head of Departments shall:	في حالة اكتشاف أي عدم امتثال نتيجة للمراجعة، يجب على المديرين أو :رؤساء الإدارات
238	Translated (0%)	identify the causes of the non-compliance.	.تحديد أسباب عدم الامتثال
239	Translated (0%)	evaluate the need for actions to achieve compliance.	.تقييم الحاجة إلى اتخاذ إجراءات لتحقيق الامتثال
240	Translated (0%)	implement appropriate corrective action.	.تنفيذ الإجراءات التصحيحية المناسبة
241	Translated (0%)	review the corrective action taken to verify its effectiveness and identify any deficiencies or weaknesses.	مراجعة الإجراءات التصحيحية المتخذة للتحقق من فعاليتها وتحديد أي .أوجه قصور أو ضعف

242	Translated (0%)	Results of the compliance reviews and corrective actions carried out by Al Hammadi Holding shall be recorded and these records shall be maintained.	يجب تسجيل نتائج مراجعات الامتثال والإجراءات التصحيحية التي تقوم بها شركة الحمادي القابضة والاحتفاظ بهذه السجلات.
243	Translated (0%)	Managers or Head of Departments shall report the compliance reviews results to the persons carrying out independent reviews when they take place in the area of their responsibility.	يجب على المديرين أو رؤساء الإدارات إبلاغ الأشخاص الذين يجرون مراجعات مستقلة بنتائج مراجعات الامتثال عند إجرائها في منطقة مسؤوليتهم.
244	Translated (0%)	Technical compliance review	مراجعة الامتثال الفني
245	Translated (0%)	Technical compliance shall be reviewed with the assistance of automated tools, which generate technical reports for subsequent interpretation by a technical specialist.	يجب مراجعة الامتثال الفني بمساعدة الأدوات الآلية، التي تنتج تقارير فنية للتفسير اللاحق من قبل أخصائي فني.
246	Translated (0%)	Penetration tests and vulnerability assessments shall be cautiously conducted and exercised in such secure manner not to lead to a compromise of the security of the tested systems.	يجب إجراء اختبارات الاختراق وتقييمات الضعف بحذر وممارستها بطريقة آمنة لا تؤدي إلى المساس بأمن الأنظمة التي تم اختبارها.
247	Translated (0%)	Technical compliance assessments shall be planned and documented.	يجب تخطيط وتوثيق تقييمات الامتثال الفني.
248	Translated (0%)	Al Hammadi Holding's technical compliance review shall only be carried out by competent, authorized persons and under the supervision of Al Hammadi Holding's management.	لا يجوز إجراء مراجعة الامتثال الفني لشركة الحمادي القابضة إلا من قبل أشخاص مختصين ومصرح لهم وتحت إشراف إدارة شركة الحمادي القابضة.
249	Translated (0%)	<1253>Whilst such a compliance review shall be performed by appropriately qualified personnel, there shall be adequate segregation of duties between the personnel performing System Administrators', System Operators', OT Admins, and System Auditors' functions within Al Hammadi Holding's.</1253><1263/><1264/><1265/><1266/><1269> Regulatory Communication & Reporting</1269>	في حين يجب إجراء مراجعة الامتثال هذه من قبل موظفين<1253> مؤهلين بشكل مناسب، يجب أن يكون هناك فصل كافٍ للواجبات بين الموظفين الذين يؤدون وظائف مسؤولي النظام ومشغلي النظام ومسؤولي التكنولوجيا التشغيلية ومراجعي النظام داخل شركة الحمادي القابضة.</1253><1263/><1264></1265></1266></1269> <الاتصالات التنظيمية وإعداد التقارير</1269>
250	Translated (0%)	Effective communication with regulators is critical during routine operations and especially during disruptive events.	يعد التواصل الفعال مع المنظمين أمرًا بالغ الأهمية أثناء العمليات الروتينية وخاصة أثناء الأحداث التخريبية.
251	Translated (0%)	Al Hammadi Holding maintains a structured approach to regulatory engagement to ensure transparency, timely reporting, and continued compliance with applicable legal and regulatory obligations.	تحافظ شركة الحمادي القابضة على نهج منظم للمشاركة التنظيمية لضمان الشفافية والإبلاغ في الوقت المناسب والامتثال المستمر للالتزامات القانونية والتنظيمية المعمول بها.
252	Translated (0%)	Identification of Regulatory Bodies:	تحديد الجهات الرقابية:
253	Translated (0%)	A register of all relevant regulators (e.g., financial, health, data protection, environmental) must be maintained and reviewed annually.	يجب الاحتفاظ بسجل لجميع الجهات التنظيمية ذات الصلة (على سبيل المثال، المالية والصحية وحماية البيانات والبيئية) ومراجعته سنويًا.
254	Translated (0%)	Official Communication Channels:	قنوات الاتصال الرسمية:
255	Translated (0%)	Each regulator's preferred method of communication (email, portal, phone, in-person) must be documented and followed.	يجب توثيق واتباع طريقة الاتصال المفضلة لكل جهة تنظيمية (البريد الإلكتروني، البوابة، الهاتف، الحضور الشخصي).
256	Translated	Relationship Management:	إدارة العلاقات:

	(0%)		
257	Translated (0%)	Designated Compliance or Legal Officers are responsible for maintaining ongoing, proactive engagement with key regulatory contacts.	مسؤولو الامتثال أو الموظفون القانونيون المعينون مسؤولون عن الحفاظ على المشاركة المستمرة والاستباقية مع جهات الاتصال التنظيمية الرئيسية.
258	Translated (0%)	Each regulation or jurisdiction may impose specific deadlines for notification and reporting.	قد تفرض كل لائحة أو ولاية قضائية مواعيد نهائية محددة للإخطار والإبلاغ.
259	Translated (0%)	Al Hammadi Holding must comply with the strictest applicable standard. including:	يجب أن تمتثل شركة الحمادي القابضة لأدق المعايير المعمول بها. بما في ذلك:
260	Translated (0%)	Incident Type	نوع البلاغ
261	Translated (0%)	Regulatory Body	الهيئة التنظيمية
262	Translated (0%)	Notification Timeline	الجدول الزمني للإشعار
263	Translated (0%)	Notification methos	إخطار بالميثوس
264	Translated (0%)	Notification Responsibility	مسؤولية الإخطار
265	Translated (0%)	Data Breach (PII)	(PII) خرق البيانات
266	Translated (0%)	Data Protection Authority	هيئة حماية البيانات
267	Translated (0%)	Within 72 hours of detection	في غضون 72 ساعة من الكشف
268	Translated (0%)	Official Communication Channels	قنوات الاتصال الرسمية
269	Translated (0%)	Data Privacy in charge	خصوصية البيانات المسؤولة
270	Translated (0%)	Cybersecurity Incident	حادث الأمن السيبراني
271	Translated (0%)	NCA	المركز الوطني للقياس
272	Translated (0%)	As soon as possible within 72 hours	في أقرب وقت ممكن في غضون 72 ساعة
273	Translated (100%)	Official Communication Channels	قنوات الاتصال الرسمية
274	Translated (100%)	Cybersecurity Manager	مدير الأمن السيبراني
275	Translated	Failure to meet timelines must be escalated and documented to the	يجب تصعيد الفشل في الالتزام بالجداول الزمنية وتوثيقه للإدارة من قبل

	(0%)	management by the responsible perosn.	.الشخص المسؤول
276	Translated (0%)	Escalation Procedure	إجراء التصعيد
277	Translated (0%)	Incident Detection:	:الكشف عن الحوادث
278	Translated (0%)	The relevant business unit or system detects a potential regulatory event.	.تكتشف وحدة أو نظام الأعمال ذات الصلة حدثًا تنظيميًا محتملًا
279	Translated (0%)	Initial Triage:	:الفرز الأولي
280	Translated (0%)	Incident is logged, and initial assessment is made by Risk/Compliance team.	يتم تسجيل الحادث، ويتم إجراء التقييم الأولي من قبل فريق .المخاطر/الامتثال
281	Translated (0%)	Escalation to Senior Management:	:التصعيد إلى الإدارة العليا
282	Translated (0%)	If regulatory notification is likely required.	.إذا كان من المحتمل أن يكون الإخطار التنظيمي مطلوبًا
283	Translated (0%)	If reputational or financial impact exceeds threshold.	.إذا تجاوز التأثير على السمعة أو التأثير المالي العتبة
284	Translated (0%)	Executive Approval:	:الموافقة التنفيذية
285	Translated (0%)	Final submission is reviewed by CEO, Compliance Officer, or authorized delegate.	تتم مراجعة التقديم النهائي من قبل الرئيس التنفيذي أو مسؤول الامتثال .أو المندوب المفوض
286	Translated (0%)	Regulator Notification:	:إشعار الجهة التنظيمية
287	Translated (0%)	Sent via the prescribed method and tracked in the Regulatory Engagement Log.	.يتم إرسالها عبر الطريقة المحددة وتتبعها في سجل المشاركة التنظيمية
288	Translated (100%)	Compliance and Adherence	الامتثال والالتزام
289	Translated (100%)	Al Hammadi Holding CEO shall ensure compliance with the cybersecurity policies and standards.	يضمن الرئيس التنفيذي لشركة الحمادي القابضة الامتثال لسياسات .ومعايير الأمن السيبراني
290	Translated (100%)	To ensure compliance, the Cybersecurity department will establish regular reporting by the Cybersecurity Manager, conduct periodic audits, or form a Cybersecurity Steering Committee for oversight.	لضمان الامتثال، سينشئ قسم الأمن السيبراني نظامًا لتقديم تقارير منتظمة يُعدّها مدير الأمن السيبراني، ويجري عمليات تدقيق دورية، أو .يشكل لجنة توجيهية للأمن السيبراني للإشراف
291	Translated (100%)	The CS manager shall ensure adherence to this policy.	.يتعين على مدير الأمن السيبراني ضمان الالتزام بهذه السياسة
292	Translated (100%)	All employees of Al Hammadi Holding must adhere to this policy.	.على جميع موظفي شركة الحمادي القابضة الالتزام بهذه السياسة
293	Translated (100%)	Violations of this policy may result in legal action in any jurisdiction or other measures as deemed appropriate by the Al Hammadi Holding.	قد تؤدي انتهاكات هذه السياسة إلى اتخاذ إجراءات قانونية في أي ولاية .قضائية أو غيرها من التدابير التي تراها شركة الحمادي القابضة مناسبة
294	Translated	Exceptions	الاستثناءات

	(100%)		
295	Translated (100%)	Violation of cybersecurity policies and standards is prohibited unless a prior justified exception is obtained from the Cybersecurity Department or the Cybersecurity Steering Committee.	يُحظر انتهاك سياسات ومعايير الأمن السيبراني ما لم يتم الحصول على استثناء مبرر مسبق من إدارة الأمن السيبراني أو اللجنة التوجيهية للأمن السيبراني.
296	Translated (100%)	In case of a conflict, applicable legislative and regulatory requirements overrule Al Hammadi Holding policies and standards.	في حالة وجود تعارض، فإن المتطلبات التشريعية والتنظيمية المعمول بها تسود على سياسات ومعايير شركة الحمادي القابضة.
297	Translated (100%)	Revision	المراجعة
298	Translated (100%)	This policy is reviewed annually, or after major changes in Al Hammadi Holding's organizational chart or infrastructure, and more frequently whenever required, to ensure it remains appropriate and current for Al Hammadi Holding, ISO 27001, and NCA requirements.	تخضع هذه السياسة لمراجعة سنوية، أو لإعادة التقييم بعد أي تغييرات جوهرية في الهيكل التنظيمي أو البنية التحتية لشركة الحمادي القابضة، إضافة إلى مراجعات دورية إضافية عند الضرورة، وذلك لضمان توافقها المستمر مع متطلبات شركة الحمادي القابضة، ومعيار آيزو ISO 27001:2022، وإرشادات الهيئة الوطنية للأمن السيبراني.
299	Translated (100%)	Approval Section	قسم الاعتماد
300	Translated (100%)	Prepared by:	إعداد:
301	Translated (100%)	Mr. Mohammed Alamer	السيد/ محمد العامر
302	Translated (100%)	GRC Cybersecurity Specialist	أخصائي حوكمة ومخاطر وامتثال في الأمن السيبراني
303	Translated (100%)	Name	الاسم
304	Translated (100%)	Designation	المسمى الوظيفي
305	Translated (100%)	Signature	التوقيع
306	Translated (100%)	Date	التاريخ
307	Translated (100%)	Reviewed by:	راجعها:
308	Translated (0%)	Mr. WAHID RAAFAT	السيد وحيد رأفت
309	Translated (100%)	Chief Audit Executive	المدير التنفيذي لعمليات التدقيق
310	Translated (100%)	Name	الاسم
311	Translated (100%)	Designation	المسمى الوظيفي

312	Translated (100%)	Signature	التوقيع
313	Translated (100%)	Date	التاريخ
314	Translated (100%)	Reviewed by:	:راجعها
315	Translated (100%)	Ms. Mashael Alotaibi	السيدة/ مشاعل العتيبي
316	Translated (100%)	Cybersecurity Manager	مدير الأمن السيبراني
317	Translated (100%)	Name	الاسم
318	Translated (100%)	Designation	المسمى الوظيفي
319	Translated (100%)	Signature	التوقيع
320	Translated (100%)	Date	التاريخ
321	Translated (100%)	Approved by:	:اعتمدها
322	Translated (100%)	Dr. Abdulaziz Al Hammadi	الحمادي<Bold><Bold></Bold></Bold> د./ عبد العزيز<Bold><Bold></Bold></Bold>
323	Translated (100%)	Chief Operating Officer	الرئيس التنفيذي للعمليات
324	Translated (100%)	Name	الاسم
325	Translated (100%)	Designation	المسمى الوظيفي
326	Translated (100%)	Signature	التوقيع
327	Translated (100%)	Date	التاريخ
328	Translated (100%)	Approved by:	:اعتمدها
329	Translated (100%)	Mr. Mohammad Al Hammadi	السيد/ محمد الحمادي
330	Translated (100%)	Chief Executive Officer	الرئيس التنفيذي
331	Translated	Name	الاسم

	(100%)		
332	Translated (100%)	Designation	المسمى الوظيفي
333	Translated (100%)	Signature	التوقيع
334	Translated (100%)	Date	التاريخ

Segment ID	Segment status	Source segment	Target segment
1	Translated (0%)	Information Security Supplier Relationship Policy	سياسة العلاقة مع الموردين في مجال أمن المعلومات
2	Translated (100%)	Page <45><36/> of <44/></45>	صفحة <45></36> من <44/></45>
3	Translated (100%)	Al Hammadi Holding	شركة الحمادي القابضة
4	Translated (100%)	Information Security Supplier Relationship Policy	سياسة العلاقة مع الموردين في مجال أمن المعلومات
5	Translated (100%)	CYBERSECURITY DEPARTMENT	إدارة الأمن السيبراني
6	Translated (100%)	Policy ID	معرّف السياسة
7	Translated (100%)	AHH-CS-ISMS-012	AHH-CS-ISMS-012
8	Translated (100%)	Class	الفئة
9	Translated (100%)	Internal Release	إصدار داخلي
10	Not Translated (0%)		
11	Translated (100%)	V3.1	V3.1
12	Translated (100%)	Published at	نُشرت في
13	Translated (100%)	April 2025	أبريل 2025
14	Translated (100%)	Document Owner	المسؤول عن المستند
15	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
16	Translated (100%)	Disclaimer	تنويه
17	Translated (100%)	The information contained in this document is property of Al Hammadi Holding and must not be copied or communicated to a third party or used for any purpose other than that for which it is supplied, without the written consent of Al Hammadi Holding.	المعلومات الواردة في هذا المستند هي ملك لشركة الحمادي القابضة ولا يجوز نسخها أو إبلاغها إلى طرف ثالث أو استخدامها لأي غرض آخر غير الغرض الذي تم توفيرها من أجله، دون موافقة خطية من شركة الحمادي القابضة.

18	Translated (99%)	Table of Contents	جدول المُحتويات
19	Translated (100%)	Document Control	ضبط المستندات
20	Translated (100%)	Document Information	معلومات المستند
21	Translated (100%)	Synopsis	الملخص
22	Translated (100%)	Document Title:	:عنوان المستند
23	Translated (100%)	Information Security Supplier Relationship Policy	سياسة العلاقة مع الموردين في مجال أمن المعلومات
24	Translated (100%)	Document Status:	:حالة المستند
25	Translated (100%)	Approved	معتمد
26	Translated (100%)	Document Effective Date:	:تاريخ سريان المستند
27	Translated (100%)	December 2024	ديسمبر 2024
28	Translated (100%)	Document Issue Date:	:تاريخ إصدار المستند
29	Translated (100%)	April 2025	أبريل 2025
30	Translated (100%)	Document Next Revision Date:	:تاريخ المراجعة التالية للمستند
31	Translated (100%)	April 2026	أبريل 2026
32	Translated (100%)	Key contacts	جهات التواصل الرئيسية
33	Translated (100%)	Document Owner:	:المسؤول عن المستند
34	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
35	Translated (100%)	Approval Authority	جهة الاعتماد
36	Translated (100%)	Document Created by:	:مُنشئ المستند
37	Translated	IT Management	إدارة تكنولوجيا المعلومات

	(100%)		
38	Translated (100%)	Document Reviewed by:	:راجع المستند
39	Translated (0%)	Al Hammadi Holding CS& IT Managers	مديرو تكنولوجيا المعلومات والخدمات في شركة الحمادي القابضة
40	Translated (100%)	Document Approved by:	:اعتمد المستند
41	Translated (100%)	Al Hammadi Holding COO & CEO	الرئيس التنفيذي للعمليات والرئيس التنفيذي في شركة الحمادي القابضة
42	Translated (100%)	Note:	:ملاحظة
43	Translated (100%)	Any additional approval will be added in the document annex	تُضاف أي اعتمادات إضافية في ملحق المستند
44	Translated (100%)	Classification	التصنيف
45	Translated (100%)	Company Internal – to be shared with 3rd parties after consent of CS Manager	داخلي لاستخدام للشركة – يُسمح بمشاركته مع جهات خارجية بعد موافقة مدير إدارة الأمن السيبراني
46	Translated (100%)	Version / Dates	الإصدار / التواريخ
47	Translated (100%)	Current Version:	:الإصدار الحالي
48	Translated (100%)	V 3.1	V 3.1
49	Translated (100%)	Date Published:	:تاريخ النشر
50	Translated (100%)	April 2025	أبريل 2025
51	Translated (100%)	Date of Next Review:	:تاريخ المراجعة التالية
52	Translated (100%)	April 2026	أبريل 2026
53	Translated (100%)	Prior Version:	:الإصدار السابق
54	Translated (0%)	V <402>3</402>.0	<402></402>V3.0
55	Translated (0%)	<408>Prior Published</408>:	:<تاريخ النشر السابق408/><408>
56	Translated (100%)	December 2023	ديسمبر 2023

57	Translated (100%)	Document Changes	التغييرات على المستند
58	Translated (100%)	Date	التاريخ
59	Translated (100%)	Version	الإصدار
60	Translated (100%)	Document Owner	المسؤول عن المستند
61	Translated (100%)	Change Description	وصف التغيير
62	Translated (0%)	December <448>2024</448>	<448>ديسمبر <448/>2024
63	Translated (100%)	3.0	3.0
64	Translated (100%)	IT Management	إدارة تكنولوجيا المعلومات
65	Translated (100%)	Updated policy number to	تحديث رقم السياسة إلى
66	Translated (100%)	AHH-IT-ISMS-012	AHH-IT-ISMS-012
67	Translated (100%)	April <472>2025</472>	<472>أبريل <472/>2025
68	Translated (100%)	3.1	3.1
69	Translated (100%)	CS Management	(CS) إدارة كائنات نهج المجموعة
70	Translated (100%)	Document reviewed and updated based on NCA ECC-2:2024 and ISO27001:2022 requirements	تمت مراجعة المستند وتحديثه استنادًا إلى متطلبات الهيئة الوطنية للأمن السيبراني (NCA) المعيار ECC-2:2024 ومعيار آيزو ISO 27001:2022.
71	Translated (100%)	Document Circulation	تعميم المستند
72	Translated (100%)	To	إلى
73	Translated (100%)	Method	الطريقة
74	Translated (100%)	IT Staff	موظفو تكنولوجيا المعلومات
75	Translated (0%)	Email/ Intranet Portal	بوابة البريد الإلكتروني/ الإنترانت
76	Translated	Objectives	الأهداف

	(100%)		
77	Translated (0%)	The purpose of this policy is to set the principles and procedural implementation guidelines, by which Al Hammadi Holding shall ensure protection of its information assets accessible, stored, transferred, or processed by suppliers, in compliance with the requirements specified in:	الغرض من هذه السياسة هو وضع المبادئ وإرشادات التنفيذ الإجرائية، والتي بموجبها تضمن شركة الحمادي القابضة حماية أصول المعلومات الخاصة بها التي يمكن الوصول إليها أو تخزينها أو نقلها أو معالجتها من قبل الموردين، وفقًا للمتطلبات المحددة في:
78	Translated (0%)	ISO/IEC 27001:2022 Annex-A :	الملحق أ ISO/IEC 27001:2022 :
79	Translated (0%)	A.5.19 Information security in supplier relationships, A.5.20 Addressing information security within supplier agreements, A.5.21 Managing information security in the ICT supply chain, A.5.22 Monitoring, review and change management of supplier services, A.5.23 Information security for use of cloud services	أ .5.19 أمن المعلومات في علاقات الموردين، أ .5.20 معالجة أمن المعلومات ضمن اتفاقيات الموردين، أ .5.21 إدارة أمن المعلومات في سلسلة توريد تكنولوجيا المعلومات والاتصالات، أ .5.22 مراقبة ومراجعة وإدارة تغيير خدمات الموردين، أ .5.23 أمن المعلومات لاستخدام الخدمات السحابية
80	Translated (100%)	NCA ECC-2:2024:	ECC-2:2024: معيار الهيئة الوطنية للأمن السيبراني رقم
81	Translated (0%)	4-1 Third-Party Cybersecurity	الأمن السيبراني للطرف الثالث 4-1
82	Translated (100%)	Scope	النطاق
83	Translated (0%)	This policy is applicable to all Al Hammadi Holding ISMS information assets, Healthcare, security operations, and all persons doing work under Al Hammadi Holding control.	تنطبق هذه السياسة على جميع أصول معلومات نظام إدارة أمن المعلومات في شركة الحمادي القابضة، والرعاية الصحية، والعمليات الأمنية، وجميع الأشخاص الذين يعملون تحت سيطرة شركة الحمادي القابضة.
84	Translated (100%)	This includes employees and contractors, suppliers, and 3rd Parties.	تشمل السياسة الموظفين والمتعاقدين والموردين والجهات الخارجية.
85	Translated (100%)	Roles and Responsibilities	الأدوار والمسؤوليات
86	Translated (0%)	Al Hammadi Holding Procurement, Information Technology, and Cybersecurity Departments are responsible for implementing, maintaining, and updating this manual with all its contents, in accordance with any changes in legislative or regulatory requirements or related standards.	تتولى إدارات المشتريات وتكنولوجيا المعلومات والأمن السيبراني في شركة الحمادي القابضة مسؤولية تنفيذ وصيانة وتحديث هذا الدليل بجميع محتوياته، وفقًا لأي تغييرات في المتطلبات التشريعية أو التنظيمية أو المعايير ذات الصلة.
87	Translated (100%)	Policy Review and Update:	مراجعة السياسة وتحديثها:
88	Translated (100%)	Cybersecurity Department.	إدارة الأمن السيبراني.
89	Translated (100%)	Policy Implementation and Enforcement:	تنفيذ السياسة وإنفاذها:
90	Translated (0%)	Procurement and IT Department.	إدارة المشتريات وتكنولوجيا المعلومات.

91	Translated (100%)	Policy Compliance Measurement:	:قياس الامتثال للسياسة
92	Translated (100%)	Cybersecurity Department.	.إدارة الأمن السيبراني
93	Translated (100%)	Principles	المبادئ
94	Translated (0%)	Information Security with Supplier Standardized procedures to govern Al Hammadi Holding relationship with third-parties shall be documented and approved before, during, and after the relationship.	يجب توثيق واعتماد الإجراءات الموحدة لأمن المعلومات مع الموردين لتنظيم .علاقة شركة الحمادي القابضة مع أطراف ثالثة قبل وأثناء وبعد العلاقة
95	Translated (0%)	Third-parties shall be carefully identified and selected in accordance with the regulatory policies and procedures of Al Hammadi Holding, and relevant legislative and regulatory requirements.	يجب تحديد الأطراف الثالثة واختيارها بعناية وفقًا للسياسات والإجراءات .التنظيمية لشركة الحمادي القابضة والمتطلبات التشريعية والتنظيمية ذات الصلة
96	Translated (0%)	Identifying and documenting the types of suppliers, e.g., IT services, logistics utilities, financial services, IT infrastructure components, whom Al Hammadi Holding will allow to access its information.	،تحديد وتوثيق أنواع الموردين، على سبيل المثال، خدمات تكنولوجيا المعلومات والمرافق اللوجستية، والخدمات المالية، ومكونات البنية التحتية لتكنولوجيا .المعلومات، الذين ستسمح لهم شركة الحمادي القابضة بالوصول إلى معلوماتها
97	Translated (0%)	A cybersecurity risk assessment must be conducted, and effective controls on risks must be ensured before signing contracts and agreements with third parties or if changes occur in relevant legal and regulatory requirements.	يجب إجراء تقييم لمخاطر الأمن السيبراني، ويجب ضمان وجود ضوابط فعالة على المخاطر قبل توقيع العقود والاتفاقيات مع أطراف ثالثة أو في حالة حدوث .تغييرات في المتطلبات القانونية والتنظيمية ذات الصلة
98	Translated (0%)	A risk assessment on third-parties and the services provided shall be performed, by auditing third-parties' projects within Al Hammadi Holding and reviewing the events logs of the third-party services periodically (if possible) before and during the relationship.	يجب إجراء تقييم للمخاطر على الأطراف الثالثة والخدمات المقدمة، من خلال تدقيق مشاريع الأطراف الثالثة داخل شركة الحمادي القابضة ومراجعة سجلات .أحداث خدمات الأطراف الثالثة بشكل دوري (إن أمكن) قبل وأثناء العلاقة
99	Translated (0%)	Al Hammadi Holding should identify information security controls for supplier’s access to Al Hammadi Holding’s information.	يجب على شركة الحمادي القابضة تحديد ضوابط أمن المعلومات من أجل وصول .المورد إلى معلومات شركة الحمادي القابضة
100	Translated (0%)	These controls should also address processes and procedures that Al Hammadi Holding require the supplier to implement, including:	يجب أن تتناول هذه الضوابط أيضًا العمليات والإجراءات التي تتطلب شركة :الحمادي القابضة من المورد تنفيذها، بما في ذلك
101	Translated (0%)	Defining, monitoring, and controlling the types of information and access that different types of suppliers will be allowed.	تحديد ومراقبة والتحكم في أنواع المعلومات والوصول إلى الأنواع المختلفة من .الموردين التي سيتم السماح بها
102	Translated (0%)	Monitoring adherence to established information security requirements for each type of supplier and type of access, including third party review and product validation.	مراقبة الالتزام بمتطلبات أمن المعلومات المحددة لكل نوع من الموردين ونوع .الوصول، بما في ذلك مراجعة الطرف الثالث والتحقق من صحة المنتج
103	Translated (0%)	Accuracy and completeness controls to ensure the integrity of the information or information processing provided by either party.	ضوابط الدقة والاكتمال لضمان سلامة المعلومات أو معالجة المعلومات المقدمة .من أي من الطرفين

104	Translated (0%)	Responsibilities of both Al Hammadi Holding and suppliers for handling incidents and contingencies associated with supplier access.	مسؤوليات كل من شركة الحمادي القابضة والموردين عن التعامل مع الحوادث والطوارئ المرتبطة بوصول الموردين.
105	Translated (0%)	Resilience, recovery, and contingency arrangements to ensure the availability of the information or information processing provided by either party.	ترتيبات المرونة والتعافي والطوارئ لضمان توافر المعلومات أو معالجة المعلومات المقدمة من أي من الطرفين.
106	Translated (0%)	Awareness training for Al Hammadi Holding's personnel interacting with supplier personnel regarding appropriate rules of engagement and behavior based on the type of supplier and the level of supplier access to Al Hammadi Holding's systems and information.	تدريب توعوي لموظفي شركة الحمادي القابضة الذين يتفاعلون مع موظفي المورد فيما يتعلق بقواعد الاشتباك والسلوك المناسبة بناءً على نوع المورد ومستوى وصول المورد إلى أنظمة ومعلومات شركة الحمادي القابضة.
107	Translated (0%)	Information security requirements and controls' agreement will be documented and signed by both parties.	سيتم توثيق وتوقيع متطلبات أمن المعلومات واتفاقية الضوابط من قبل الطرفين.
108	Translated (0%)	Managing the necessary transitions of information, information processing facilities and anything else that needs to be moved and ensuring that information security is maintained throughout the transition period.	إدارة التحولات اللازمة للمعلومات ومرافق معالجة المعلومات وأي شيء آخر يحتاج إلى نقل وضمان الحفاظ على أمن المعلومات طوال الفترة الانتقالية.
109	Translated (0%)	Contracts and agreements with third-parties shall state the compliance of the third-party to the implementation of information security requirements and policies of Al Hammadi Holding and relevant legislative and regulatory requirements.	يجب أن تنص العقود والاتفاقيات المبرمة مع أطراف ثالثة على امتثال الطرف الثالث لتنفيذ متطلبات وسياسات أمن المعلومات الخاصة بشركة الحمادي القابضة والمتطلبات التشريعية والتنظيمية ذات الصلة.
110	Translated (0%)	Third-parties' contracts and agreements shall be reviewed by the Department of Legal, and the procurrent (if needed), to ensure their compliance with the terms of the agreement during the contract period and after and any breach will expose third-party to legal liability.	تتم مراجعة عقود واتفاقيات الأطراف الثالثة من قبل إدارة الشؤون القانونية، والوكيل (إذا لزم الأمر)، لضمان امتثالها لشروط الاتفاقية خلال فترة العقد وبعده وأي خرق سيعرض الطرف الثالث للمسؤولية القانونية.
111	Translated (0%)	Contracts and agreements shall enclose non-disclosure clauses of information and secure removal by the third-party of Al Hammadi Holding when the relationship ends.	يجب أن ترفق العقود والاتفاقيات بنود عدم الإفصاح عن المعلومات والإزالة الآمنة من قبل الطرف الثالث لشركة الحمادي القابضة عند انتهاء العلاقة.
112	Translated (0%)	Information security requirements with third-parties shall be reviewed periodically.	يجب مراجعة متطلبات أمن المعلومات مع الأطراف الثالثة بشكل دوري.
113	Translated (0%)	Information security third-party policy shall be reviewed annually, and any changes are documented and approved.	يجب مراجعة سياسة الطرف الثالث لأمن المعلومات سنويًا، ويتم توثيق أي تغييرات والموافقة عليها.
114	Translated (0%)	Outsourced and Managed Services Requirements	متطلبات الخدمات المستعان فيها بمصادر خارجية والخدمات المدارة
115	Translated (0%)	For outsourced or managed services, third-party shall be carefully chosen, according to the following:	بالنسبة للخدمات التي يتم الاستعانة بمصادر خارجية أو إدارتها، يجب اختيار الطرف الثالث بعناية، وفقًا لما يلي:
116	Translated (0%)	Conducting risks assessment and ensuring risks are at an acceptable level, before signing the contracts/agreements or	إجراء تقييم للمخاطر والتأكد من أن المخاطر عند مستوى مقبول، قبل توقيع العقود/الاتفاقيات أو عند حدوث تغييرات في المتطلبات التشريعية والتنظيمية

		when changes happened to the relevant legislative and regulatory requirements.	.ذات الصلة
117	Translated (0%)	The Security Operation Center of the outsourced and managed services that uses remote access shall be located entirely within the KSA.	يجب أن يكون مركز العمليات الأمنية للخدمات التي يتم الاستعانة بمصادر خارجية وإدارتها والتي تستخدم الوصول عن بُعد موجودًا بالكامل داخل المملكة .العربية السعودية
118	Translated (0%)	Outsourcing services of critical systems shall be to Saudi companies only, in accordance with the relevant legislative and regulatory requirements.	يجب أن تكون خدمات الاستعانة بمصادر خارجية للأنظمة الحيوية للشركات .السعودية فقط، وفقًا للمتطلبات التشريعية والتنظيمية ذات الصلة
119	Translated (0%)	Third Party Employment Requirements	متطلبات توظيف الطرف الثالث
120	Translated (0%)	Security screening and vetting shall be conducted on the third-party companies, and personnel, that is working on critical systems.	يجب إجراء الفحص الأمني والتدقيق على الشركات الخارجية والموظفين الذين .يعملون على الأنظمة الحيوية
121	Translated (0%)	(the related personal shall be aware of such activity and a confirmation shall be taken to ensure the protection of PII)	يجب أن يكون الشخص ذو الصلة على دراية بهذا النشاط ويجب أخذ تأكيد) (لضمان حماية معلومات تحديد الهوية الشخصية
122	Translated (0%)	Information security responsibilities and non-Disclosure clauses shall be included in third-party employee contracts (that include during and after the employment relationship of Al Hammadi Holding).	يجب تضمين مسؤوليات أمن المعلومات وبنود عدم الإفصاح في عقود موظفي .الطرف الثالث (التي تشمل أثناء وبعد علاقة العمل مع شركة الحمادي القابضة)
123	Translated (0%)	Authorization and Access Controls	التصريح وضوابط الوصول
124	Translated (0%)	Third parties shall develop and follow a formal access management process to all information and technical systems that process, transmit, or store information of Al Hammadi Holding, according to the information security requirements and policies of Al Hammadi Holding.	يجب على الأطراف الثالثة تطوير واتباع عملية رسمية لإدارة الوصول إلى جميع المعلومات والأنظمة التقنية التي تعالج أو تنقل أو تخزن معلومات شركة الحمادي القابضة، وفقًا لمتطلبات وسياسات أمن المعلومات الخاصة بشركة الحمادي .القابضة
125	Translated (0%)	Access to Al Hammadi Holding shall be secured and monitored.	.يجب تأمين الوصول إلى شركة الحمادي القابضة ومراقبته
126	Translated (0%)	The password authentication shall be applied to all users who have access to information of Al Hammadi Holding, according to the information security requirements and policies of Al Hammadi Holding.	يتم تطبيق مصادقة كلمة المرور على جميع المستخدمين الذين لديهم حق الوصول إلى معلومات شركة الحمادي القابضة، وفقًا لمتطلبات وسياسات أمن المعلومات .الخاصة بشركة الحمادي القابضة
127	Translated (0%)	Multi-factor authentication shall be applied to critical systems access that process, transmit or store information of Al Hammadi Holding.	يجب تطبيق المصادقة متعددة العوامل على الوصول إلى الأنظمة الحيوية التي .تعالج أو تنقل أو تخزن معلومات شركة الحمادي القابضة
128	Translated (0%)	Access rights shall be removed immediately upon the termination of the services of any third-party personal who has access right to information assets of Al Hammadi Holding, or when the employee changes the job role and does not require that access	يجب إزالة حقوق الوصول فور إنهاء خدمات أي شخص تابع لجهة خارجية لديه حق الوصول إلى أصول المعلومات الخاصة بالحمادي القابضة، أو عندما يغير .الموظف الدور الوظيفي ولا يتطلب هذا الوصول بعد الآن

		anymore.	
129	Translated (0%)	Access permissions shall be reviewed periodically in accordance with the information security policies adopted in Al Hammadi Holding.	يجب مراجعة أذونات الوصول بشكل دوري وفقًا لسياسات أمن المعلومات المعتمدة في شركة الحمادي القابضة.
130	Translated (0%)	All audit records shall be stored, maintained, and made available upon request of Al Hammadi Holding.	يجب تخزين جميع سجلات التدقيق والاحتفاظ بها وإتاحتها بناءً على طلب شركة الحمادي القابضة.
131	Translated (0%)	Information security Change Management Requirements	متطلبات إدارة التغيير لأمن المعلومات
132	Translated (0%)	Third-parties shall follow the formal change management process in accordance with Al Hammadi Holding policies, procedures, and information security requirements.	يجب على الأطراف الثالثة اتباع عملية إدارة التغيير الرسمية وفقًا لسياسات وإجراءات شركة الحمادي القابضة ومتطلبات أمن المعلومات.
133	Translated (0%)	The changes to the information assets of Al Hammadi Holding shall be tested before applying it to the Production Environment.	يجب اختبار التغييرات التي تطرأ على أصول المعلومات الخاصة بالحمادي القابضة قبل تطبيقها على بيئة الإنتاج.
134	Translated (0%)	The parties concerned in Al Hammadi Holding shall be informed of any changes under planning and changes were applied to information assets of Al Hammadi Holding.	يجب إبلاغ الأطراف المعنية في شركة الحمادي القابضة بأي تغييرات قيد التخطيط وتم تطبيق التغييرات على أصول المعلومات الخاصة بشركة الحمادي القابضة.
135	Translated (0%)	Incident Response and Business Continuous Requirements	الاستجابة للحوادث ومتطلبات الأعمال المستمرة
136	Translated (0%)	Contract and agreements with third-parties shall include requirements related to reporting information security incidents to Al Hammadi Holding, in case the third-party is exposed to an information security incident.	يجب أن يتضمن العقد والاتفاقيات مع أطراف ثالثة المتطلبات المتعلقة بالإبلاغ عن حوادث أمن المعلومات إلى شركة الحمادي القابضة، في حالة تعرض الطرف الثالث لحادث أمن معلومات.
137	Translated (0%)	The communication procedure and escalation matric between the third-party and Al Hammadi Holding shall be documented, if the third-party is exposed to an information security incident, and these procedures shall be reviewed and updated periodically.	يجب توثيق إجراءات الاتصال ومصفوفة التصعيد بين الطرف الثالث والحمادي القابضة، إذا تعرض الطرف الثالث لحادث أمن معلومات، ويجب مراجعة هذه الإجراءات وتحديثها بشكل دوري.
138	Translated (0%)	A business continuity plan shall be developed to avoid the unavailability of services Al Hammadi Holding in accordance with the business continuity requirements and disaster recovery plan for Al Hammadi Holding.	يجب وضع خطة استمرارية الأعمال لتجنب عدم توفر خدمات شركة الحمادي القابضة وفقًا لمتطلبات استمرارية الأعمال وخطة التعافي من الكوارث لشركة الحمادي القابضة.
139	Translated (0%)	Information Security Requirements	متطلبات أمن المعلومات
140	Translated (0%)	Third-parties shall process, store, and destroy data and information of Al Hammadi Holding in accordance with the data protection policy and standard approved in Al Hammadi Holding.	يجب على الأطراف الثالثة معالجة وتخزين وإتلاف بيانات ومعلومات شركة الحمادي القابضة وفقًا لسياسة ومعيار حماية البيانات المعتمدين في شركة الحمادي القابضة.
141	Translated (0%)	Encryption shall be applied to protect the data and information of Al Hammadi Holding to ensure its confidentiality, integrity, and availability are maintained in accordance with the cryptography policy and standard adopted in Al Hammadi Holding.	يجب تطبيق التشفير لحماية بيانات ومعلومات شركة الحمادي القابضة لضمان الحفاظ على سريتها وسلامتها وتوافرها وفقًا لسياسة التشفير والمعايير المعتمدة في شركة الحمادي القابضة.

142	Translated (0%)	Data backup of Al Hammadi Holding shall be performed periodically and in accordance with the backup policy of Al Hammadi Holding.	يجب إجراء النسخ الاحتياطي لبيانات شركة الحمادي القابضة بشكل دوري ووفقًا لسياسة النسخ الاحتياطي لشركة الحمادي القابضة.
143	Translated (0%)	Processing critical systems' data by external parties in the testing environment is not allowed, unless adequate controls are applied to protect that data, such as data masking, data scrambling, or data Anonymization.	لا يُسمح بمعالجة بيانات الأنظمة الحيوية من قبل أطراف خارجية في بيئة الاختبار، ما لم يتم تطبيق ضوابط كافية لحماية تلك البيانات، مثل إخفاء البيانات أو تشويش البيانات أو إخفاء هوية البيانات.
144	Translated (0%)	Al Hammadi Holding's data of critical systems, which are processed by third parties shall not be transferred out of the production environment.	لا يجوز نقل بيانات الأنظمة الحرجة لشركة الحمادي القابضة، والتي تتم معالجتها من قبل أطراف ثالثة، خارج بيئة الإنتاج.
145	Translated (0%)	Al Hammadi Holding's data of critical systems, which are processed by third parties shall be classified according to the data classification policy approved in Al Hammadi Holding.	يتم تصنيف بيانات شركة الحمادي القابضة للأنظمة الحرجة، والتي تتم معالجتها من قبل أطراف ثالثة وفقًا لسياسة تصنيف البيانات المعتمدة في شركة الحمادي القابضة.
146	Translated (0%)	Include cybersecurity responsibilities and clauses of Non-Disclosure and secure deletion of Al Hammadi Holding's data.	تضمين مسؤوليات الأمن السيبراني وبنود عدم الإفصاح والحذف الآمن لبيانات شركة الحمادي القابضة.
147	Translated (99%)	Audit	التدقيق
148	Translated (0%)	Al Hammadi Holding shall conduct an audit of the relevant processes and systems where necessary and required.	يجب على شركة الحمادي القابضة إجراء تدقيق للعمليات والأنظمة ذات الصلة عند الضرورة والمطلوب.
149	Translated (0%)	All third-party management and employees shall cooperate fully with the audit activities performed by Al Hammadi Holding including the reviews carried out.	يجب على جميع إدارة وموظفي الطرف الثالث التعاون الكامل مع أنشطة التدقيق التي تقوم بها شركة الحمادي القابضة بما في ذلك المراجعات التي يتم إجراؤها.
150	Translated (0%)	Information security within supplier agreements	أمن المعلومات ضمن اتفاقيات الموردين
151	Translated (0%)	The following terms should be considered for inclusion in the agreements in order to satisfy the identified information security requirements:	يجب النظر في الشروط التالية لإدراجها في الاتفاقيات من أجل تلبية متطلبات أمن المعلومات المحددة:
152	Translated (0%)	Description of the information to be provided or accessed and methods of providing or accessing the information.	وصف المعلومات التي سيتم تقديمها أو الوصول إليها وطرق تقديم المعلومات أو الوصول إليها.
153	Translated (0%)	Classification of information according to Al Hammadi Holding’s classification scheme.	تصنيف المعلومات حسب مخطط تصنيف شركة الحمادي القابضة.
154	Translated (0%)	If necessary, also mapping between Al Hammadi Holding’s own classification scheme and the classification scheme of the supplier.	إذا لزم الأمر، قم أيضًا بالتعيين بين مخطط التصنيف الخاص بشركة الحمادي القابضة ومخطط تصنيف المورد.
155	Translated (0%)	Legal and regulatory requirements, including data protection, intellectual property rights and copyright, and a description of how it will be ensured that they are met.	المتطلبات القانونية والتنظيمية، بما في ذلك حماية البيانات وحقوق الملكية الفكرية وحقوق الطبع والنشر، ووصف لكيفية ضمان استيفائها.
156	Translated (0%)	Obligations for access control, performance review, monitoring, reporting and auditing.	التزامات التحكم في الوصول ومراجعة الأداء والمراقبة والإبلاغ والتدقيق.

157	Translated (0%)	Rules of acceptable and unacceptable use of information.	.قواعد الاستخدام المقبول وغير المقبول للمعلومات
158	Translated (0%)	Explicit list of supplier personnel authorized to access or receive Al Hammadi Holding's information.	قائمة صريحة بموظفي المورد المصرح لهم بالوصول إلى معلومات شركة .الحمادي القابضة أو تلقيها
159	Translated (0%)	Al Hammadi Holding's information security policies relevant to each specific contract.	سياسات أمن المعلومات الخاصة بشركة الحمادي القابضة ذات الصلة بكل عقد .محدد
160	Translated (0%)	Incident management requirements and procedures (especially notification and collaboration during incident remediation).	متطلبات وإجراءات إدارة الحوادث (خاصة الإخطار والتعاون أثناء معالجة .(الحوادث
161	Translated (0%)	Training and awareness requirements for specific procedures and information security requirements, e.g., for incident response, authorization procedures.	متطلبات التدريب والتوعية لإجراءات محددة ومتطلبات أمن المعلومات، على .سبيل المثال، للاستجابة للحوادث وإجراءات الترخيص
162	Translated (0%)	Relevant regulations for sub-contracting, including the controls that need to be implemented.	.اللوائح ذات الصلة للتعاقد من الباطن، بما في ذلك الضوابط التي يجب تنفيذها
163	Translated (0%)	Contact persons for information security issues.	.جهات الاتصال لقضايا أمن المعلومات
164	Translated (0%)	Screening requirements for supplier's personnel.	.متطلبات الفحص لموظفي المورد
165	Translated (0%)	Right to audit the supplier processes and controls related to the agreement.	.الحق في تدقيق عمليات الموردين والضوابط المتعلقة بالاتفاقية
166	Translated (0%)	Defect and conflict resolution processes.	.عمليات حل العيوب والنزاعات
167	Translated (0%)	Supplier's obligation to periodically deliver an independent report on the effectiveness of controls and agreement on timely correction of relevant issues raised in the report.	التزام المورد بتقديم تقرير دوري مستقل عن فعالية الضوابط والاتفاق على .التصحيح في الوقت المناسب للقضايا ذات الصلة التي أثيرت في التقرير
168	Translated (0%)	Supplier's obligations to comply with Al Hammadi Holding's security requirements.	.التزامات المورد بالامتثال للمتطلبات الأمنية لشركة الحمادي القابضة
169	Translated (100%)	Compliance and Adherence	الامتثال والالتزام
170	Translated (100%)	Al Hammadi Holding CEO shall ensure compliance with the cybersecurity policies and standards.	يضمن الرئيس التنفيذي لشركة الحمادي القابضة الامتثال لسياسات ومعايير الأمن .السيبراني
171	Translated (0%)	To ensure compliance, the Cybersecurity department will establish regular reporting by the Cybersecurity Manager, conduct periodic audits, or form a Cybersecurity Steering Committee for oversight.	لضمان الامتثال، ستقوم إدارة الأمن السيبراني بإعداد تقارير منتظمة من قبل مدير الأمن السيبراني، أو إجراء عمليات تدقيق دورية، أو تشكيل لجنة توجيهية للأمن .السيبراني للإشراف
172	Translated (100%)	The CS manager shall ensure adherence to this policy.	.يتعين على مدير الأمن السيبراني ضمان الالتزام بهذه السياسة
173	Translated (100%)	All employees of Al Hammadi Holding must adhere to this policy.	.على جميع موظفي شركة الحمادي القابضة الالتزام بهذه السياسة
174	Translated	Violations of this policy may result in legal action in any	قد تؤدي انتهاكات هذه السياسة إلى اتخاذ إجراءات قانونية في أي ولاية قضائية أو

	(100%)	jurisdiction or other measures as deemed appropriate by the Al Hammadi Holding.	.غيرها من التدابير التي تراها شركة الحمادي القابضة مناسبة
175	Translated (100%)	Exceptions	الاستثناءات
176	Translated (100%)	Violation of cybersecurity policies and standards is prohibited unless a prior justified exception is obtained from the Cybersecurity Department or the Cybersecurity Steering Committee.	يُحظر انتهاك سياسات ومعايير الأمن السيبراني ما لم يتم الحصول على استثناء .مبرر مسبق من إدارة الأمن السيبراني أو اللجنة التوجيهية للأمن السيبراني
177	Translated (100%)	In case of a conflict, applicable legislative and regulatory requirements overrule Al Hammadi Holding policies and standards.	في حالة وجود تعارض، فإن المتطلبات التشريعية والتنظيمية المعمول بها تسود .على سياسات ومعايير شركة الحمادي القابضة
178	Translated (100%)	Revision	المراجعة
179	Translated (100%)	This policy is reviewed annually, or after major changes in Al Hammadi Holding's organizational chart or infrastructure, and more frequently whenever required, to ensure it remains appropriate and current for Al Hammadi Holding, ISO 27001, and NCA requirements.	تخضع هذه السياسة لمراجعة سنوية، أو لإعادة التقييم بعد أي تغييرات جوهرية في الهيكل التنظيمي أو البنية التحتية لشركة الحمادي القابضة، إضافة إلى مراجعات دورية إضافية عند الضرورة، وذلك لضمان توافقها المستمر مع وإرشادات، ISO 27001:2022 متطلبات شركة الحمادي القابضة، ومعيار آيزو .الهيئة الوطنية للأمن السيبراني
180	Translated (100%)	Approval Section	قسم الاعتماد
181	Translated (100%)	Prepared by:	:إعداد
182	Translated (100%)	Mr. Mohammed Alamer	السيد/ محمد العامر
183	Translated (100%)	GRC Cybersecurity Specialist	أخصائي حوكمة ومخاطر وامتثال في الأمن السيبراني
184	Translated (100%)	Name	الاسم
185	Translated (100%)	Designation	المسمى الوظيفي
186	Translated (100%)	Signature	التوقيع
187	Translated (100%)	Date	التاريخ
188	Translated (100%)	Reviewed by:	:راجعها
189	Translated (100%)	Ms. Mashael Alotaibi	السيدة/ مشاعل العتيبي
190	Translated	Cybersecurity Manager	مدير الأمن السيبراني

	(100%)		
191	Translated (100%)	Name	الاسم
192	Translated (100%)	Designation	المسمى الوظيفي
193	Translated (100%)	Signature	التوقيع
194	Translated (100%)	Date	التاريخ
195	Translated (100%)	Reviewed by:	راجعها:
196	Translated (100%)	Mr. Majid Al Nahdi	السيد/ ماجد النهدي
197	Translated (100%)	HR Manager	مدير الموارد البشرية
198	Translated (100%)	Name	الاسم
199	Translated (100%)	Designation	المسمى الوظيفي
200	Translated (100%)	Signature	التوقيع
201	Translated (100%)	Date	التاريخ
202	Translated (100%)	Reviewed by:	راجعها:
203	Translated (100%)	Mr. Deepak Dasan	السيد/ ديباك داسان
204	Translated (100%)	IT Manager	مدير تكنولوجيا المعلومات
205	Translated (100%)	Name	الاسم
206	Translated (100%)	Designation	المسمى الوظيفي
207	Translated (100%)	Signature	التوقيع
208	Translated (100%)	Date	التاريخ
209	Translated (100%)	Reviewed by:	راجعها:

210	Translated (0%)	Mr. Omar Alnogeamish	السيد عمر النجيميش
211	Translated (99%)	Lawyer	محامي
212	Translated (100%)	Name	الاسم
213	Translated (100%)	Designation	المسمى الوظيفي
214	Translated (100%)	Signature	التوقيع
215	Translated (100%)	Date	التاريخ
216	Translated (100%)	Approved by:	:اعتمدها
217	Translated (100%)	Dr. Abdulaziz Al Hammadi	الحمادي<Bold></Bold> د./ عبد العزيز<Bold></Bold> <Bold></Bold>
218	Translated (100%)	Chief Operating Officer	الرئيس التنفيذي للعمليات
219	Translated (100%)	Name	الاسم
220	Translated (100%)	Designation	المسمى الوظيفي
221	Translated (100%)	Signature	التوقيع
222	Translated (100%)	Date	التاريخ
223	Translated (100%)	Approved by:	:اعتمدها
224	Translated (100%)	Mr. Mohammad Al Hammadi	السيد/ محمد الحمادي
225	Translated (100%)	Chief Executive Officer	الرئيس التنفيذي
226	Translated (100%)	Name	الاسم
227	Translated (100%)	Designation	المسمى الوظيفي
228	Translated (100%)	Signature	التوقيع
229	Translated	Date	التاريخ

	(100%)		

Segment ID	Segment status	Source segment	Target segment
1	Translated (0%)	<3/><7/><26><10>Information Security Workstation, Mobile Devices, and BYOD Policy<20/> </10></26>	محطة عمل أمن المعلومات والأجهزة المحمولة<10><26><7/><3/> <20/> </10><26/>وسياسة استخدام الجهاز الشخصي
2	Translated (100%)	Page <37><28/> of <36/></37>	<37/></36> من <28></37>صفحة
3	Translated (100%)	Al Hammadi Holding	شركة الحمادي القابضة
4	Translated (0%)	Information Security Workstation,	،محطة عمل أمن المعلومات
5	Translated (0%)	Mobile Devices, and BYOD Policy	الأجهزة المحمولة، وسياسة الاستخدام الشخصي
6	Translated (100%)	CYBERSECURITY DEPARTMENT	إدارة الأمن السيبراني
7	Translated (100%)	Policy ID	معرّف السياسة
8	Translated (100%)	AHH-CS-ISMS-013	AHH-CS-ISMS-013
9	Translated (100%)	Class	الفئة
10	Translated (100%)	Internal Release	إصدار داخلي
11	Not Translated (0%)		
12	Translated (100%)	V3.1	V3.1
13	Translated (100%)	Published at	نُشرت في
14	Translated (100%)	April 2025	أبريل 2025
15	Translated (100%)	Document Owner	المسؤول عن المستند
16	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
17	Translated (100%)	Disclaimer	تنويه
18	Translated (100%)	The information contained in this document is the property of Hammadi Holdings and must not be copied or communicated to a	المعلومات الواردة في هذا المستند هي ملك لشركة الحمادي القابضة ولا يجوز نسخها أو إبلاغها إلى طرف ثالث أو استخدامها لأي غرض آخر غير

		third party or used for any purpose other than that for which it is supplied, without the written consent of Al Hammadi Holding.	الغرض الذي تم توفيرها من أجله، دون موافقة خطية من شركة الحمادي القابضة.
19	Translated (100%)	Contents	جدول المحتويات
20	Translated (100%)	Document Control	ضبط المستندات
21	Translated (100%)	Document Information	معلومات المستند
22	Translated (100%)	Synopsis	الملخص
23	Translated (100%)	Document Title:	عنوان المستند:
24	Translated (0%)	Information Security Workstation, Mobile Devices, and BYOD Policy	محطة عمل أمن المعلومات والأجهزة المحمولة وسياسة استخدام الجهاز الشخصي
25	Translated (100%)	Document Status:	حالة المستند:
26	Translated (100%)	Approved	معتمد
27	Translated (100%)	Document Effective Date:	تاريخ سريان المستند:
28	Translated (100%)	April 2025	أبريل 2025
29	Translated (100%)	Document Issue Date:	تاريخ إصدار المستند:
30	Translated (100%)	April 2025	أبريل 2025
31	Translated (100%)	Document Next Revision Date:	تاريخ المراجعة التالية للمستند:
32	Translated (100%)	April <227>2026</227>	أبريل <227>2026<227/>
33	Translated (100%)	Key contacts	جهات التواصل الرئيسية
34	Translated (100%)	Document Owner:	المسؤول عن المستند:
35	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
36	Translated (100%)	Approval Authority	جهة الاعتماد
37	Translated	Document Created by:	مُنشئ المستند:

	(100%)		
38	Translated (100%)	IT Management	إدارة تكنولوجيا المعلومات
39	Translated (100%)	Document Reviewed by:	راجع المستند:
40	Translated (100%)	Al Hammadi Holding CS &IT Managers	مديرو الأمن السيبراني وتكنولوجيا المعلومات في شركة الحمادي القابضة
41	Translated (100%)	Document Approved by:	اعتمد المستند:
42	Translated (100%)	Al Hammadi Holding COO & CEO	الرئيس التنفيذي للعمليات والرئيس التنفيذي في شركة الحمادي القابضة
43	Translated (100%)	Note:	ملاحظة:
44	Translated (100%)	Any additional approval will be added in the document annex	تُضاف أي اعتمادات إضافية في ملحق المستند
45	Translated (100%)	Classification	التصنيف
46	Translated (100%)	<272>Company Internal – </272>to be shared with 3rd parties after consent of CS Manager	داخلي لاستخدام للشركة<272> – <272/><272/>يُسمح<272> بمشاركته مع جهات خارجية بعد موافقة مدير إدارة الأمن السيبراني
47	Translated (100%)	Version / Dates	الإصدار / التواريخ
48	Translated (100%)	Current Version:	الإصدار الحالي:
49	Translated (100%)	V 3.1	V 3.1
50	Translated (100%)	Date Published:	تاريخ النشر:
51	Translated (100%)	April 2025	أبريل 2025
52	Translated (100%)	Date of Next Review:	تاريخ المراجعة التالية:
53	Translated (100%)	April <317>2026</317>	<317/>2026<317> أبريل<
54	Translated (100%)	Prior Version:	الإصدار السابق:
55	Translated (100%)	V 3.0	V 3.0
56	Translated (100%)	Prior Published:	تاريخ النشر السابق:

57	Translated (100%)	December <344>2024</344>	<344>ديسمبر 2024</344>
58	Translated (100%)	Document Changes	التغييرات على المستند
59	Translated (100%)	Date	التاريخ
60	Translated (100%)	Version	الإصدار
61	Translated (100%)	Document Owner	المسؤول عن المستند
62	Translated (100%)	Change Description	وصف التغيير
63	Translated (100%)	December <371>2024</371>	<371>ديسمبر 2024</371>
64	Translated (100%)	3.0	3.0
65	Translated (100%)	IT Management	إدارة تكنولوجيا المعلومات
66	Translated (0%)	Policy number changed from 6.1.1 to AHH-IT-ISMS-002	تم تغيير رقم السياسة من 6.1.1 إلى AHH - IT - ISMS -002
67	Translated (100%)	April <395>2025</395>	<395>أبريل 2025</395>
68	Translated (100%)	3.1	3.1
69	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
70	Translated (0%)	Document structure changed from Manual to policy and updated based on ISO27001:2022 and NCA ECC-2:2024	تم تغيير هيكل المستند من دليل إلى سياسة وتحديثها بناءً على NCA ECC -2:2024 و ISO27001:2022
71	Translated (100%)	Document Circulation	تعميم المستند
72	Translated (100%)	To	إلى
73	Translated (100%)	Method	الطريقة
74	Translated (100%)	IT Staff	موظفو تكنولوجيا المعلومات
75	Translated (100%)	April 2025	أبريل 2025
76	Translated	Intranet Portal	بوابة الإنترانت

	(100%)		
77	Translated (100%)	All Al Hammadi Staff	جميع موظفي شركة الحمادي
78	Translated (100%)	April 2025	أبريل 2025
79	Translated (100%)	Intranet Portal	بوابة الإنترانت
80	Translated (100%)	Objectives	الأهداف
81	Translated (0%)	The purpose of this policy is to set the principles and procedural implementation by which Al Hammadi Holding shall reduce risks and preserve confidentiality and integrity of all operations handled by Al Hammadi Holding Workstations and Mobile/Personal devices, in compliance with the requirements specified in:	الغرض من هذه السياسة هو تحديد المبادئ والتنفيذ الإجرائي الذي يجب على شركة الحمادي القابضة من خلاله تقليل المخاطر والحفاظ على سرية وسلامة جميع العمليات التي تتعامل معها محطات عمل الحمادي القابضة والأجهزة المحمولة/الشخصية، وفقًا للمتطلبات المحددة في:
82	Translated (0%)	ISO/IEC 27001:2022 Annex-A:A.8.1 User endpoint devices	أجهزة نقطة نهاية المستخدم A.8.1:الملحق أ ISO/IEC 27001:2022
83	Translated (100%)	NCA ECC-2:2024:	ECC-2:2024: معيار الهيئة الوطنية للأمن السيبراني رقم
84	Translated (0%)	2-6 Mobile Devices Security	أمن الأجهزة المحمولة 2-6
85	Translated (100%)	Scope	النطاق
86	Translated (0%)	This policy is applicable to all Al Hammadi Holding ISMS information assets, security operations, and all persons working under Al Hammadi control; this includes employees, contractors, suppliers, and 3rd Parties.	تنطبق هذه السياسة على جميع أصول معلومات نظام إدارة أمن المعلومات في الحمادي القابضة والعمليات الأمنية وجميع الأشخاص الذين يعملون تحت سيطرة الحمادي؛ وهذا يشمل الموظفين والمقاولين والموردين والأطراف الثالثة.
87	Translated (0%)	In addition, this policy particularly covers all workstations, mobile and personal devices for Al Hammadi employees.	بالإضافة إلى ذلك، تغطي هذه السياسة بشكل خاص جميع محطات العمل والأجهزة المحمولة والشخصية لموظفي الحمادي.
88	Translated (0%)	Devices are classified into:	تصنف الأجهزة إلى:
89	Translated (0%)	Workstations:	محطات العمل:
90	Translated (0%)	Fully managed by Al Hammadi Holding, with security configurations enforced.	تدار بالكامل من قبل شركة الحمادي القابضة، مع فرض التكوينات الأمنية.
91	Translated (0%)	Personal and mobile devices BYOD (Bring Your Own Device):	الأجهزة الشخصية والمتنقلة BYOD (أحضر جهازك الخاص):
92	Translated (0%)	Personal devices permitted for accessing corporate resources, with security controls such as encryption, VPN, and remote wipe enabled.	الأجهزة الشخصية المسموح بها للوصول إلى موارد الشركة، مع تمكين عناصر التحكم الأمنية مثل التشفير و VPN والمسح عن بُعد.
93	Translated	Roles and Responsibilities	الأدوار والمسؤوليات

	(100%)		
94	Translated (100%)	Al Hammadi Holding Cybersecurity and IT Departments are responsible for maintaining this policy with all its contents, in accordance with any changes in the applicable regulations and legislation, where:	تتولى إدارات الأمن السيبراني وتكنولوجيا المعلومات في شركة الحمادي القابضة مسؤولية حفظ هذه السياسة بجميع محتوياتها، وفقًا لأي تغييرات تطرأ على اللوائح والتشريعات المعمول بها، وذلك وفقًا لما يلي:
95	Translated (100%)	Policy Review and Update:	مراجعة السياسة وتحديثها:
96	Translated (100%)	Cybersecurity Department.	إدارة الأمن السيبراني.
97	Translated (100%)	Policy Implementation and Enforcement:	تنفيذ السياسة وإنفاذها:
98	Translated (100%)	IT Department.	إدارة تكنولوجيا المعلومات.
99	Translated (100%)	Policy Compliance Measurement:	قياس الامتثال للسياسة:
100	Translated (100%)	Cybersecurity Department.	إدارة الأمن السيبراني.
101	Translated (0%)	Principle	المبدأ
102	Translated (100%)	General	أحكام عامة
103	Translated (0%)	The data and information stored in users' workstations, mobile devices, and BYOD shall be protected according to their classification by using proper security controls to restrict access and to prevent unauthorized access to this information.	يجب حماية البيانات والمعلومات المخزنة في محطات عمل المستخدمين والأجهزة المحمولة وجهاز الكمبيوتر الشخصي وفقًا لتصنيفها باستخدام ضوابط أمنية مناسبة لتقييد الوصول ومنع الوصول غير المصرح به إلى هذه المعلومات.
104	Translated (0%)	Users' workstations and mobile devices shall be updated including operating systems, programs, and applications in accordance with the patch management policy approved in Al Hammadi Holding.	يجب تحديث محطات عمل المستخدمين والأجهزة المحمولة بما في ذلك أنظمة التشغيل والبرامج والتطبيقات وفقًا لسياسة إدارة التصحيح المعتمدة في شركة الحمادي القابضة.
105	Translated (0%)	Configuration and Hardening shall be applied to workstations and mobile devices in accordance with cybersecurity standards, regulations and legislation.	يجب تطبيق التكوين والتصلب على محطات العمل والأجهزة المحمولة وفقًا لمعايير ولوائح وتشريعات الأمن السيبراني.
106	Translated (0%)	Users must consent to:	يجب أن يوافق المستخدمون على:
107	Translated (0%)	Remote wipe of Al Hammadi Holding data (not personal data)	المسح عن بعد لبيانات شركة الحمادي القابضة (وليس البيانات الشخصية)
108	Translated (0%)	Monitoring/logging of access for audit and compliance purposes	مراقبة/تسجيل الوصول لأغراض التدقيق والامتثال
109	Translated (0%)	Employees should not be granted a full privileged access on workstations and mobile devices, and privileges shall be granted	لا ينبغي منح الموظفين حق الوصول المميز الكامل على محطات العمل والأجهزة المحمولة، وتمنح الامتيازات وفقًا لمبدأ الامتياز الأقل.

		according to the least privilege principle.	
110	Translated (0%)	Default user accounts in operating systems and applications shall be deleted or reconfigured during device setup.	يجب حذف حسابات المستخدم الافتراضية في أنظمة التشغيل والتطبيقات أو إعادة تكوينها أثناء إعداد الجهاز.
111	Translated (0%)	The clock shall be synchronized centrally from an accurate and trusted source for all workstations and mobile devices.	يجب مزامنة الساعة مركزيًا من مصدر دقيق وموثوق لجميع محطات العمل والأجهزة المحمولة.
112	Translated (0%)	Corporate data must not be stored in personal apps (e.g., WhatsApp, personal email, unapproved cloud services).	يجب عدم تخزين بيانات الشركة في التطبيقات الشخصية (على سبيل المثال، واتساب والبريد الإلكتروني الشخصي والخدمات السحابية غير المعتمدة).
113	Translated (0%)	Only approved apps from trusted sources may be installed on user's mobile devices.	يمكن تثبيت التطبيقات المعتمدة فقط من مصادر موثوقة على أجهزة الجوال الخاصة بالمستخدم.
114	Translated (0%)	Users and mobile devices shall be provided with a banner (e.g., warnings about monitoring) before login to allow authorized use.	يجب تزويد المستخدمين والأجهزة المحمولة ببانر (على سبيل المثال، تحذيرات حول المراقبة) قبل تسجيل الدخول للسماح بالاستخدام المصرح به.
115	Translated (0%)	Applications allowed shall be whitelisted and data leakage prevention and data monitoring shall be enabled.	يجب إدراج التطبيقات المسموح بها في القائمة البيضاء ويجب تمكين منع تسرب البيانات ومراقبة البيانات.
116	Translated (0%)	Storage media of high privileged users' workstations and mobile devices shall be encrypted according to the encryption standard approved in Al Hammadi Holding.	يجب تشفير وسائط التخزين الخاصة بمحطات عمل المستخدمين ذوي الامتيازات العالية والأجهزة المحمولة وفقًا لمعيار التشفير المعتمد في شركة الحمادي القابضة.
117	Translated (0%)	External storage media shall be prohibited, and prior permission shall be obtained from the Cybersecurity Department in case needed.	يحظر استخدام وسائط التخزين الخارجية، ويجب الحصول على إذن مسبق من إدارة الأمن السيبراني عند الحاجة.
118	Translated (0%)	Users' workstations, mobile devices, and personal devices (BYOD) with outdated or expired software (including operating systems, programs, and applications) should not be allowed to connect to Al Hammadi Holding network to prevent any arising security threats from outdated software.	يجب عدم السماح لمحطات عمل المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD) التي تحتوي على برامج قديمة أو منتهية الصلاحية (بما في ذلك أنظمة التشغيل والبرامج والتطبيقات) بالاتصال بشبكة الحمادي القابضة لمنع أي تهديدات أمنية ناشئة عن البرامج القديمة.
119	Translated (0%)	Users' workstations, mobile devices, and personal devices (BYOD) that are not equipped with the latest protection solutions are prohibited from being connected to Al Hammadi network, to avoid any cyber risks such as unauthorized access, malware infections, or data leakage.	يحظر توصيل محطات عمل المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD) غير المجهزة بأحدث حلول الحماية بشبكة الحمادي، لتجنب أي مخاطر إلكترونية مثل الوصول غير المصرح به أو عدوى البرامج الضارة أو تسرب البيانات.
120	Translated (0%)	Protection solutions include antivirus, anti-malware, host-based firewall, and advanced host-based intrusion detection/prevention systems.	تشمل حلول الحماية مكافحة الفيروسات ومكافحة البرامج الضارة وجدار الحماية القائم على المضيف وأنظمة متقدمة للكشف عن/منع التسلل القائم على المضيف.
121	Translated (0%)	Session timeout shall be configured in unattended user workstations and mobile devices for 5 minutes.	يجب تكوين مهلة الجلسة في محطات عمل المستخدم غير المراقبة والأجهزة المحمولة لمدة 5 دقائق.
122	Translated (0%)	Users' workstations shall be managed using Active Directory Server for Al Hammadi Holding domain or another central administrative system.	يجب إدارة محطات عمل المستخدمين باستخدام خادم Active Directory لنطاق شركة الحمادي القابضة أو نظام إداري مركزي آخر.
123	Translated (0%)	Users' workstations, mobile devices shall be configured with the Domain Controller units to enforce company policies and	يجب تكوين محطات عمل المستخدمين والأجهزة المحمولة مع وحدات تحكم المجال لفرض سياسات الشركة وتكويناتها.

		configurations.	
124	Translated (0%)	Group policy in Al Hammadi Holding shall be implemented and applied in all workstations and mobile devices to ensure that Al Hammadi Holding complies with regulatory and cybersecurity controls.	يجب تنفيذ سياسة المجموعة في شركة الحمادي القابضة وتطبيقها في جميع محطات العمل والأجهزة المحمولة لضمان امتثال شركة الحمادي القابضة للضوابط التنظيمية وضوابط الأمن السيبراني.
125	Translated (0%)	Workstations Information Security Requirements	متطلبات أمن معلومات محطات العمل
126	Translated (0%)	High privileged users' devices of the technical team shall be defined and isolated in a management network and not connected to any other networks or services.	يجب تحديد أجهزة المستخدمين ذوي الامتيازات العالية للفريق الفني وعزلها في شبكة إدارة وعدم توصيلها بأي شبكات أو خدمات أخرى.
127	Translated (0%)	High privileged users' devices shall be configured to send logs and events records to a centralized SIEM system in accordance with the cybersecurity event log and monitoring management policy, with disabling the ability to change this configuration by the user.	يجب تكوين أجهزة المستخدمين ذوي الامتيازات العالية لإرسال السجلات المركزي وفقًا لسجل أحداث الأمن SIEM وسجلات الأحداث إلى نظام السيبراني وسياسة إدارة المراقبة، مع تعطيل القدرة على تغيير هذا التكوين من قبل المستخدم.
128	Translated (0%)	Users' devices shall be physically secured within Al Hammadi Holding buildings.	يجب تأمين أجهزة المستخدمين فعليًا داخل مباني شركة الحمادي القابضة.
129	Translated (0%)	Mobile Devices Cybersecurity Requirements	متطلبات الأمن السيبراني للأجهزة المحمولة
130	Translated (0%)	The mobile devices access to the critical systems is prohibited except for a temporary period only, after conducting the risk assessment and taking the necessary approvals from the Cybersecurity Department.	يُحظر وصول الأجهزة المحمولة إلى الأنظمة الحرجة إلا لفترة مؤقتة فقط، بعد إجراء تقييم المخاطر وأخذ الموافقات اللازمة من إدارة الأمن السيبراني.
131	Translated (0%)	Full disk encryption shall be applied for mobile devices that have access to critical systems.	يجب تطبيق تشفير القرص الكامل للأجهزة المحمولة التي يمكنها الوصول إلى الأنظمة الحيوية.
132	Translated (0%)	BYOD Cybersecurity Requirements	متطلبات الأمن السيبراني للاستخدام الشخصي
133	Translated (0%)	Mobile devices shall be managed centrally using the Mobile Device Management System (MDM).	يجب إدارة الأجهزة المحمولة مركزيًا باستخدام نظام إدارة الأجهزة المحمولة (MDM).
134	Translated (0%)	The data and information of Al Hammadi Holding stored on the employees' personal devices (BYOD) shall be isolated and encrypted.	يجب عزل وتشفير بيانات ومعلومات شركة الحمادي القابضة المخزنة على الأجهزة الشخصية للموظفين (BYOD).
135	Translated (100%)	Other Requirements	متطلبات أخرى
136	Translated (0%)	Perform data backup periodically of workstations and mobile devices, in accordance with the backup policy approved in Al Hammadi Holding.	إجراء نسخ احتياطي للبيانات بشكل دوري لمحطات العمل والأجهزة المحمولة، وفقًا لسياسة النسخ الاحتياطي المعتمدة في شركة الحمادي القابضة.
137	Translated (0%)	Upon termination of employment or contract, access to Al Hammadi Holding resources shall be revoked.	عند إنهاء العمل أو العقد، يتم إلغاء الوصول إلى موارد شركة الحمادي القابضة.
138	Translated (0%)	Al Hammadi Holding data must be removed from the device through a secure wipe or un-enrollment process.	يجب إزالة بيانات شركة الحمادي القابضة من الجهاز من خلال مسح آمن أو عملية إلغاء التسجيل.
139	Translated	Al Hammadi Holding reserves the right to restrict or revoke access at	تحتفظ شركة الحمادي القابضة بالحق في تقييد أو إلغاء الوصول في أي

	(0%)	any time.	.وقت
140	Translated (0%)	Al Hammadi data stored on mobile and personal devices (BYOD) shall be deleted in the following cases:	يتم حذف بيانات الحمادي المخزنة على الأجهزة المحمولة والشخصية (BYOD) في الحالات التالية:
141	Translated (0%)	Loss or theft of the mobile device.	.فقدان أو سرقة الجهاز المحمول
142	Translated (0%)	Termination of the relationship between the user and Al Hammadi Holding.	.إنهاء العلاقة بين المستخدم والحمادي القابضة
143	Translated (0%)	employees aware about the proper use of workstations and mobile devices, and their responsibilities towards it, in accordance with the acceptable use policy approved in Al Hammadi Holding, and conduct private awareness sessions for high privileged users of critical systems.	،الموظفون على دراية بالاستخدام السليم لمحطات العمل والأجهزة المحمولة ومسؤولياتهم تجاهها، وفقًا لسياسة الاستخدام المقبول المعتمدة في شركة الحمادي القابضة، وإجراء جلسات توعية خاصة للمستخدمين ذوي .الامتيازات العالية للأنظمة الحرجة
144	Translated (0%)	Workstation and mobile devices and BYOD policy shall be reviewed annually, document the changes and approve it.	يجب مراجعة محطة العمل والأجهزة المحمولة وسياسة استخدام الجهاز .الشخصي سنويًا وتوثيق التغييرات والموافقة عليها
145	Translated (100%)	Compliance and Adherence	الامتثال والالتزام
146	Translated (100%)	Al Hammadi Holding CEO shall ensure compliance with the cybersecurity policies and standards.	يضمن الرئيس التنفيذي لشركة الحمادي القابضة الامتثال لسياسات ومعايير .الأمن السيبراني
147	Translated (100%)	To ensure compliance, the Cybersecurity department will establish regular reporting by the Cybersecurity Manager, conduct periodic audits, or form a Cybersecurity Committee for oversight.	لضمان الامتثال، سينشئ قسم الأمن السيبراني نظامًا لتقديم تقارير منتظمة يُعدّها مدير الأمن السيبراني، ويجري عمليات تدقيق دورية، أو يشكل لجنة .للأمن السيبراني للإشراف
148	Translated (100%)	The CS manager shall ensure adherence to this policy.	.يتعين على مدير الأمن السيبراني ضمان الالتزام بهذه السياسة
149	Translated (100%)	All employees of Al Hammadi Holding must adhere to this policy.	.على جميع موظفي شركة الحمادي القابضة الالتزام بهذه السياسة
150	Translated (100%)	Violations of this policy may result in legal action in any jurisdiction or other measures as deemed appropriate by the Al Hammadi Holding.	قد تؤدي انتهاكات هذه السياسة إلى اتخاذ إجراءات قانونية في أي ولاية .قضائية أو غيرها من التدابير التي تراها شركة الحمادي القابضة مناسبة
151	Translated (100%)	Exceptions	الاستثناءات
152	Translated (100%)	Violation of cybersecurity policies and standards is prohibited unless a prior justified exception is obtained from the Cybersecurity Department or the Cybersecurity Steering Committee.	يُحظر انتهاك سياسات ومعايير الأمن السيبراني ما لم يتم الحصول على استثناء مبرر مسبق من إدارة الأمن السيبراني أو اللجنة التوجيهية للأمن .السيبراني
153	Translated (100%)	In case of a conflict, applicable legislative and regulatory requirements overrule Al Hammadi Holding policies and standards.	في حالة وجود تعارض، فإن المتطلبات التشريعية والتنظيمية المعمول بها .تسود على سياسات ومعايير شركة الحمادي القابضة
154	Translated (100%)	Revision	المراجعة
155	Translated (100%)	This policy is reviewed annually, after major changes in Al Hammadi Holding’s organizational chart or infrastructure, and more frequently whenever required, to ensure it remains appropriate and current for	تخضع هذه السياسة لمراجعة سنوية، ولإعادة التقييم بعد أي تغييرات ،جوهرية في الهيكل التنظيمي أو البنية التحتية لشركة الحمادي القابضة إضافة إلى مراجعات دورية إضافية عند الضرورة، وذلك لضمان توافقها

		Al Hammadi Holding, ISO 27001, and NCA requirements.	ISO المستمر مع متطلبات شركة الحمادي القابضة، ومعيار آيزو .وإرشادات الهيئة الوطنية للأمن السيبراني ،27001:2022
156	Translated (100%)	Approval Section	قسم الاعتماد
157	Translated (100%)	Prepared by:	:إعداد
158	Translated (100%)	Mr. Mohammed Alamer	السيد/ محمد العامر
159	Translated (100%)	GRC Cybersecurity Specialist	أخصائي حوكمة ومخاطر وامتثال في الأمن السيبراني
160	Translated (100%)	Name	الاسم
161	Translated (100%)	Designation	المسمى الوظيفي
162	Translated (100%)	Signature	التوقيع
163	Translated (100%)	Date	التاريخ
164	Translated (100%)	Reviewed by:	:راجعها
165	Translated (100%)	Mr. Deepak Dasan	السيد/ ديباك داسان
166	Translated (100%)	IT Manager	مدير تكنولوجيا المعلومات
167	Translated (100%)	Name	الاسم
168	Translated (100%)	Designation	المسمى الوظيفي
169	Translated (100%)	Signature	التوقيع
170	Translated (100%)	Date	التاريخ
171	Translated (100%)	Reviewed by:	:راجعها
172	Translated (100%)	Ms. Mashael Alotaibi	السيدة/ مشاعل العتيبي
173	Translated (100%)	*<1152>*Cybersecurity *</1152>*Manager	*<*مدير *<1152>*الأمن السيبراني*/1152>*
174	Translated	Name	الاسم

	(100%)		
175	Translated (100%)	Designation	المسمى الوظيفي
176	Translated (100%)	Signature	التوقيع
177	Translated (100%)	Date	التاريخ
178	Translated (100%)	Approved by:	اعتمدها:
179	Translated (100%)	Dr. Abdulaziz Al Hammadi	الحمادي<Bold><Bold></Bold></Bold> د./ عبد العزيز<Bold><Bold> <Bold><Bold></Bold></Bold>
180	Translated (100%)	Chief Operating Officer	الرئيس التنفيذي للعمليات
181	Translated (100%)	Name	الاسم
182	Translated (100%)	Designation	المسمى الوظيفي
183	Translated (100%)	Signature	التوقيع
184	Translated (100%)	Date	التاريخ
185	Translated (100%)	Approved by:	اعتمدها:
186	Translated (100%)	Mr. Mohammad Al Hammadi	السيد/ محمد الحمادي
187	Translated (100%)	Chief Executive Officer	الرئيس التنفيذي
188	Translated (100%)	Name	الاسم
189	Translated (100%)	Designation	المسمى الوظيفي
190	Translated (100%)	Signature	التوقيع
191	Translated (100%)	Date	التاريخ

Segment ID	Segment status	Source segment	Target segment
1	Translated (0%)	<2>Information Security Physical & Environmental Management Policy </2><13/><17/><21/>	أمن المعلومات سياسة الإدارة المادية والبيئية<2> </2><13/><17/><21/>
2	Translated (100%)	Page <38><29/> of <37/></38>	صفحة <38></29> من <37/></38>
3	Translated (100%)	Al Hammadi Holding	شركة الحمادي القابضة
4	Translated (0%)	Information Security Physical & Environmental Management Policy	سياسة إدارة أمن المعلومات المادية والبيئية
5	Translated (100%)	CYBERSECURITY DEPARTMENT	إدارة الأمن السيبراني
6	Translated (100%)	Policy ID	معرّف السياسة
7	Translated (100%)	AHH-CS-ISMS-014	AHH-CS-ISMS-014
8	Translated (100%)	Class	الفئة
9	Translated (100%)	Internal Release	إصدار داخلي
10	Not Translated (0%)		
11	Translated (100%)	V3.1	V3.1
12	Translated (100%)	Published at	نُشرت في
13	Translated (100%)	April 2025	أبريل 2025
14	Translated (100%)	Document Owner	المسؤول عن المستند
15	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
16	Translated (100%)	Disclaimer	تنويه
17	Translated (100%)	The information contained in this document is the property of Hammadi Holding and must not be copied or communicated to a third party or used for any purpose other than that for which it is supplied, without the written consent of Al Hammadi Holding.	المعلومات الواردة في هذا المستند هي ملك لشركة الحمادي القابضة ولا يجوز نسخها أو إبلاغها إلى طرف ثالث أو استخدامها لأي غرض آخر غير الغرض الذي تم توفيرها من أجله، دون موافقة خطية من شركة الحمادي القابضة.

18	Translated (100%)	Contents	جدول المحتويات
19	Translated (100%)	Document Control	ضبط المستندات
20	Translated (100%)	Document Information	معلومات المستند
21	Translated (100%)	Synopsis	الملخص
22	Translated (100%)	Document Title:	:عنوان المستند
23	Translated (100%)	Information Security Physical & Environmental Management Policy	سياسة إدارة أمن المعلومات المادية والبيئية
24	Translated (100%)	Document Status:	:حالة المستند
25	Translated (100%)	Approved	معتمد
26	Translated (100%)	Document Effective Date:	:تاريخ سريان المستند
27	Translated (100%)	April 2025	أبريل 2025
28	Translated (100%)	Document Issue Date:	:تاريخ إصدار المستند
29	Translated (0%)	April<212> </212>2025	أبريل<212> <212/>2025
30	Translated (100%)	Document Next Revision Date:	:تاريخ المراجعة التالية للمستند
31	Translated (100%)	April 2026	أبريل 2026
32	Translated (100%)	Key contacts	جهات التواصل الرئيسية
33	Translated (100%)	Document Owner:	:المسؤول عن المستند
34	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
35	Translated (100%)	Approval Authority	جهة الاعتماد
36	Translated (100%)	Document Created by:	:مُنشئ المستند
37	Translated	IT Management	إدارة تكنولوجيا المعلومات

	(100%)		
38	Translated (100%)	Document Reviewed by:	:راجع المستند
39	Translated (100%)	Al Hammadi Holding CS&IT Managers	مديرو الأمن السيبراني وتكنولوجيا المعلومات في شركة الحمادي القابضة
40	Translated (100%)	Document Approved by:	:اعتمد المستند
41	Translated (0%)	Al Hammadi Holding COO, CEO	المدير التنفيذي لشركة الحمادي القابضة
42	Translated (100%)	Note:	:ملاحظة
43	Translated (100%)	Any additional approval will be added in the document annex	تُضاف أي اعتمادات إضافية في ملحق المستند
44	Translated (100%)	Classification	التصنيف
45	Translated (100%)	<281>Company Internal – </281>to be shared with 3rd parties after consent of CS Manager	داخلي لاستخدام للشركة<281> – </281><281/>يُسمح<281> بمشاركته مع جهات خارجية بعد موافقة مدير إدارة الأمن السيبراني
46	Translated (100%)	Version / Dates	الإصدار / التواريخ
47	Translated (100%)	Current Version:	:الإصدار الحالي
48	Translated (100%)	V3.1	V3.1
49	Translated (100%)	Date Published:	:تاريخ النشر
50	Translated (100%)	April 2025	أبريل 2025
51	Translated (100%)	Date of Next Review:	:تاريخ المراجعة التالية
52	Translated (100%)	April 2026	أبريل 2026
53	Translated (100%)	Prior Version:	:الإصدار السابق
54	Translated (100%)	V3.0	V3.0
55	Translated (100%)	Prior Published:	:تاريخ النشر السابق
56	Translated (100%)	December 2024	ديسمبر 2024

57	Translated (100%)	Document Changes	التغييرات على المستند
58	Translated (100%)	Date	التاريخ
59	Translated (100%)	Version	الإصدار
60	Translated (100%)	Document Owner	المسؤول عن المستند
61	Translated (100%)	Change Description	وصف التغيير
62	Translated (100%)	December 2024	ديسمبر 2024
63	Translated (100%)	3.0	3.0
64	Translated (100%)	IT Management	إدارة تكنولوجيا المعلومات
65	Translated (100%)	Updated policy number to AHH-IT-ISMS-008	AHH-IT-ISMS-008 تحديث رقم السياسة إلى
66	Translated (100%)	April 2025	أبريل 2025
67	Translated (100%)	3.1	3.1
68	Translated (0%)	Cybersecurity department	إدارة الأمن السيبراني
69	Translated (0%)	Policy reviewed and updated based on NCA ECC-2:2024 and ISO27001:2022 requirements	و NCA ECC -2:2024 تمت مراجعة السياسة وتحديثها بناءً على متطلبات ISO27001:2022
70	Translated (100%)	Document Circulation	تعميم المستند
71	Translated (100%)	To	إلى
72	Translated (100%)	Date	التاريخ
73	Translated (100%)	Method	الطريقة
74	Translated (0%)	All ITDT Staff	جميع موظفي إدارة تكنولوجيا المعلومات والتحول الرقمي
75	Translated (100%)	April 2025	أبريل 2025
76	Translated	Intranet Portal	بوابة الإنترانت

	(100%)		
77	Translated (100%)	All Al Hammadi Staff	جميع موظفي شركة الحمادي
78	Translated (100%)	April 2025	أبريل 2025
79	Translated (100%)	Intranet Portal	بوابة الإنترانت
80	Translated (100%)	Objectives	الأهداف
81	Translated (0%)	<430>The purpose of this policy is to set the principles and procedural implementation by which </430><442><440>Al Hammadi Holding</440></442><445> shall protect physical areas and environment that contain critical information technology assets and facilities against unauthorized physical access, damage, and interference, in compliance with the requirements specified in:</445>	الغرض من هذه السياسة هو وضع المبادئ والتنفيذ الإجرائي الذي<430> يجب على<440><442> شركة الحمادي القابضة</430> من خلاله<445> حماية المناطق المادية والبيئة التي </440></442> تحتوي على أصول ومرافق تكنولوجيا المعلومات الحيوية من الوصول المادي غير المصرح به والتلف والتدخل، وفقًا للمتطلبات المحددة في: </445>
82	Translated (100%)	ISO/IEC 27001 Annex-A:	الملحق أ ISO 27001:2022/معيار آيزو:
83	Translated (0%)	A.7.1 Physical security perimeters, A.7.2 Physical entry, A.7.3 Securing offices, rooms and facilities, A.7.4 Physical security monitoring, A.7.5 Protecting against physical and environmental threats, A.7.6 Working in secure areas, A.7.7 Clear desk and clear screen, A.7.8 Equipment siting and protection, A.7.9 Security of assets off-premises, A.7.11 Supporting utilities, A.7.12 Cabling security, A.7.13 Equipment maintenance, A.7.14 Secure disposal or re-use of equipment	أ .7.1 محيط الأمن المادي، أ .7.2 الدخول المادي، أ .7.3 تأمين المكاتب والغرف والمرافق، أ .7.4 مراقبة الأمن المادي، أ .7.5 الحماية من التهديدات المادية والبيئية، أ .7.6 العمل في مناطق آمنة، أ .7.7 مكتب وشاشة واضحة، أ .7.8 تحديد موقع المعدات وحمايتها، أ .7.9 أمن الأصول خارج أماكن العمل، أ .7.11 المرافق الداعمة، أ .7.12 أمن الكابلات، أ .7.13 صيانة المعدات، أ .7.14 التخلص الآمن من المعدات أو إعادة استخدامها
84	Translated (100%)	NCA ECC-2:2024:	ECC-2:2024: معيار الهيئة الوطنية للأمن السيبراني رقم
85	Translated (0%)	2-14 Physical Security	2-14 الأمن المادي
86	Translated (100%)	Scope	النطاق
87	Translated (0%)	This policy is applicable to all Al Hammadi Holding ISMS information assets, areas, facilities, and all persons doing work under Al Hammadi Holding’s control.	تنطبق هذه السياسة على جميع أصول معلومات نظام إدارة أمن المعلومات في شركة الحمادي القابضة والمناطق والمرافق وجميع الأشخاص الذين يعملون تحت سيطرة شركة الحمادي القابضة.
88	Translated (93%)	This includes employees and contractors, contractors, suppliers, and 3rd Parties.	تشمل السياسة الموظفين والمتعاقدين والمقاولين والموردين والجهات الخارجية.
89	Translated (100%)	Roles and Responsibilities	الأدوار والمسؤوليات
90	Translated (100%)	Al Hammadi Holding Cybersecurity and IT Departments are responsible for maintaining this policy with all its contents, in accordance with any	تتولى إدارات الأمن السيبراني وتكنولوجيا المعلومات في شركة الحمادي القابضة مسؤولية حفظ هذه السياسة بجميع محتوياتها، وفقًا لأي تغييرات

		changes in the applicable regulations and legislation, where:	:تطرأ على اللوائح والتشريعات المعمول بها، وذلك وفقًا لما يلي
91	Translated (100%)	Policy Review and Update:	:مراجعة السياسة وتحديثها
92	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
93	Translated (0%)	The Physical Security Team is responsible for notifying Al Hammadi Holding CS and IT Departments about any violations or physical security breaches to IT facilities according to the defined controls in this policy.	يكون فريق الأمن المادي مسؤولًا عن إخطار شركة الحمادي القابضة للخدمات الأمنية وإدارات تكنولوجيا المعلومات بأي انتهاكات أو خروقات أمنية مادية لمرافق تكنولوجيا المعلومات وفقًا للضوابط المحددة في هذه السياسة.
94	Translated (0%)	Al Hammadi Holding IT is responsible for supporting the relevant business functions in the implementation of the defined controls.	الحمادي القابضة لتقنية المعلومات هي المسؤولة عن دعم وظائف الأعمال ذات الصلة في تنفيذ الضوابط المحددة.
95	Translated (0%)	Secure Areas	المناطق الآمنة
96	Translated (0%)	Physical Security Perimeter	محيط الأمن المادي
97	Translated (0%)	Al Hammadi Holding security perimeters shall be defined and used to protect areas that contain sensitive or critical information and technology facilities.	يجب تحديد واستخدام المحيط الأمني لشركة الحمادي القابضة لحماية المناطق التي تحتوي على مرافق معلوماتية وتقنية حساسة أو حرجة.
98	Translated (0%)	The siting and strength of each perimeter shall depend on the security requirements of the assets and the results of Al Hammadi Holding risk assessments.	يجب أن يعتمد موقع وقوة كل محيط على المتطلبات الأمنية للأصول ونتائج تقييمات مخاطر الحمادي القابضة.
99	Translated (0%)	Periodic testing and assessment shall be conducted over all implemented environmental and physical protection controls.	يجب إجراء اختبار وتقييم دوريين على جميع ضوابط الحماية البيئية والمادية المنفذة.
100	Translated (0%)	Unused and unsupervised network access points providing access to Al Hammadi Holding IT environment shall be disabled.	يجب تعطيل نقاط الوصول إلى الشبكة غير المستخدمة وغير الخاضعة للإشراف التي توفر الوصول إلى بيئة تكنولوجيا المعلومات في شركة الحمادي القابضة.
101	Translated (0%)	Perimeters of Al Hammadi Holding buildings or sites containing information technology facilities shall be physically sound with no gaps or areas where a break-in could easily occur.	يجب أن تكون محيط مباني شركة الحمادي القابضة أو المواقع التي تحتوي على مرافق تكنولوجيا المعلومات سليمة جسديًا مع عدم وجود فجوات أو مناطق يمكن أن يحدث فيها اقتحام بسهولة.
102	Translated (0%)	Where applicable, roofs, walls, and flooring of sites shall be of solid construction.	حيثما ينطبق ذلك، يجب أن تكون الأسطح والجدران والأرضيات في المواقع من البناء الصلب.
103	Translated (0%)	All external doors shall be protected against unauthorized access with control mechanisms, (e.g., bars, alarms, locks).	يجب حماية جميع الأبواب الخارجية من الوصول غير المصرح به مع آليات التحكم، (على سبيل المثال، القضبان والإنذارات والأقفال).
104	Translated (0%)	Site doors and windows shall be locked when unattended and external protection shall be considered for windows, particularly at ground level.	يجب قفل أبواب ونوافذ الموقع عند عدم وجود مراقبة ويجب مراعاة الحماية الخارجية للنوافذ، لا سيما على مستوى الأرض.
105	Translated (0%)	Security guards shall be present at the building entrance to control and monitor physical access to the site or building.	يجب أن يكون حراس الأمن موجودين عند مدخل المبنى للتحكم في الوصول المادي إلى الموقع أو المبنى ومراقبته.
106	Translated (0%)	Where applicable, physical barriers shall be built to prevent unauthorized physical access and environmental contamination.	حيثما ينطبق ذلك، يجب بناء حواجز مادية لمنع الوصول المادي غير المصرح به والتلوث البيئي.

107	Translated (0%)	All fire doors on a perimeter shall be alarmed, monitored, and tested.	.يجب إنذار جميع أبواب الحريق على المحيط ومراقبتها واختبارها
108	Translated (0%)	Intruder detection systems shall be installed.	.يجب تركيب أنظمة الكشف عن الدخلاء
109	Translated (0%)	Unoccupied areas shall always be alarmed.	.يجب دائمًا إنذار المناطق غير المأهولة
110	Translated (0%)	<755><747>IT facilities managed by Al Hammadi Holding shall be physically separated from</747></755><758> </758><764><762>those managed by external parties.</762></764>	يجب فصل مرافق تكنولوجيا المعلومات التي تديرها<755><747> شركة الحمادي القابضة فعليًا عن</747/></755/><758> تلك التي تديرها أطراف خارجية.</762/></764/><762></764></758>
111	Translated (0%)	<773><768>Al Hammadi Holding shall comply with regional, national, and international standards</768></773><776> </776><782><780>which shall operate in accordance with local authorities and fire code.</780></782>	تلتزم شركة الحمادي القابضة بالمعايير الإقليمية والوطنية<773><768> والدولية</768/></773/><776> <776/><780><782> التي يجب أن تعمل وفقًا للسلطات المحلية وقواعد مكافحة الحرائق.</780/><782/>
112	Translated (0%)	Devices that process payment card data shall be protected and inspected periodically against tampering and substitution.	يجب حماية الأجهزة التي تعالج بيانات بطاقة الدفع وفحصها بشكل دوري .ضد التلاعب والاستبدال
113	Translated (0%)	Privacy-sensitive zones (e.g., counseling rooms, patient interview areas) must ensure visual and auditory privacy (e.g., soundproofing, signage).	يجب أن تضمن المناطق الحساسة للخصوصية (مثل غرف الاستشارة ومناطق مقابلة المرضى) الخصوصية البصرية والسمعية (مثل العزل .(الصوتي واللافتات
114	Translated (0%)	Surveillance (e.g., CCTV) must avoid areas where personal data is visible and comply with privacy laws (e.g., no surveillance in restrooms or private offices without notification).	يجب أن تتجنب المراقبة (على سبيل المثال، كاميرات المراقبة) المناطق التي تكون فيها البيانات الشخصية مرئية وأن تمتثل لقوانين الخصوصية على سبيل المثال، لا توجد مراقبة في الحمامات أو المكاتب الخاصة دون) .(إشعار
115	Translated (0%)	Physical Entry Controls	ضوابط الدخول المادي
116	Translated (0%)	Al Hammadi Holding Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	يجب حماية المناطق الآمنة التابعة لشركة الحمادي القابضة من خلال ضوابط الدخول المناسبة لضمان السماح بالوصول للأفراد المصرح لهم .فقط
117	Translated (0%)	Al Hammadi Holding visitors shall be escorted unless access has been previously approved.	يجب مرافقة زوار شركة الحمادي القابضة ما لم تتم الموافقة على .الوصول مسبقًا
118	Translated (0%)	Visitors shall only be granted access for specific and authorized purposes and locations.	.لا يُسمح للزوار بالوصول إلا لأغراض ومواقع محددة ومصرح بها
119	Translated (0%)	The identity of visitors shall be authenticated by appropriate means.	.يجب المصادقة على هوية الزوار بالوسائل المناسبة
120	Translated (0%)	Date and time of entry and departure of visitors shall be recorded.	.يجب تسجيل تاريخ ووقت دخول ومغادرة الزوار
121	Translated (0%)	Access to areas where confidential information is processed or stored shall be restricted to authorized individuals only.	يقتصر الوصول إلى المناطق التي تتم فيها معالجة المعلومات السرية أو .تخزينها على الأفراد المصرح لهم فقط
122	Translated (0%)	A log audit trail of all access shall be securely maintained and monitored.	يجب الحفاظ على مسار تدقيق السجل لجميع عمليات الوصول ومراقبته .بشكل آمن

123	Translated (0%)	Al Hammadi Holding employees, contractors and external parties shall wear visible identification.	يجب على موظفي شركة الحمادي القابضة والمقاولين والأطراف الخارجية ارتداء بطاقة تعريف مرئية.
124	Translated (0%)	Any unescorted individual not wearing visible identification shall immediately be reported to Al Hammadi Holding security personnel.	يجب إبلاغ أفراد أمن شركة الحمادي القابضة على الفور بأي فرد غير مصحوب لا يرتدي بطاقة هوية مرئية.
125	Translated (0%)	External party support service personnel shall be granted restricted access to secure areas only when required, this access shall be authorized and monitored.	لا يُسمح لموظفي خدمة دعم الطرف الخارجي بالوصول المقيد إلى المناطق الآمنة إلا عند الاقتضاء، ويجب التصريح بهذا الوصول ومراقبته.
126	Translated (0%)	Access rights to secure areas shall be regularly reviewed, updated, and revoked when necessary.	يجب مراجعة حقوق الوصول إلى المناطق الآمنة وتحديثها وإلغاؤها بانتظام عند الضرورة.
127	Translated (100%)	Signs are not to be posted on wiring closets, telephone rooms, data center facilities or other equipment components that would attract the attention of unauthorized individuals.	يُحظر تعليق لافتات على غرف الأسلاك، أو غرف الهواتف، أو مرافق مراكز البيانات، أو أي مكونات أخرى من المعدات قد تجذب انتباه الأفراد غير المصرح لهم.
128	Translated (0%)	Data Centers and IT Communication Facilities	مراكز البيانات ومرافق اتصالات تكنولوجيا المعلومات
129	Translated (0%)	Data center locations and IT communication facilities shall be separated and protected from physical and environmental threats.	يجب فصل مواقع مراكز البيانات ومرافق اتصالات تكنولوجيا المعلومات وحمايتها من التهديدات المادية والبيئية.
130	Translated (0%)	Hazardous or combustible materials shall be securely stored separately and at a safe distance from any secure areas.	يجب تخزين المواد الخطرة أو القابلة للاحتراق بشكل آمن بشكل منفصل وعلى مسافة آمنة من أي مناطق آمنة.
131	Translated (0%)	All data center facilities are protected against fire, water damage, vandalism, and other threats known or likely to occur at their geographical locations.	جميع مرافق مراكز البيانات محمية من الحرائق والأضرار الناجمة عن المياه والتخريب والتهديدات الأخرى المعروفة أو التي من المحتمل أن تحدث في مواقعها الجغرافية.
132	Translated (0%)	Walls surrounding data centers are non-combustible and resistant to fire.	الجدران المحيطة بمراكز البيانات غير قابلة للاحتراق ومقاومة للحريق.
133	Translated (0%)	All openings to these walls (e.g., doors, ventilation ducts, etc.) should be self-closing and resistant to fire.	يجب أن تكون جميع فتحات هذه الجدران (مثل الأبواب وقنوات التهوية وما إلى ذلك) ذاتية الإغلاق ومقاومة للحريق.
134	Translated (0%)	All IT equipment in Al Hammadi Holding data centers always operate in a climate-controlled environment.	تعمل جميع معدات تكنولوجيا المعلومات في مراكز بيانات الحمادي القابضة دائمًا في بيئة يتم التحكم فيها بالمناخ.
135	Translated (0%)	Temperature and humidity sensors are installed to detect any environmental change and trigger an alarm.	يتم تركيب مستشعرات درجة الحرارة والرطوبة للكشف عن أي تغيير بيئي وإطلاق إنذار.
136	Translated (0%)	All necessary measures shall be in place to ensure that if a fire breaks out, it can be quickly controlled and suppressed.	يجب اتخاذ جميع التدابير اللازمة لضمان أنه في حالة اندلاع حريق، يمكن السيطرة عليه وإخماده بسرعة.
137	Translated (0%)	Specific measures shall be in place such as smoke detectors, automated fire suppression systems as well as fire extinguishers.	يجب أن تكون هناك تدابير محددة مثل كاشفات الدخان وأنظمة إخماد الحرائق الآلية وكذلك طفايات الحريق.
138	Translated (0%)	All data center personnel are trained in the use of portable fire extinguishers.	يتم تدريب جميع موظفي مركز البيانات على استخدام طفايات الحريق المحمولة.
139	Translated (0%)	Data centers shall be equipped with environmental controls to manage the environment such as water, power or temperature.	يجب أن تكون مراكز البيانات مجهزة بضوابط بيئية لإدارة البيئة مثل المياه أو الطاقة أو درجة الحرارة.
140	Translated (0%)	Uninterruptible Power Supplies (UPS) are used to provide short-term power when the power fails and to protect information systems from	لتوفير الطاقة على (UPS) يتم استخدام إمدادات الطاقة غير المنقطعة المدى القصير عند انقطاع التيار الكهربائي وحماية أنظمة المعلومات من

		voltage spikes and reductions.	.طفرات الجهد والتخفيضات
141	Translated (0%)	Where appropriate (risk-based approach), redundant electrical power supply (e.g., backup power generator) shall be in place to support information systems in the event of a prolonged power outage.	عند الاقتضاء (النهج القائم على المخاطر)، يجب أن يكون مصدر الطاقة الكهربائية الزائد (على سبيل المثال، مولد الطاقة الاحتياطية) في مكانه .لدعم أنظمة المعلومات في حالة انقطاع التيار الكهربائي لفترة طويلة
142	Translated (0%)	Decentralized computer rooms (IDFs/MDFs) containing network, wiring or communications equipment (e.g., wiring closets, etc.) are always locked with access restricted to authorized personnel only.	التي تحتوي على (IDFs/MDFs) يتم دائمًا قفل غرف الكمبيوتر اللامركزية ،شبكة أو أسلاك أو معدات اتصالات (على سبيل المثال، خزانات الأسلاك .وما إلى ذلك) مع تقييد الوصول إلى الموظفين المصرح لهم فقط
143	Translated (100%)	Signs are not to be posted on wiring closets, telephone rooms, data center facilities or other equipment components that would attract the attention of unauthorized individuals.	يُحظر تعليق لافتات على غرف الأسلاك، أو غرف الهواتف، أو مرافق مراكز البيانات، أو أي مكونات أخرى من المعدات قد تجذب انتباه الأفراد .غير المصرح لهم
144	Translated (0%)	Securing Offices, Rooms, and Facilities	تأمين المكاتب والغرف والمرافق
145	Translated (0%)	Al Hammadi Holding key facilities shall be sited to avoid access by the public.	يجب وضع المرافق الرئيسية لشركة الحمادي القابضة لتجنب وصول .الجمهور إليها
146	Translated (0%)	Where applicable, Al Hammadi Holding buildings shall be given minimum indication of their purpose, with no obvious signs, outside or inside the building, identifying the presence of IT operations.	حيثما ينطبق ذلك، يجب إعطاء مباني الحمادي القابضة الحد الأدنى من الإشارة إلى الغرض منها، مع عدم وجود علامات واضحة، خارج المبنى أو .داخله، تحدد وجود عمليات تكنولوجيا المعلومات
147	Translated (0%)	Al Hammadi Holding facilities shall be configured to prevent confidential information or activities from being visible and audible from the outside.	يجب تهيئة مرافق الحمادي القابضة لمنع المعلومات أو الأنشطة السرية .من أن تكون مرئية ومسموعة من الخارج
148	Translated (0%)	Electromagnetic shielding shall also be considered as appropriate.	.يجب أيضًا اعتبار التدريع الكهرومغناطيسي مناسبًا
149	Translated (0%)	Al Hammadi Holding directories and internal telephone books identifying locations of confidential IT operations facilities shall not be readily accessible to anyone unauthorized.	لا يجوز لأي شخص غير مصرح له الوصول بسهولة إلى أدلة الحمادي القابضة ودفاتر الهاتف الداخلية التي تحدد مواقع مرافق عمليات .تكنولوجيا المعلومات السرية
150	Translated (0%)	Protecting Against External and Environmental Threats	الحماية من التهديدات الخارجية والبيئية
151	Translated (0%)	Physical protection against natural disasters, malicious attacks or accidents shall be designed and applied.	يجب تصميم وتطبيق الحماية المادية ضد الكوارث الطبيعية أو الهجمات .الكيدية أو الحوادث
152	Translated (0%)	Al Hammadi Holding shall avoid damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster.	يجب على شركة الحمادي القابضة تجنب الأضرار الناجمة عن الحرائق والفيضانات والزلازل والانفجارات والاضطرابات المدنية وغيرها من .أشكال الكوارث الطبيعية أو التي من صنع الإنسان
153	Translated (0%)	Emergency procedures regarding the safe evacuation of areas or buildings shall be developed and documented.	يجب تطوير وتوثيق إجراءات الطوارئ المتعلقة بالإخلاء الآمن للمناطق أو .المباني
154	Translated (0%)	Locations shall contain emergency equipment, and this equipment shall be inspected on an annual basis or as defined by local regulations.	يجب أن تحتوي المواقع على معدات طوارئ، ويجب فحص هذه المعدات .على أساس سنوي أو على النحو المحدد في اللوائح المحلية
155	Translated (0%)	Environmental conditions shall be monitored for conditions that could adversely affect the operation of information processing locations.	يجب مراقبة الظروف البيئية للظروف التي يمكن أن تؤثر سلبًا على تشغيل .مواقع معالجة المعلومات
156	Translated (0%)	Alarms and detection equipment shall be monitored, periodically tested and maintained.	يجب مراقبة أجهزة الإنذار ومعدات الكشف واختبارها وصيانتها بشكل .دوري

157	Translated (0%)	IT and physical security equipment shall be protected from power failures and other disruptions.	يجب حماية معدات تكنولوجيا المعلومات والأمن المادي من انقطاع التيار الكهربائي والانقطاعات الأخرى.
158	Translated (0%)	Working In-Secure Areas	مناطق العمل غير الآمنة
159	Translated (0%)	Al Hammadi Holding personnel shall only be aware of the existence of, or activities within, a secure area on a need-to-know basis.	يجب أن يكون موظفو شركة الحمادي القابضة على دراية بوجود أو أنشطة داخل منطقة آمنة فقط على أساس الحاجة إلى المعرفة.
160	Translated (0%)	Unsupervised working in secure areas shall be avoided to prevent opportunities for malicious activities.	يجب تجنب العمل غير الخاضع للإشراف في المناطق الآمنة لمنع فرص الأنشطة الخبيثة.
161	Translated (0%)	Vacant secure areas shall be physically locked and periodically reviewed.	يجب إغلاق المناطق الآمنة الشاغرة فعليًا ومراجعتها بشكل دوري.
162	Translated (0%)	Photographic, video, audio or other recording equipment, such as cameras in mobile devices, shall not be allowed, unless authorized.	لا يُسمح بالتصوير الفوتوغرافي أو الفيديو أو الصوت أو معدات التسجيل الأخرى، مثل الكاميرات في الأجهزة المحمولة، ما لم يتم التصريح بذلك.
163	Translated (0%)	Delivery and Loading Areas	مناطق التسليم والتحميل
164	Translated (0%)	Access to Al Hammadi Holding delivery and loading areas from outside of the building shall be restricted to identified and authorized personnel.	يجب أن يقتصر الوصول إلى مناطق التسليم والتحميل التابعة لشركة الحمادي القابضة من خارج المبنى على الموظفين المحددين والمصرح لهم.
165	Translated (0%)	Al Hammadi Holding delivery and loading areas shall be designed so that supplies can be loaded and unloaded without delivery personnel gaining access to other parts of the building.	يجب تصميم مناطق التسليم والتحميل الخاصة بالحمادي القابضة بحيث يمكن تحميل الإمدادات وتفريغها دون أن يتمكن موظفو التسليم من الوصول إلى أجزاء أخرى من المبنى.
166	Translated (0%)	Al Hammadi Holding external doors of a delivery and loading areas shall be secured when the internal doors are opened.	يجب تأمين الأبواب الخارجية لشركة الحمادي القابضة لمناطق التسليم والتحميل عند فتح الأبواب الداخلية.
167	Translated (0%)	Incoming material shall be inspected and examined for explosives, chemicals or other hazardous materials, before it is moved from a delivery and loading area.	يجب فحص المواد الواردة وفحصها بحثًا عن المتفجرات أو المواد الكيميائية أو المواد الخطرة الأخرى، قبل نقلها من منطقة التسليم والتحميل.
168	Translated (0%)	Incoming materials shall be registered in accordance with asset management policy.	يجب تسجيل المواد الواردة وفقًا لسياسة إدارة الأصول.
169	Translated (0%)	Incoming and outgoing shipments shall be physically segregated, where possible.	يجب فصل الشحنات الواردة والصادرة ماديًا، حيثما أمكن ذلك.
170	Translated (0%)	Incoming material shall be inspected for evidence of end-route tampering.	يجب فحص المواد الواردة بحثًا عن أدلة على العبث بالطريق النهائي.
171	Translated (0%)	If such is discovered, it shall be immediately reported to security personnel.	إذا تم اكتشاف ذلك، يجب إبلاغ أفراد الأمن على الفور.
172	Translated (99%)	Equipment	المعدات
173	Translated (0%)	Equipment Siting and Protection	تحديد موقع المعدات وحمايتها
174	Translated (0%)	Al Hammadi Holding equipment shall be sited to minimize unnecessary access to work areas.	يجب وضع معدات الحمادي القابضة لتقليل الوصول غير الضروري إلى مناطق العمل.
175	Translated	Al Hammadi Holding IT operations facilities handling sensitive data shall	يجب وضع مرافق عمليات تكنولوجيا المعلومات في الحمادي القابضة

	(0%)	be positioned carefully to reduce the risk of information being viewed by unauthorized persons during their use.	التي تتعامل مع البيانات الحساسة بعناية لتقليل مخاطر عرض المعلومات من قبل أشخاص غير مصرح لهم أثناء استخدامها.
176	Translated (0%)	Al Hammadi Holding IT storage facilities shall be secured to avoid unauthorized access.	يجب تأمين مرافق تخزين تكنولوجيا المعلومات في شركة الحمادي القابضة لتجنب الوصول غير المصرح به.
177	Translated (0%)	Controls shall be adopted to minimize the risk of potential physical and environmental threats, e.g., theft, fire, explosives, smoke, water, dust.	يجب اعتماد ضوابط لتقليل مخاطر التهديدات المادية والبيئية المحتملة، على سبيل المثال، السرقة والحريق والمتفجرات والدخان والماء والغبار.
178	Translated (0%)	Guidelines for eating, drinking and smoking in proximity to IT operations facilities shall be established.	يجب وضع مبادئ توجيهية للأكل والشرب والتدخين بالقرب من مرافق عمليات تكنولوجيا المعلومات.
179	Translated (0%)	Environmental conditions, such as temperature and humidity, shall be monitored for conditions which could adversely affect the operation of IT facilities.	يجب مراقبة الظروف البيئية، مثل درجة الحرارة والرطوبة، بحثًا عن الظروف التي قد تؤثر سلبًا على تشغيل مرافق تكنولوجيا المعلومات.
180	Translated (0%)	Lightning protection shall be applied to all buildings.	يجب تطبيق الحماية من الصواعق على جميع المباني.
181	Translated (0%)	Lightning protection filters shall be fitted to all incoming power and communications lines.	يجب تركيب مرشحات الحماية من الصواعق على جميع خطوط الطاقة والاتصالات الواردة.
182	Translated (0%)	Supporting Utilities	المرافق الداعمة
183	Translated (0%)	Al Hammadi Holding IT equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	يجب حماية معدات تكنولوجيا المعلومات الخاصة بالحمادي القابضة من أعطال الطاقة وغيرها من الأعطال الناجمة عن الأعطال في المرافق الداعمة.
184	Translated (0%)	Supporting utilities (e.g., electricity, telecommunications, water supply, gas, sewage, ventilation and air conditioning) shall:	يجب على المرافق الداعمة (مثل الكهرباء والاتصالات السلكية واللاسلكية وإمدادات المياه والغاز والصرف الصحي والتهوية وتكييف الهواء):
185	Translated (0%)	conform to equipment manufacturer’s specifications.	مطابقة لمواصفات الشركة المصنعة للمعدات.
186	Translated (0%)	conform to local legal requirements.	يتوافق مع المتطلبات القانونية المحلية.
187	Translated (0%)	be appraised regularly for their capacity to meet business growth and interactions with other supporting utilities.	يتم تقييمها بانتظام لقدرتها على تلبية نمو الأعمال والتفاعلات مع المرافق الداعمة الأخرى.
188	Translated (0%)	be inspected and tested regularly to ensure their proper functioning.	يتم فحصها واختبارها بانتظام لضمان عملها بشكل صحيح.
189	Translated (0%)	Where necessary, be alarmed to detect malfunctions.	عند الضرورة، كن حذرًا للكشف عن الأعطال.
190	Translated (0%)	Where necessary, have multiple feeds with diverse physical routing.	عند الضرورة، احصل على خلاصات متعددة مع توجيه مادي متنوع.
191	Translated (0%)	Emergency lighting and communications shall be provided.	يجب توفير الإضاءة والاتصالات في حالات الطوارئ.
192	Translated (0%)	Emergency switches and valves to cut off power, water, gas or other utilities shall be located near emergency exits or equipment rooms.	يجب وضع مفاتيح وصمامات الطوارئ لقطع التيار الكهربائي أو الماء أو الغاز أو المرافق الأخرى بالقرب من مخارج الطوارئ أو غرف المعدات.
193	Translated	Where necessary, additional redundancy for network connectivity shall	عند الضرورة، يجب الحصول على احتياطي إضافي لاتصال الشبكة عن

	(0%)	be obtained by means of multiple routes from more than one utility provider.	.طريق طرق متعددة من أكثر من مزود خدمة واحد
194	Translated (0%)	Cabling Security	أمن الكابلات
195	Translated (0%)	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference, or damage.	يجب حماية كابلات الطاقة والاتصالات التي تحمل البيانات أو خدمات .المعلومات الداعمة من الاعتراض أو التداخل أو التلف
196	Translated (0%)	Power and telecommunications lines in IT operations facilities shall be underground, where possible, or subject to adequate alternative protection.	يجب أن تكون خطوط الطاقة والاتصالات السلكية واللاسلكية في مرافق عمليات تكنولوجيا المعلومات تحت الأرض، حيثما أمكن، أو تخضع لحماية .بديلة كافية
197	Translated (0%)	Power cables shall be segregated from communications cables to prevent interference.	.يجب فصل كابلات الطاقة عن كابلات الاتصالات لمنع التداخل
198	Translated (0%)	Al Hammadi Holding shall install armored conduit and locked rooms or boxes at inspection and termination points.	تقوم شركة الحمادي القابضة بتركيب قناة مدرعة وغرف أو صناديق .مغلقة عند نقاط التفتيش والإنهاء
199	Translated (0%)	Al Hammadi Holding shall use electromagnetic shielding to protect cables.	يجب على شركة الحمادي القابضة استخدام الدرع الكهرومغناطيسي .لحماية الكابلات
200	Translated (0%)	Al Hammadi Holding shall perform technical sweeps and physical inspections for unauthorized devices being attached to the cables.	يجب على شركة الحمادي القابضة إجراء عمليات المسح الفني والفحص .المادي للأجهزة غير المصرح بها التي يتم توصيلها بالكابلات
201	Translated (0%)	Al Hammadi Holding shall control access to patch panels and cable rooms.	يجب على شركة الحمادي القابضة التحكم في الوصول إلى لوحات .التصحيح وغرف الكابلات
202	Translated (100%)	Equipment Maintenance	صيانة المعدات
203	Translated (0%)	Al Hammadi Holding equipment shall be correctly maintained to ensure its continued availability and integrity.	يجب صيانة معدات شركة الحمادي القابضة بشكل صحيح لضمان .استمرار توافرها وسلامتها
204	Translated (0%)	Al Hammadi Holding equipment shall be maintained in accordance with the supplier's recommended service intervals and specifications.	يجب صيانة معدات شركة الحمادي القابضة وفقًا لفترات الخدمة .والمواصفات الموصى بها من المورد
205	Translated (0%)	Only authorized maintenance personnel shall carry out repairs and service equipment.	يجب على موظفي الصيانة المصرح لهم فقط إجراء الإصلاحات ومعدات .الخدمة
206	Translated (0%)	Records shall be kept of all suspected or actual faults, and of all preventive and corrective maintenance.	يجب الاحتفاظ بسجلات لجميع الأخطاء المشتبه بها أو الفعلية، وجميع .الصيانة الوقائية والتصحيحية
207	Translated (0%)	Appropriate equipment-specific cautions and controls shall be implemented when equipment is scheduled for maintenance.	يجب تنفيذ التحذيرات والضوابط الخاصة بالمعدات المناسبة عند جدولة .المعدات للصيانة
208	Translated (0%)	Where necessary, confidential information shall be cleared of the equipment, or the maintenance personnel shall be sufficiently cleared.	عند الضرورة، يجب مسح المعلومات السرية من المعدات، أو يجب مسح .موظفي الصيانة بشكل كافٍ
209	Translated (0%)	All maintenance requirements imposed by insurance policies shall be complied with.	.يجب الامتثال لجميع متطلبات الصيانة التي تفرضها وثائق التأمين
210	Translated (0%)	After maintenance, Al Hammadi Holding equipment shall be inspected to ensure that it has not been tampered with and does not malfunction.	بعد الصيانة، يجب فحص معدات شركة الحمادي القابضة للتأكد من عدم .العبث بها وعدم تعطلها
211	Translated	Removal of Assets	إزالة الأصول

	(0%)		
212	Translated (0%)	Al Hammadi Holding equipment, information or software shall not be taken off-site without prior authorization.	لا يجوز إخراج معدات أو معلومات أو برامج شركة الحمادي القابضة من الموقع دون إذن مسبق.
213	Translated (0%)	Al Hammadi Holding employees and external party users who have authority to permit off-site removal of assets shall be identified.	يجب تحديد موظفي شركة الحمادي القابضة والمستخدمين الخارجيين الذين لديهم صلاحية السماح بإزالة الأصول خارج الموقع.
214	Translated (0%)	Al Hammadi Holding assets shall be recorded as being removed off-site and recorded when returned.	يجب تسجيل أصول شركة الحمادي القابضة على أنها تم إزالتها خارج الموقع وتسجيلها عند إعادتها.
215	Translated (0%)	Time limits for asset removal shall be set and returns verified for compliance.	يجب تعيين حدود زمنية لإزالة الأصول والتحقق من إرجاعها للامتثال.
216	Translated (0%)	Regular spot checks shall be undertaken to detect unauthorized removal of assets and shall only be performed with authorization appropriate for the legal and regulatory requirements.	يجب إجراء عمليات تفتيش مفاجئة منتظمة للكشف عن الإزالة غير المصرح بها للأصول ويجب إجراؤها فقط بترخيص مناسب للمتطلبات القانونية والتنظيمية.
217	Translated (0%)	Security of Equipment and Assets Off-Premises	أمن المعدات والأصول خارج أماكن العمل
218	Translated (0%)	Security shall be applied to off-site assets against the different risks of working outside Al Hammadi Holding premises.	يجب تطبيق الضمان على الأصول خارج الموقع ضد المخاطر المختلفة للعمل خارج مباني شركة الحمادي القابضة.
219	Translated (0%)	Use of information storing and processing equipment outside Al Hammadi Holding's premises shall be authorized by management.	يجب أن تصرح الإدارة باستخدام معدات تخزين المعلومات ومعالجتها خارج مقر شركة الحمادي القابضة.
220	Translated (0%)	Equipment owned privately shall be inspected and authorized before being used on behalf of Al Hammadi Holding.	يجب فحص المعدات المملوكة للقطاع الخاص والتصريح بها قبل استخدامها نيابة عن شركة الحمادي القابضة.
221	Translated (0%)	Equipment taken off Al Hammadi Holding premises shall not be left unattended.	يجب عدم ترك المعدات المأخوذة من مباني شركة الحمادي القابضة دون مراقبة.
222	Translated (0%)	Manufacturers' instructions for protecting equipment shall always be observed.	يجب دائمًا مراعاة تعليمات الشركات المصنعة لحماية المعدات.
223	Translated (0%)	Al Hammadi Holding controls for working off-premises, such as teleworking and temporary sites, shall be determined and applied by a risk assessment process.	يجب تحديد وتطبيق ضوابط شركة الحمادي القابضة للعمل خارج أماكن العمل، مثل العمل عن بعد والمواقع المؤقتة، من خلال عملية تقييم المخاطر.
224	Translated (0%)	Al Hammadi Holding off-premises equipment transferred among individuals or external parties shall be logged and maintained to define the chain of custody for the equipment.	يجب تسجيل المعدات الخارجية لشركة الحمادي القابضة المنقولة بين الأفراد أو الأطراف الخارجية وصيانتها لتحديد سلسلة الحيازة للمعدات.
225	Translated (0%)	As seen appropriate, Al Hammadi Holding shall prevent certain employees from working off-site or restrict their use of portable IT equipment.	كما هو مناسب، يجب على شركة الحمادي القابضة منع بعض الموظفين من العمل خارج الموقع أو تقييد استخدامهم لمعدات تكنولوجيا المعلومات المحمولة.
226	Translated (0%)	Secure Disposal or Re-Use of Equipment	التخلص الآمن من المعدات أو إعادة استخدامها
227	Translated (0%)	Al Hammadi Holding Equipment shall be verified to ensure whether storage media is contained prior to disposal or re-use.	يجب التحقق من معدات الحمادي القابضة للتأكد من احتواء وسائط التخزين قبل التخلص منها أو إعادة استخدامها.
228	Translated (0%)	Damaging equipment containing storage media shall require a risk assessment to determine whether the items shall be physically	يجب أن تتطلب المعدات التالفة التي تحتوي على وسائط تخزين تقييمًا للمخاطر لتحديد ما إذا كان يجب تدمير العناصر ماديًا أو إرسالها للإصلاح

		destroyed, sent for repair, or discarded.	.أو التخلص منها
229	Translated (0%)	Al Hammadi Holding storage media containing confidential information shall be physically destroyed or the information shall be deleted or overwritten using non-retrievable techniques.	يجب تدمير وسائط تخزين شركة الحمادي القابضة التي تحتوي على معلومات سرية ماديًا أو يجب حذف المعلومات أو الكتابة فوقها باستخدام .تقنيات غير قابلة للاسترداد
230	Translated (0%)	Techniques for securely overwriting storage media shall be reviewed to make sure that they are applicable to the technology of the storage media.	يجب مراجعة تقنيات الكتابة فوق وسائط التخزين بشكل آمن للتأكد من .أنها قابلة للتطبيق على تكنولوجيا وسائط التخزين
231	Translated (0%)	Unattended User Equipment	معدات المستخدم غير المراقبة
232	Translated (0%)	All Al Hammadi Holding users shall be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection.	يجب أن يكون جميع مستخدمي شركة الحمادي القابضة على دراية بالمتطلبات والإجراءات الأمنية لحماية المعدات غير المراقبة، بالإضافة إلى .مسؤولياتهم عن تنفيذ هذه الحماية
233	Translated (0%)	Al Hammadi Holding users shall terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g., a password protected screen saver.	يجب على مستخدمي شركة الحمادي القابضة إنهاء الجلسات النشطة عند الانتهاء، ما لم يكن من الممكن تأمينها بواسطة آلية قفل مناسبة، على سبيل .المثال، شاشة التوقف المحمية بكلمة مرور
234	Translated (0%)	Al Hammadi Holding users shall log off from applications or network services when no longer needed.	يجب على مستخدمي شركة الحمادي القابضة تسجيل الخروج من .التطبيقات أو خدمات الشبكة عند عدم الحاجة إليها
235	Translated (0%)	Al Hammadi Holding users shall secure computers or mobile devices from unauthorized use by a key lock or an equivalent control, e.g., password access, when not in use.	يجب على مستخدمي شركة الحمادي القابضة تأمين أجهزة الكمبيوتر أو الأجهزة المحمولة من الاستخدام غير المصرح به بواسطة قفل مفتاح أو عنصر تحكم مكافئ، على سبيل المثال، الوصول إلى كلمة المرور، عندما لا .تكون قيد الاستخدام
236	Translated (0%)	Terminals shall be locked after a period of inactivity and a password shall be required to restart the session.	يجب قفل الوحدات الطرفية بعد فترة من عدم النشاط ويجب طلب كلمة .مرور لإعادة بدء الجلسة
237	Translated (0%)	Clear Desk and Clear Screen Policy	سياسة المكتب الواضح والشاشة الواضحة
238	Translated (0%)	Al Hammadi Holding clear desk and clear screen policy shall consider the information classifications, cultural aspects, and legal and contractual requirements.	يجب على مكتب الحمادي القابضة الواضح وسياسة الشاشة الواضحة مراعاة تصنيفات المعلومات والجوانب الثقافية والمتطلبات القانونية .والتعاقدية
239	Translated (0%)	Documents containing personal data must not be left unattended or in unsecured storage.	يجب عدم ترك المستندات التي تحتوي على بيانات شخصية دون مراقبة .أو في مخزن غير آمن
240	Translated (0%)	Al Hammadi Holding sensitive information shall be locked in a safe or cabinet when not required and when the office is vacated.	يجب تأمين المعلومات الحساسة لشركة الحمادي القابضة في خزنة أو .خزانة عندما لا تكون مطلوبة وعندما يتم إخلاء المكتب
241	Translated (0%)	Al Hammadi Holding computers and terminals shall be left logged off or protected with a screen and keyboard locking mechanism when unattended or not in use.	يجب ترك أجهزة الكمبيوتر والمحطات الطرفية التابعة لشركة الحمادي القابضة مغلقة أو محمية بآلية قفل الشاشة ولوحة المفاتيح عند عدم .مراقبتها أو عدم استخدامها
242	Translated (0%)	Unauthorized use of photocopiers and other reproduction technology (e.g., scanners, digital cameras) shall be prevented.	يجب منع الاستخدام غير المصرح به لآلات النسخ وغيرها من تقنيات .الاستنساخ (مثل الماسحات الضوئية والكاميرات الرقمية)
243	Translated (0%)	Al Hammadi Holding media containing sensitive, personalor classified information shall be removed from printers immediately.	يجب إزالة وسائط شركة الحمادي القابضة التي تحتوي على معلومات .حساسة أو شخصية أو سرية من الطابعات على الفور

244	Translated (0%)	Al Hammadi Holding shall use printers with PIN code function, so the originators are the only ones who can get their printouts and only when standing next to the printer.	يجب أن تستخدم شركة الحمادي القابضة طابعات مزودة بوظيفة رمز PIN، وبالتالي فإن المنشئين هم الوحيدون الذين يمكنهم الحصول على مطبوعاتهم وفقط عند الوقوف بجانب الطابعة.
245	Translated (100%)	Compliance and Adherence	الامتثال والالتزام
246	Translated (100%)	Al Hammadi Holding CEO shall ensure compliance with the cybersecurity policies and standards.	يضمن الرئيس التنفيذي لشركة الحمادي القابضة الامتثال لسياسات ومعايير الأمن السيبراني.
247	Translated (100%)	To ensure compliance, the Cybersecurity department will establish regular reporting by the Cybersecurity Manager, conduct periodic audits, or form a Cybersecurity Committee for oversight.	لضمان الامتثال، سينشئ قسم الأمن السيبراني نظامًا لتقديم تقارير منتظمة يُعدّها مدير الأمن السيبراني، ويجري عمليات تدقيق دورية، أو يشكل لجنة للأمن السيبراني للإشراف.
248	Translated (100%)	The CS manager shall ensure adherence to this policy.	يتعين على مدير الأمن السيبراني ضمان الالتزام بهذه السياسة.
249	Translated (100%)	All employees of Al Hammadi Holding must adhere to this policy.	على جميع موظفي شركة الحمادي القابضة الالتزام بهذه السياسة.
250	Translated (100%)	Violations of this policy may result in legal action in any jurisdiction or other measures as deemed appropriate by the Al Hammadi Holding.	قد تؤدي انتهاكات هذه السياسة إلى اتخاذ إجراءات قانونية في أي ولاية قضائية أو غيرها من التدابير التي تراها شركة الحمادي القابضة مناسبة.
251	Translated (100%)	Exceptions	الاستثناءات
252	Translated (100%)	Violation of cybersecurity policies and standards is prohibited unless a prior justified exception is obtained from the Cybersecurity Department or the Cybersecurity Steering Committee.	يُحظر انتهاك سياسات ومعايير الأمن السيبراني ما لم يتم الحصول على استثناء مبرر مسبق من إدارة الأمن السيبراني أو اللجنة التوجيهية للأمن السيبراني.
253	Translated (100%)	In case of a conflict, applicable legislative and regulatory requirements overrule Al Hammadi Holding policies and standards.	في حالة وجود تعارض، فإن المتطلبات التشريعية والتنظيمية المعمول بها تسود على سياسات ومعايير شركة الحمادي القابضة.
254	Translated (100%)	Revision	المراجعة
255	Translated (99%)	This policy is reviewed annually, or after major changes in Al Hammadi Holding’s organizational chart or infrastructure, and more frequently whenever required, to ensure it remains appropriate and current for Al Hammadi Holding, ISO 27001, and NCA requirements.	تخضع هذه السياسة لمراجعة سنوية، أو لإعادة التقييم بعد أي تغييرات جوهرية في الهيكل التنظيمي أو البنية التحتية لشركة الحمادي القابضة، إضافة إلى مراجعات دورية إضافية عند الضرورة، وذلك لضمان توافقها المستمر مع متطلبات شركة الحمادي القابضة، ومعيار آيزو ISO 27001:2022، وإرشادات الهيئة الوطنية للأمن السيبراني.
256	Translated (100%)	Approval Section	قسم الاعتماد
257	Translated (100%)	Prepared by:	إعداد:
258	Translated (100%)	Mr. Mohammed Alamer	السيد/ محمد العامر
259	Translated (100%)	GRC Cybersecurity Specialist	أخصائي حوكمة ومخاطر وامتثال في الأمن السيبراني
260	Translated	Name	الاسم

	(100%)		
261	Translated (100%)	Designation	المسمى الوظيفي
262	Translated (100%)	Signature	التوقيع
263	Translated (100%)	Date	التاريخ
264	Translated (100%)	Reviewed by:	راجعها:
265	Translated (100%)	Mr. Deepak Dasan	السيد/ ديباك داسان
266	Translated (100%)	IT Manager	مدير تكنولوجيا المعلومات
267	Translated (100%)	Name	الاسم
268	Translated (100%)	Designation	المسمى الوظيفي
269	Translated (100%)	Signature	التوقيع
270	Translated (100%)	Date	التاريخ
271	Translated (100%)	Reviewed by:	راجعها:
272	Translated (0%)	Faisal Alhzani	فيصل الحزاني
273	Translated (0%)	Security Manager	مدير الأمن
274	Translated (100%)	Name	الاسم
275	Translated (100%)	Designation	المسمى الوظيفي
276	Translated (100%)	Signature	التوقيع
277	Translated (100%)	Date	التاريخ
278	Translated (100%)	Reviewed by:	راجعها:
279	Translated (100%)	Ms. Mashael Alotaibi	السيدة/ مشاعل العتيبي

280	Translated (100%)	<1867>Cybersecurity </1867>Manager	<مدير <1867>الأمن السيبراني</1867/>
281	Translated (100%)	Name	الاسم
282	Translated (100%)	Designation	المسمى الوظيفي
283	Translated (100%)	Signature	التوقيع
284	Translated (100%)	Date	التاريخ
285	Translated (100%)	Approved by:	:اعتمدها
286	Translated (100%)	Dr. Abdulaziz Al Hammadi	الحمادي<Bold><Bold> د./ عبد العزيز</Bold></Bold> <Bold><Bold></Bold></Bold>
287	Translated (100%)	Chief Operating Officer	الرئيس التنفيذي للعمليات
288	Translated (100%)	Name	الاسم
289	Translated (100%)	Designation	المسمى الوظيفي
290	Translated (100%)	Signature	التوقيع
291	Translated (100%)	Date	التاريخ
292	Translated (100%)	Approved by:	:اعتمدها
293	Translated (100%)	Mr. Mohammad AlHammadi	السيد/ محمد الحمادي
294	Translated (100%)	Chief Executive Officer	الرئيس التنفيذي
295	Translated (100%)	Name	الاسم
296	Translated (100%)	Designation	المسمى الوظيفي
297	Translated (100%)	Signature	التوقيع
298	Translated (100%)	Date	التاريخ

Segment ID	Segment status	Source segment	Target segment
1	Translated (0%)	<3/> <26><6>HR Management Internal Organization <16/><20/>Policy</6></26>	سياسة التنظيم الداخلي لإدارة الموارد<3/> <26><6><16/><20/>البشرية</6></26>
2	Translated (100%)	Page <37><28/> of <36/></37>	صفحة <37></28><37> من <36/></37>
3	Translated (100%)	Al Hammadi Holding	شركة الحمادي القابضة
4	Translated (0%)	HR Management Internal Organization Policy	سياسة التنظيم الداخلي لإدارة الموارد البشرية
5	Translated (100%)	CYBERSECURITY DEPARTMENT	إدارة الأمن السيبراني
6	Translated (100%)	Policy ID	معرّف السياسة
7	Translated (100%)	AHH-CS-ISMS-016	AHH-CS-ISMS-016
8	Translated (100%)	Class	الفئة
9	Translated (100%)	Internal Release	إصدار داخلي
10	Not Translated (0%)		
11	Translated (100%)	V 1.0	V 1.0
12	Translated (100%)	Published at	نُشرت في
13	Translated (100%)	April 2025	أبريل 2025
14	Translated (100%)	Document Owner	المسؤول عن المستند
15	Translated (100%)	Cybersecurity <116>Department</116>	إدارة<116/> الأمن السيبراني<116>
16	Translated (100%)	Disclaimer	تنويه
17	Translated (100%)	The information contained in this document is the property of Al Hammadi Holding and must not be copied or communicated to a third party or used for any purpose other than that for which it is supplied, without the written consent of Al Hammadi Holding.	المعلومات الواردة في هذا المستند هي ملك لشركة الحمادي القابضة ولا يجوز نسخها أو إبلاغها إلى طرف ثالث أو استخدامها لأي غرض آخر غير الغرض الذي تم توفيرها من أجله، دون موافقة خطية من شركة الحمادي القابضة.

18	Translated (100%)	Contents	جدول المحتويات
19	Translated (100%)	Document Control	ضبط المستندات
20	Translated (100%)	Document Information	معلومات المستند
21	Translated (100%)	Synopsis	الملخص
22	Translated (100%)	Document Title:	:عنوان المستند
23	Translated (100%)	HR Management Internal Organization Policy	سياسة التنظيم الداخلي لإدارة الموارد البشرية
24	Translated (100%)	Document Status:	:حالة المستند
25	Translated (100%)	Approved	معتمد
26	Translated (100%)	Document Effective Date:	:تاريخ سريان المستند
27	Translated (0%)	April 202<227>5</227>	أبريل 2025
28	Translated (100%)	Document Issue Date:	:تاريخ إصدار المستند
29	Translated (100%)	April 202<242>5</242>	أبريل 2025
30	Translated (100%)	Document Next Revision Date:	:تاريخ المراجعة التالية للمستند
31	Translated (100%)	April 2026	أبريل 2026
32	Translated (100%)	Key contacts	جهات التواصل الرئيسية
33	Translated (100%)	Document Owner:	:المسؤول عن المستند
34	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
35	Translated (100%)	Approval Authority	جهة الاعتماد
36	Translated (100%)	Document Created by:	:مُنشئ المستند
37	Translated	Cybersecurity Department	إدارة الأمن السيبراني

	(100%)		
38	Translated (100%)	Document Reviewed by:	:راجع المستند
39	Translated (0%)	Al Hammadi Holding HR&CS&IT Manager	الحمادي القابضة مدير الموارد البشرية والخدمات الاستشارية وتكنولوجيا المعلومات
40	Translated (100%)	Document Approved by:	:اعتمد المستند
41	Translated (100%)	Al Hammadi Holding COO & CEO	الرئيس التنفيذي للعمليات والرئيس التنفيذي في شركة الحمادي القابضة
42	Translated (100%)	Note:	:ملاحظة
43	Translated (100%)	Any additional approval will be added in the document annex	تُضاف أي اعتمادات إضافية في ملحق المستند
44	Translated (100%)	Classification	التصنيف
45	Translated (100%)	<344>Company Internal</344> – to be shared with 3rd parties after consent of CS Manager	داخلي لاستخدام للشركة – <344/>يُسمح بمشاركته مع جهات<344> خارجية بعد موافقة مدير إدارة الأمن السيبراني
46	Translated (100%)	Version / Dates	الإصدار / التواريخ
47	Translated (100%)	Current Version:	:الإصدار الحالي
48	Translated (100%)	1.0	1.0
49	Translated (100%)	Date Published:	:تاريخ النشر
50	Translated (100%)	April 2025	أبريل 2025
51	Translated (100%)	Date of Next Review:	:تاريخ المراجعة التالية
52	Translated (100%)	April 2026	أبريل 2026
53	Translated (100%)	Document Changes	التغييرات على المستند
54	Translated (100%)	Date	التاريخ
55	Translated (100%)	Version	الإصدار
56	Translated (100%)	Document Owner	المسؤول عن المستند

57	Translated (100%)	Change Description	وصف التغيير
58	Translated (100%)	April 2025	أبريل 2025
59	Translated (100%)	1.0	1.0
60	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
61	Translated (100%)	Document Established	تم إنشاء المستند
62	Translated (100%)	Document Circulation	تعميم المستند
63	Translated (100%)	To	إلى
64	Translated (100%)	Date	التاريخ
65	Translated (100%)	Method	الطريقة
66	Translated (100%)	All Al Hammadi Staff	جميع موظفي شركة الحمادي
67	Translated (100%)	April 2025	أبريل 2025
68	Translated (100%)	Intranet Portal	بوابة الإنترانت
69	Translated (100%)	Objectives	الأهداف
70	Translated (0%)	The Policy Objective and Purpose of this policy at Al Hammadi Holding is to minimize the potential for the misuse or damage of the Al Hammadi's technological and digital information systems and assets.	يتمثل هدف السياسة والغرض منها في شركة الحمادي القابضة في تقليل احتمالية إساءة استخدام أو إتلاف أنظمة وأصول المعلومات التكنولوجية والرقمية في الحمادي.
71	Translated (0%)	This will be accomplished by verifying the integrity of Al Hammadi Holding personnel who are granted access to these information systems as part of their job responsibilities.	سيتم تحقيق ذلك من خلال التحقق من نزاهة موظفي شركة الحمادي القابضة الذين يتم منحهم حق الوصول إلى أنظمة المعلومات هذه كجزء من مسؤولياتهم الوظيفية.
72	Translated (0%)	Additionally, the aim is to ensure that all members of Al Hammadi Holding, including temporary personnel, trainees, and service providers in similar roles, fully comprehend their obligations and functions regarding information security.	بالإضافة إلى ذلك، فإن الهدف هو التأكد من أن جميع أعضاء شركة الحمادي القابضة، بما في ذلك الموظفين المؤقتين والمتدربين ومقدمي الخدمات في أدوار مماثلة، يفهمون تمامًا التزاماتهم ووظائفهم فيما يتعلق بأمن المعلومات.
73	Translated (0%)	They must be well-versed in the applicable disciplinary measures that will be taken in the event of non-compliance with the stipulations outlined in this policy.	يجب أن يكونوا على دراية جيدة بالإجراءات التأديبية المعمول بها التي سيتم اتخاذها في حالة عدم الامتثال للشروط الموضحة في هذه السياسة.

74	Translated (100%)	Scope	النطاق
75	Translated (0%)	This policy applies to all Al Hammadi Holding Cybersecurity Management operations, assets, and activities, including employees, trainees, service providers,<482> </482>and third parties under its control.	تنطبق هذه السياسة على جميع عمليات وأصول وأنشطة إدارة الأمن السيبراني لشركة الحمادي القابضة، بما في ذلك الموظفين والمتدربين ومقدمي الخدمات<482> <482/>والجهات الخارجية الخاضعة لسيطرتها.
76	Translated (100%)	Roles and Responsibilities	الأدوار والمسؤوليات
77	Translated (97%)	<494><492>Al Hammadi Holding </492></494><497>management is responsible for implementing, maintaining, and updating this policy with all its contents, in accordance with any changes in the Statement of Applicability, Al Hammadi Holding-SOA Document.</497>	تتحمل إدارة <494>شركة الحمادي القابضة <494/>مسؤولية تنفيذ هذه السياسة وحفظها وتحديثها بكامل محتوياتها، وذلك بما يتماشى مع أي تغييرات في بيان التطبيق الخاص بشركة الحمادي القابضة.
78	Translated (100%)	Principles	المبادئ
79	Translated (100%)	General Requirements	المتطلبات العامة
80	Translated (0%)	The Cybersecurity Management at Al Hammadi Holding, in coordination with the Human Resources Management and Financial Affairs, must define the specific cybersecurity requirements related to human resources before, during, and after recruitment.	يجب على إدارة الأمن السيبراني في شركة الحمادي القابضة، بالتنسيق مع إدارة الموارد البشرية والشؤون المالية، تحديد متطلبات الأمن السيبراني المحددة المتعلقة بالموارد البشرية قبل وأثناء وبعد التوظيف.
81	Translated (0%)	The Cybersecurity Management at Al Hammadi Holding, in collaboration with the Human Resources Management and Financial Affairs, should coordinate with all departments and divisions to ensure compliance with all policy clauses and their continuous implementation.	يجب على إدارة الأمن السيبراني في شركة الحمادي القابضة، بالتعاون مع إدارة الموارد البشرية والشؤون المالية، التنسيق مع جميع الإدارات والأقسام لضمان الامتثال لجميع بنود السياسة وتنفيذها المستمر.
82	Translated (0%)	All users of Al Hammadi Holding's information and technology assets must sign and agree to the terms and conditions of their employment contract.	على جميع مستخدمي الأصول المعلوماتية والتكنولوجية لشركة الحمادي القابضة التوقيع والموافقة على شروط وأحكام عقد العمل الخاص بهم.
83	Translated (0%)	These terms and conditions outline the personnel's responsibilities regarding adhering to cybersecurity controls within the Al Hammadi Holding environment.	تحدد هذه الشروط والأحكام مسؤوليات الموظفين فيما يتعلق بالالتزام بضوابط الأمن السيبراني داخل بيئة شركة الحمادي القابضة.
84	Translated (0%)	All personnel at Al Hammadi Holding bear the primary responsibility for continuous compliance with cybersecurity policies.	يتحمل جميع الموظفين في شركة الحمادي القابضة المسؤولية الأساسية عن الامتثال المستمر لسياسات الأمن السيبراني.
85	Translated (0%)	The Cybersecurity Management at Al Hammadi Holding must implement a cybersecurity awareness program for all personnel within the organization.	يجب على إدارة الأمن السيبراني في شركة الحمادي القابضة تنفيذ برنامج توعية بالأمن السيبراني لجميع الموظفين داخل المنظمة.
86	Translated (0%)	All necessary channels and measures should be provided to read, understand, and commit to the program by all personnel.	يجب توفير جميع القنوات والتدابير اللازمة لقراءة البرنامج وفهمه والالتزام به من قبل جميع الموظفين.
87	Translated (0%)	Support and technical development roles for sensitive systems at Al Hammadi Holding should be occupied by highly skilled individuals.	يجب أن يشغل أفراد ذوو مهارات عالية أدوار الدعم والتطوير الفني للأنظمة الحساسة في شركة الحمادي القابضة.

88	Translated (0%)	The Human Resources Management and Financial Affairs at Al Hammadi Holding must support the implementation of cybersecurity controls related to the employee lifecycle in the organization.	يجب على إدارة الموارد البشرية والشؤون المالية في شركة الحمادي القابضة دعم تنفيذ ضوابط الأمن السيبراني المتعلقة بدورة حياة الموظف في المؤسسة.
89	Translated (99%)	This includes:	وتشمل هذا ما يلي:
90	Translated (0%)	Pre-employment phase.	مرحلة ما قبل التوظيف.
91	Translated (0%)	During the employment period.	خلال فترة التوظيف.
92	Translated (0%)	Upon the termination or modification of employment contracts.	عند إنهاء أو تعديل عقود العمل.
93	Translated (0%)	Pre-Employment – Roles and Responsibilities	ما قبل التوظيف – الأدوار والمسؤوليات
94	Translated (0%)	HR department must conduct a background investigation check for any employee in Al Hammadi	يجب على قسم الموارد البشرية إجراء تحقيق في الخلفية لأي موظف في الحمادي
95	Translated (0%)	The Cybersecurity Management at Al Hammadi Holding must inform all newly affiliated individuals of the organization's cybersecurity roles and responsibilities through orientation sessions as part of the onboarding process (within the first week of joining, and no later than one month from the joining date).	يجب على إدارة الأمن السيبراني في شركة الحمادي القابضة إبلاغ جميع الأفراد المنتسبين حديثًا بأدوار ومسؤوليات الأمن السيبراني للمؤسسة من خلال جلسات توجيهية كجزء من عملية التأهيل (خلال الأسبوع الأول من الانضمام، وفي موعد لا يتجاوز شهرًا واحدًا من تاريخ الانضمام).
96	Translated (0%)	During Employment - Organizational Responsibilities	أثناء التوظيف - المسؤوليات التنظيمية
97	Translated (0%)	The Cybersecurity Management at Al Hammadi Holding, in collaboration with the Human Resources Management and Financial Affairs, must conduct regular training courses for awareness and to ensure that personnel at Al Hammadi Holding understand the cybersecurity policies and procedures within the organization.	يجب على إدارة الأمن السيبراني في شركة الحمادي القابضة، بالتعاون مع إدارة الموارد البشرية والشؤون المالية، إجراء دورات تدريبية منتظمة للتوعية والتأكد من أن الموظفين في شركة الحمادي القابضة يفهمون سياسات وإجراءات الأمن السيبراني داخل المنظمة.
98	Translated (0%)	The Cybersecurity Management at Al Hammadi Holding should coordinate with all departments within Al Hammadi Holding to ensure that personnel and external service providers.	يجب على إدارة الأمن السيبراني في شركة الحمادي القابضة التنسيق مع جميع الإدارات داخل شركة الحمادي القابضة لضمان أن الموظفين ومقدمي الخدمات الخارجيين.
99	Translated (0%)	Are aware of their roles and responsibilities related to data protection and cybersecurity.	على دراية بأدوارهم ومسؤولياتهم المتعلقة بحماية البيانات والأمن السيبراني.
100	Translated (0%)	The roles and responsibilities of Cybersecurity Management, Information Technology at Al Hammadi Holding, should encompass specific responsibilities to safeguard Al Hammadi Holding information and technology assets.	يجب أن تشمل أدوار ومسؤوليات إدارة الأمن السيبراني وتكنولوجيا المعلومات في شركة الحمادي القابضة مسؤوليات محددة لحماية أصول المعلومات والتكنولوجيا الخاصة بشركة الحمادي القابضة.
101	Translated (0%)	Possess a level of awareness regarding data security relevant to their roles and responsibilities within Al Hammadi Holding.	امتلاك مستوى من الوعي فيما يتعلق بأمن البيانات ذات الصلة بأدوارهم ومسؤولياتهم داخل شركة الحمادي القابضة.
102	Translated	Commit to the terms and conditions of employment, encompassing	الالتزام بشروط وأحكام التوظيف، بما في ذلك سياسات الأمن السيبراني

	(0%)	cybersecurity policies within Al Hammadi Holding and the acceptable use policy for information and technology assets, as well as appropriate workplace practices within Al Hammadi Holding.	داخل شركة الحمادي القابضة وسياسة الاستخدام المقبول لأصول المعلومات والتكنولوجيا، وكذلك ممارسات مكان العمل المناسبة داخل شركة الحمادي القابضة.
103	Translated (0%)	Undergo periodic cybersecurity awareness assessments and take appropriate measures to address any identified gaps.	الخضوع لتقييمات دورية للتوعية بالأمن السيبراني واتخاذ التدابير المناسبة لمعالجة أي ثغرات محددة.
104	Translated (0%)	Each department or division manager must ensure the attendance of all their employees in the cybersecurity training and awareness sessions whenever these are conducted.	على كل مدير إدارة أو قسم التأكد من حضور جميع موظفيه في جلسات التدريب والتوعية بالأمن السيبراني كلما أجريت هذه الجلسات.
105	Translated (0%)	<746>All department or division managers within </746><752><750>Al Hammadi Holding </750></752><755>should ensure that personnel and external service providers who offer services to their respective departments are well-versed in and committed to the cybersecurity policies before being granted access to Al Hammadi Holding information and technology assets.</755>	على <746>جميع مديري الإدارات أو الأقسام داخل شركة الحمادي القابضة</746><752><750> التأكد من أن الموظفين ومقدمي الخدمات</750></752><755> الخارجيين الذين يقدمون الخدمات لإداراتهم الخاصة على دراية جيدة بسياسات الأمن السيبراني والالتزام بها قبل منحهم حق الوصول إلى أصول المعلومات والتكنولوجيا الخاصة بشركة الحمادي القابضة. </755>
106	Translated (0%)	Al Hammadi Holding should establish procedures for job changes and the termination of employment contracts due to non-compliance with this policy, related policies, and non-disclosure agreements.	يجب على شركة الحمادي القابضة وضع إجراءات لتغيير الوظائف وإنهاء عقود العمل بسبب عدم الامتثال لهذه السياسة والسياسات ذات الصلة واتفاقيات عدم الإفصاح.
107	Translated (0%)	Cybersecurity requirements must also be considered during this process.	يجب أيضًا مراعاة متطلبات الأمن السيبراني خلال هذه العملية.
108	Translated (0%)	The Human Resources Management and Financial Affairs at Al Hammadi Holding should promptly notify Cybersecurity Management of any changes, new hires, or termination of services for personnel, contractors, or vendors interacting with Al Hammadi Holding.	يجب على إدارة الموارد البشرية والشؤون المالية في شركة الحمادي القابضة إخطار إدارة الأمن السيبراني على الفور بأي تغييرات أو تعيينات جديدة أو إنهاء خدمات للموظفين أو المقاولين أو البائعين الذين يتفاعلون مع شركة الحمادي القابضة.
109	Translated (0%)	The Information Technology at Al Hammadi Holding should immediately revoke access rights to information technology assets and data processing centers for employees whose employment contracts have ended.	يجب على شركة تكنولوجيا المعلومات في الحمادي القابضة أن تلغي على الفور حقوق الوصول إلى أصول تكنولوجيا المعلومات ومراكز معالجة البيانات للموظفين الذين انتهت عقود عملهم.
110	Translated (0%)	This action should be based on risk assessment factors, including the current value of available assets, employee responsibilities, whether the termination or change was initiated by the employee or the management, and the reason for the change or termination.	يجب أن يستند هذا الإجراء إلى عوامل تقييم المخاطر، بما في ذلك القيمة الحالية للأصول المتاحة، ومسؤوليات الموظف، وما إذا كان الإنهاء أو التغيير قد بدأه الموظف أو الإدارة، وسبب التغيير أو الإنهاء.
111	Translated (0%)	Maintaining Information Confidentiality	الحفاظ على سرية المعلومات
112	Translated (0%)	All temporary associates at Al Hammadi Holding must sign a confidentiality agreement as an indication of their commitment to safeguarding confidential and sensitive information within the organization.	على جميع الشركاء المؤقتين في شركة الحمادي القابضة التوقيع على اتفاقية سرية كدليل على التزامهم بحماية المعلومات السرية والحساسة داخل المنظمة.
113	Translated	This should be done before granting them access to critical and sensitive	يجب أن يتم ذلك قبل منحهم حق الوصول إلى المرافق الحيوية

	(0%)	facilities.	.والحساسة
114	Translated (0%)	The Human Resources Management and Financial Affairs at Al Hammadi Holding should review the confidentiality agreement whenever there are changes in services or contract terms.	يجب على إدارة الموارد البشرية والشؤون المالية في شركة الحمادي القابضة مراجعة اتفاقية السرية كلما حدثت تغييرات في الخدمات أو .شروط العقد
115	Translated (0%)	The Cybersecurity Management at Al Hammadi Holding should periodically review the confidentiality agreements, service contract agreements, or non-disclosure agreements signed with temporary associates.	يجب على إدارة الأمن السيبراني في شركة الحمادي القابضة مراجعة اتفاقيات السرية أو اتفاقيات عقود الخدمة أو اتفاقيات عدم الإفصاح .الموقعة مع الشركاء المؤقتين بشكل دوري
116	Translated (0%)	The Cybersecurity Management at Al Hammadi Holding should ensure that the confidentiality agreements include a commitment from the organization's associates not to use instant messaging applications, social communication platforms, or personal cloud storage services to create, store, or share enterprise data, except for secure messaging applications approved by the Cybersecurity Management.	يجب على إدارة الأمن السيبراني في شركة الحمادي القابضة التأكد من أن اتفاقيات السرية تتضمن التزامًا من شركاء المؤسسة بعدم استخدام تطبيقات المراسلة الفورية أو منصات التواصل الاجتماعي أو خدمات التخزين السحابي الشخصية لإنشاء بيانات المؤسسة أو تخزينها أو مشاركتها، باستثناء تطبيقات المراسلة الآمنة المعتمدة من قبل إدارة .الأمن السيبراني
117	Translated (0%)	Awareness, Education, and Training Programs	برامج التوعية والتثقيف والتدريب
118	Translated (0%)	The Cybersecurity Management should plan a cybersecurity awareness program for Al Hammadi Holding employees and collaborate with all stakeholders to develop an annual training plan.	يجب على إدارة الأمن السيبراني تخطيط برنامج توعية بالأمن السيبراني لموظفي شركة الحمادي القابضة والتعاون مع جميع أصحاب المصلحة .لوضع خطة تدريب سنوية
119	Translated (0%)	This plan should include specialized training focused on cybersecurity for associates of the Cybersecurity Management and the General Administration for IT and Technology.	يجب أن تتضمن هذه الخطة تدريبًا متخصصًا يركز على الأمن السيبراني لشركاء إدارة الأمن السيبراني والإدارة العامة لتقنية المعلومات .والتكنولوجيا
120	Translated (0%)	The cybersecurity training and awareness plan should be developed annually by the Cybersecurity Management to ensure the dissemination of up-to-date knowledge related to cybersecurity.	يجب تطوير خطة التدريب والتوعية بالأمن السيبراني سنويًا من قبل إدارة الأمن السيبراني لضمان نشر المعرفة الحديثة المتعلقة بالأمن .السيبراني
121	Translated (0%)	All suppliers or external parties who may have access to Al Hammadi Holding information assets and technology must be educated about the cybersecurity practices followed within the organization before being granted access privileges.	يجب توعية جميع الموردين أو الجهات الخارجية الذين قد يكون لديهم حق الوصول إلى أصول وتكنولوجيا معلومات شركة الحمادي القابضة حول ممارسات الأمن السيبراني المتبعة داخل المؤسسة قبل منحهم .امتيازات الوصول
122	Translated (0%)	The Human Resources Management and Financial Affairs should maintain attendance records for the training sessions.	يجب على إدارة الموارد البشرية والشؤون المالية الاحتفاظ بسجلات .الحضور للجلسات التدريبية
123	Translated (0%)	Various records and notes from the training session should be retained and provided to the Cybersecurity Management.	يجب الاحتفاظ بسجلات وملاحظات مختلفة من الجلسة التدريبية .وتقديمها إلى إدارة الأمن السيبراني
124	Translated (0%)	The Human Resources Management and Financial Affairs should periodically review training records to ensure that all relevant individuals have completed the required training and awareness programs according to the training or awareness plan.	يجب على إدارة الموارد البشرية والشؤون المالية مراجعة سجلات التدريب بشكل دوري للتأكد من أن جميع الأفراد المعنيين قد أكملوا برامج .التدريب والتوعية المطلوبة وفقًا لخطة التدريب أو التوعية
125	Translated (0%)	The Cybersecurity Management should develop cybersecurity awareness campaigns and data confidentiality campaigns using different means,	يجب على إدارة الأمن السيبراني تطوير حملات التوعية بالأمن السيبراني وحملات سرية البيانات باستخدام وسائل مختلفة، مثل رسائل البريد

		such as email messages, newsletters, etc., to educate users about their responsibilities towards cybersecurity.	الإلكتروني والنشرات الإخبارية وما إلى ذلك، لتثقيف المستخدمين حول مسؤولياتهم تجاه الأمن السيبراني.
126	Translated (0%)	The Cybersecurity Management should update and enhance the existing training and awareness plan based on reports of identified technical and digital security vulnerabilities throughout the year to increase the effectiveness of the activities conducted by Al Hammadi Holding employees in mitigating cyber risks.	يجب على إدارة الأمن السيبراني تحديث وتعزيز خطة التدريب والتوعية الحالية بناءً على تقارير نقاط الضعف الأمنية التقنية والرقمية المحددة على مدار العام لزيادة فعالية الأنشطة التي يقوم بها موظفو شركة الحمادي القابضة في التخفيف من المخاطر السيبرانية.
127	Translated (0%)	Disciplinary Procedures	الإجراءات التأديبية
128	Translated (0%)	The Cybersecurity Management should keep records of security breaches committed by all internal and external network users of Al Hammadi Holding.	يجب أن تحتفظ إدارة الأمن السيبراني بسجلات الخروقات الأمنية التي يرتكبها جميع مستخدمي الشبكة الداخلية والخارجية لشركة الحمادي القابضة.
129	Translated (0%)	The Human Resources Management and Financial Affairs and other department managers should ensure that associates, suppliers, and external parties are aware of the official disciplinary procedures that may be taken against them in case of violation of Al Hammadi Holding cybersecurity policies or participation in any form of security breaches.	يجب على إدارة الموارد البشرية والشؤون المالية ومديري الإدارات الآخرين التأكد من أن الشركاء والموردين والأطراف الخارجية على دراية بالإجراءات التأديبية الرسمية التي يمكن اتخاذها ضدهم في حالة انتهاك سياسات الأمن السيبراني لشركة الحمادي القابضة أو المشاركة في أي شكل من أشكال الخروقات الأمنية.
130	Translated (0%)	Official disciplinary procedures should be provided for a graduated response, considering factors such as:	يجب توفير إجراءات تأديبية رسمية للاستجابة التدريجية، مع مراعاة عوامل مثل:
131	Translated (0%)	The nature of the breach - type of data case or incident and its impact on cybersecurity.	طبيعة الخرق - نوع حالة أو واقعة البيانات وتأثيرها على الأمن السيبراني.
132	Translated (0%)	The severity of the breach - the impact of the breach on Al Hammadi Holding reputation, financial operations, etc.	شدة الخرق - تأثير الخرق على سمعة شركة الحمادي القابضة والعمليات المالية وما إلى ذلك.
133	Translated (0%)	Asset Returns	عوائد الأصول
134	Translated (0%)	The General Administration for IT and Technology should facilitate the return of assets and the removal of access rights for departing employees, contractors, and service providers from external parties on their last day.	يجب على الإدارة العامة لتقنية المعلومات والتكنولوجيا تسهيل إعادة الأصول وإزالة حقوق الوصول للموظفين المغادرين والمقاولين ومقدمي الخدمات من الأطراف الخارجية في آخر يوم لهم.
135	Translated (0%)	This should be done within 24 hours of the timeline, and the Cybersecurity Management should be notified.	يجب أن يتم ذلك في غضون 24 ساعة من الجدول الزمني، ويجب إخطار إدارة الأمن السيبراني.
136	Translated (0%)	The Cybersecurity Management should ensure the periodic removal of access rights to digital networks for departing employees, and ensure that assets have been handled in accordance with approved procedures.	يجب أن تضمن إدارة الأمن السيبراني الإزالة الدورية لحقوق الوصول إلى الشبكات الرقمية للموظفين المغادرين، والتأكد من التعامل مع الأصول وفقًا للإجراءات المعتمدة.
137	Translated (0%)	Access Rights Revocation	إلغاء حقوق الوصول
138	Translated (0%)	The Cybersecurity Management and the General Administration for IT and Technology should ensure the revocation of all access rights for information systems in Al Hammadi Holding in a timely manner when	يجب على إدارة الأمن السيبراني والإدارة العامة لتقنية المعلومات والتكنولوجيا ضمان إلغاء جميع حقوق الوصول لأنظمة المعلومات في شركة الحمادي القابضة في الوقت المناسب عندما يقوم الموظفون أو

		employees, contract workers, or parties under agreement change or terminate their engagement.	.العمال المتعاقدون أو الأطراف بموجب اتفاقية بتغيير أو إنهاء مشاركتهم
139	Translated (0%)	A termination of engagement form should be signed by the relevant management after ensuring the removal of access rights from all relevant systems and applications.	يجب توقيع نموذج إنهاء المشاركة من قبل الإدارة المعنية بعد ضمان .إزالة حقوق الوصول من جميع الأنظمة والتطبيقات ذات الصلة
140	Translated (0%)	Physical access rights to work areas and access to sensitive applications and systems should be disabled by the General Administration for IT and Technology.	يجب تعطيل حقوق الوصول المادي إلى مناطق العمل والوصول إلى التطبيقات والأنظمة الحساسة من قبل الإدارة العامة لتقنية المعلومات .والتكنولوجيا
141	Translated (0%)	The Cybersecurity Management, in collaboration with the General Administration for IT and Technology, should review access rights for information systems and data centers when reassigning or relocating employees to different Al Hammadi Holding locations and initiate appropriate procedures.	يجب على إدارة الأمن السيبراني، بالتعاون مع الإدارة العامة لتقنية المعلومات والتكنولوجيا، مراجعة حقوق الوصول لأنظمة المعلومات ومراكز البيانات عند إعادة تعيين أو نقل الموظفين إلى مواقع الحمادي .القابضة المختلفة وبدء الإجراءات المناسبة
142	Translated (0%)	(For example, reissuing keys and identity cards, closing old accounts and creating new ones, changing access rights to sensitive applications and systems).	على سبيل المثال، إعادة إصدار المفاتيح وبطاقات الهوية، وإغلاق) الحسابات القديمة وإنشاء حسابات جديدة، وتغيير حقوق الوصول إلى .(التطبيقات والأنظمة الحساسة
143	Translated (100%)	Compliance and Adherence	الامتثال والالتزام
144	Translated (100%)	Al Hammadi Holding CEO shall ensure compliance with the cybersecurity policies and standards.	يضمن الرئيس التنفيذي لشركة الحمادي القابضة الامتثال لسياسات .ومعايير الأمن السيبراني
145	Translated (100%)	To ensure compliance, the Cybersecurity department will establish regular reporting by the Cybersecurity Manager, conduct periodic audits, or form a Cybersecurity Steering Committee for oversight.	لضمان الامتثال، سينشئ قسم الأمن السيبراني نظامًا لتقديم تقارير منتظمة يُعدّها مدير الأمن السيبراني، ويجري عمليات تدقيق دورية، أو .يشكل لجنة توجيهية للأمن السيبراني للإشراف
146	Translated (100%)	The CS manager shall ensure adherence to this policy.	.يتعين على مدير الأمن السيبراني ضمان الالتزام بهذه السياسة
147	Translated (100%)	All employees of Al Hammadi Holding must adhere to this policy.	.على جميع موظفي شركة الحمادي القابضة الالتزام بهذه السياسة
148	Translated (100%)	Violations of this policy may result in legal action in any jurisdiction or other measures as deemed appropriate by the Al Hammadi Holding.	قد تؤدي انتهاكات هذه السياسة إلى اتخاذ إجراءات قانونية في أي ولاية .قضائية أو غيرها من التدابير التي تراها شركة الحمادي القابضة مناسبة
149	Translated (100%)	Exceptions	الاستثناءات
150	Translated (100%)	Violation of cybersecurity policies and standards is prohibited unless a prior justified exception is obtained from the Cybersecurity Department or the Cybersecurity Steering Committee.	يُحظر انتهاك سياسات ومعايير الأمن السيبراني ما لم يتم الحصول على استثناء مبرر مسبق من إدارة الأمن السيبراني أو اللجنة التوجيهية للأمن .السيبراني
151	Translated (100%)	In case of a conflict, applicable legislative and regulatory requirements overrule Al Hammadi Holding policies and standards.	في حالة وجود تعارض، فإن المتطلبات التشريعية والتنظيمية المعمول .بها تسود على سياسات ومعايير شركة الحمادي القابضة
152	Translated (100%)	Revision	المراجعة
153	Translated	This policy is reviewed annually, after major changes in Al Hammadi	تخضع هذه السياسة لمراجعة سنوية، ولإعادة التقييم بعد أي تغييرات

	(100%)	Holding’s organizational chart or infrastructure, and more frequently whenever required, to ensure it remains appropriate and current for Al Hammadi Holding, ISO 27001, and NCA requirements.	،جوهرية في الهيكل التنظيمي أو البنية التحتية لشركة الحمادي القابضة إضافة إلى مراجعات دورية إضافية عند الضرورة، وذلك لضمان توافقها ISO المستمر مع متطلبات شركة الحمادي القابضة، ومعيار آيزو .وإرشادات الهيئة الوطنية للأمن السيبراني ،27001:2022
154	Translated (100%)	Approval Section	قسم الاعتماد
155	Translated (100%)	Prepared by:	:إعداد
156	Translated (100%)	Mr. Mohammed Alamer	السيد/ محمد العامر
157	Translated (100%)	GRC Cybersecurity Specialist	أخصائي حوكمة ومخاطر وامتثال في الأمن السيبراني
158	Translated (100%)	Name	الاسم
159	Translated (100%)	Designation	المسمى الوظيفي
160	Translated (100%)	Signature	التوقيع
161	Translated (100%)	Date	التاريخ
162	Translated (100%)	Reviewed by:	:راجعها
163	Translated (100%)	Mr. Deepak Dasan	السيد/ ديباك داسان
164	Translated (100%)	IT Manager	مدير تكنولوجيا المعلومات
165	Translated (100%)	Name	الاسم
166	Translated (100%)	Designation	المسمى الوظيفي
167	Translated (100%)	Signature	التوقيع
168	Translated (100%)	Date	التاريخ
169	Translated (100%)	Reviewed by:	:راجعها
170	Translated (100%)	Mr. Majid Al Nahdi	السيد/ ماجد النهدي
171	Translated	Human Resources Manager	مدير الموارد البشرية

	(100%)		
172	Translated (100%)	Name	الاسم
173	Translated (100%)	Designation	المسمى الوظيفي
174	Translated (100%)	Signature	التوقيع
175	Translated (100%)	Date	التاريخ
176	Translated (100%)	Reviewed by:	راجعها:
177	Translated (100%)	Ms. Mashael Alotaibi	السيدة/ مشاعل العتيبي
178	Translated (100%)	Cybersecurity Manager	مدير الأمن السيبراني
179	Translated (100%)	Name	الاسم
180	Translated (100%)	Designation	المسمى الوظيفي
181	Translated (100%)	Signature	التوقيع
182	Translated (100%)	Date	التاريخ
183	Translated (100%)	Approved by:	اعتمدها:
184	Translated (100%)	Dr. Abdulaziz Al Hammadi	الحمادي<Bold><Bold></Bold></Bold> د./ عبد العزيز<Bold><Bold></Bold></Bold>
185	Translated (100%)	Chief Operating Officer	الرئيس التنفيذي للعمليات
186	Translated (100%)	Name	الاسم
187	Translated (100%)	Designation	المسمى الوظيفي
188	Translated (100%)	Signature	التوقيع
189	Translated (100%)	Date	التاريخ
190	Translated (100%)	Approved by:	اعتمدها:

191	Translated (100%)	Mr. Mohammad AlHammadi	السيد/ محمد الحمادي
192	Translated (100%)	Chief Executive Officer	الرئيس التنفيذي
193	Translated (100%)	Name	الاسم
194	Translated (100%)	Designation	المسمى الوظيفي
195	Translated (100%)	Signature	التوقيع
196	Translated (100%)	Date	التاريخ

Segment ID	Segment status	Source segment	Target segment
1	Translated (0%)	<3/><7/><26><10>Email Security Policy<20/> </10></26>	<3/><7/><26><10>26/><10/> </20>سياسة أمان البريد الإلكتروني<
2	Translated (100%)	Page <37><28/> of <36/></37>	37/></36> من </28><37>صفحة<
3	Translated (100%)	Al Hammadi Holding	شركة الحمادي القابضة
4	Translated (0%)	Email Security Policy	سياسة أمان البريد الإلكتروني
5	Translated (100%)	CYBERSECURITY DEPARTMENT	إدارة الأمن السيبراني
6	Translated (100%)	Policy ID	معرّف السياسة
7	Translated (100%)	AHH-CS-ISMS-017	AHH-CS-ISMS-017
8	Translated (100%)	Class	الفئة
9	Translated (100%)	Internal Release	إصدار داخلي
10	Not Translated (0%)		
11	Translated (100%)	V1.0	V1.0
12	Translated (100%)	Published at	نُشرت في
13	Translated (100%)	April 2025	أبريل 2025
14	Translated (100%)	Document Owner	المسؤول عن المستند
15	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
16	Translated (100%)	Disclaimer	تنويه
17	Translated (99%)	The information contained in this document is the property of Hammadi Holdings and must not be copied or communicated to a third party or used for any purpose other than that for which it is supplied, without the written consent of Al Hammadi	المعلومات الواردة في هذا المستند هي ملك لشركة الحمادي القابضة ولا يجوز نسخها أو إبلاغها إلى طرف ثالث أو استخدامها لأي غرض آخر غير الغرض الذي تم توفيرها من أجله، دون موافقة خطية من شركة الحمادي القابضة.

		Holding.	
18	Translated (100%)	Contents	جدول المحتويات
19	Translated (100%)	Document Control	ضبط المستندات
20	Translated (100%)	Document Information	معلومات المستند
21	Translated (100%)	Synopsis	الملخص
22	Translated (100%)	Document Title:	:عنوان المستند
23	Translated (100%)	Email Security Policy	سياسة أمان البريد الإلكتروني
24	Translated (100%)	Document Status:	:حالة المستند
25	Translated (100%)	Approved	معتمد
26	Translated (100%)	Document Effective Date:	:تاريخ سريان المستند
27	Translated (100%)	April 2025	أبريل 2025
28	Translated (100%)	Document Issue Date:	:تاريخ إصدار المستند
29	Translated (100%)	April 2025	أبريل 2025
30	Translated (100%)	Document Next Revision Date:	:تاريخ المراجعة التالية للمستند
31	Translated (100%)	April 2026	أبريل 2026
32	Translated (100%)	Key contacts	جهات التواصل الرئيسية
33	Translated (100%)	Document Owner:	:المسؤول عن المستند
34	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
35	Translated (100%)	Approval Authority	جهة الاعتماد
36	Translated (100%)	Document Created by:	:مُنشئ المستند

37	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
38	Translated (100%)	Document Reviewed by:	راجع المستند:
39	Translated (100%)	Al Hammadi Holding CS &IT Managers	مديرو الأمن السيبراني وتكنولوجيا المعلومات في شركة الحمادي القابضة
40	Translated (100%)	Document Approved by:	اعتمد المستند:
41	Translated (100%)	Al Hammadi Holding COO & CEO	الرئيس التنفيذي للعمليات والرئيس التنفيذي في شركة الحمادي القابضة
42	Translated (100%)	Note:	ملاحظة:
43	Translated (100%)	Any additional approval will be added in the document annex	تُضاف أي اعتمادات إضافية في ملحق المستند
44	Translated (100%)	Classification	التصنيف
45	Translated (100%)	<254>Company Internal – </254>to be shared with 3rd parties after consent of CS Manager	داخلي لاستخدام للشركة<254> – <254/><254/>يُسمح بمشاركته مع<254> جهات خارجية بعد موافقة مدير إدارة الأمن السيبراني
46	Translated (100%)	Version / Dates	الإصدار / التواريخ
47	Translated (100%)	Current Version:	الإصدار الحالي:
48	Translated (100%)	V1.0	V1.0
49	Translated (100%)	Date Published:	تاريخ النشر:
50	Translated (100%)	April 2025	أبريل 2025
51	Translated (100%)	Date of Next Review:	تاريخ المراجعة التالية:
52	Translated (100%)	April <281>2026</281>	<أبريل <281>2026<281/>
53	Translated (100%)	Document Changes	التغييرات على المستند
54	Translated (100%)	Date	التاريخ
55	Translated (100%)	Version	الإصدار
56	Translated	Document Owner	المسؤول عن المستند

	(100%)		
57	Translated (100%)	Change Description	وصف التغيير
58	Translated (100%)	April 2025	أبريل 2025
59	Translated (100%)	1.0	1.0
60	Translated (100%)	Cybersecurity Department	إدارة الأمن السيبراني
61	Translated (0%)	Document Created	تم إنشاء المستند
62	Translated (100%)	Document Circulation	تعميم المستند
63	Translated (100%)	To	إلى
64	Translated (100%)	Date	التاريخ
65	Translated (100%)	Method	الطريقة
66	Translated (0%)	All IT Staff	جميع موظفي تكنولوجيا المعلومات
67	Translated (100%)	April 2025	أبريل 2025
68	Translated (100%)	Intranet Portal	بوابة الإنترانت
69	Translated (100%)	All Al Hammadi Staff	جميع موظفي شركة الحمادي
70	Translated (100%)	April 2025	أبريل 2025
71	Translated (100%)	Intranet Portal	بوابة الإنترانت
72	Translated (100%)	Objectives	الأهداف
73	Translated (0%)	This policy establishes the necessary controls and practices to ensure the secure use of email systems, protect against threats such as phishing, spam, malware, and data leakage, and ensure compliance with:	تحدد هذه السياسة الضوابط والممارسات اللازمة لضمان الاستخدام الآمن لأنظمة البريد الإلكتروني، والحماية من التهديدات مثل التصيد الاحتيالي والبريد المزعج والبرامج الضارة وتسرب البيانات، وضمان الامتثال لما يلي:
74	Translated (100%)	NCA ECC-2:2024:	معيار الهيئة الوطنية للأمن السيبراني رقم ECC-2:2024:

75	Translated (0%)	2-4 Email Protection.	2-4 حماية البريد الإلكتروني.
76	Translated (100%)	Scope	النطاق
77	Translated (0%)	This policy applies to all employees, contractors, third-party users, and any individual granted access to the organization’s email systems, whether cloud-based or on-premises.	تنطبق هذه السياسة على جميع الموظفين والمقاولين والمستخدمين الخارجيين وأي فرد ممنوح حق الوصول إلى أنظمة البريد الإلكتروني الخاصة بالمؤسسة، سواء كانت سحابية أو محلية.
78	Translated (100%)	Roles and Responsibilities	الأدوار والمسؤوليات
79	Translated (100%)	Al Hammadi Holding Cybersecurity and IT Departments are responsible for maintaining this policy with all its contents, in accordance with any changes in the applicable regulations and legislation, where:	تتولى إدارات الأمن السيبراني وتكنولوجيا المعلومات في شركة الحمادي القابضة مسؤولية حفظ هذه السياسة بجميع محتوياتها، وفقًا لأي تغييرات تطرأ على اللوائح والتشريعات المعمول بها، وذلك وفقًا لما يلي:
80	Translated (0%)	IT Department:	قسم تكنولوجيا المعلومات:
81	Translated (0%)	Configure and maintain email security systems	تكوين أنظمة أمان البريد الإلكتروني وصيانتها
82	Translated (0%)	Cybersecurity Team:	فريق الأمن السيبراني:
83	Translated (0%)	Enforce policy compliance, monitor email threats and policy review and update	فرض الامتثال للسياسة، ومراقبة تهديدات البريد الإلكتروني ومراجعة السياسة وتحديثها
84	Translated (0%)	All Users:	جميع المستخدمين:
85	Translated (0%)	Comply with email use guidelines, report suspicious emails	الامتثال لإرشادات استخدام البريد الإلكتروني، والإبلاغ عن رسائل البريد الإلكتروني المشبوهة
86	Translated (0%)	<406>Policy </406><407/>Statement	<406>بيان</406> السياسة <407/>
87	Translated (0%)	Administrative Control of E-Mail System	الرقابة الإدارية على نظام البريد الإلكتروني
88	Translated (0%)	E-mail administrator shall ensure that the e-mail IDs of Al Hammadi Holding employees, contractors and third-party staff are categorized separately, and these shall be reviewed at least once a year.	يجب على مسؤول البريد الإلكتروني التأكد من أن معرفات البريد الإلكتروني لموظفي شركة الحمادي القابضة والمقاولين وموظفي الطرف الثالث مصنفة بشكل منفصل، ويجب مراجعتها مرة واحدة على الأقل في السنة.
89	Translated (0%)	Non-essential and higher-order ports as well as vendor-default services that are not necessary for delivering email service shall be disabled.	يجب تعطيل المنافذ غير الأساسية والأعلى رتبة وكذلك الخدمات الافتراضية للبائع غير الضرورية لتقديم خدمة البريد الإلكتروني.
90	Translated (0%)	The e-mail system shall be configured not to allow the auto-forwarding of e-mails.	يجب تكوين نظام البريد الإلكتروني بحيث لا يسمح بإعادة التوجيه التلقائي للبريد الإلكتروني.
91	Translated	The roles for the administrative and maintenance activities	يجب تحديد أدوار الأنشطة الإدارية والصيانة.

	(0%)	shall be identified.	
92	Translated (0%)	Access rights to these roles shall be granted based on “need-to-know” and “need-to-have” principles.	تُمنح حقوق الوصول إلى هذه الأدوار بناءً على مبادئ "الحاجة إلى المعرفة" و "الحاجة إلى امتلاك".
93	Translated (0%)	The e-mail system shall be kept up to date with the latest service pack or patches.	يجب تحديث نظام البريد الإلكتروني بأحدث حزمة خدمة أو تصحيحات.
94	Translated (0%)	The patches shall be applied as per the Change Management Process.	يجب تطبيق التصحيحات وفقًا لعملية إدارة التغيير.
95	Translated (0%)	Al Hammadi Holding e-mail systems shall be scanned for vulnerabilities at least once in six months and undergo penetration tests at least once a year.	يجب فحص أنظمة البريد الإلكتروني لشركة الحمادي القابضة بحثًا عن نقاط الضعف مرة واحدة على الأقل كل ستة أشهر والخضوع لاختبارات الاختراق مرة واحدة على الأقل في السنة.
96	Translated (0%)	Individual as well as group e-mail IDs of the users shall be created, as per the registration process defined in Access Management Process.	يجب إنشاء معرفات بريد إلكتروني فردية وجماعية للمستخدمين، وفقًا لعملية التسجيل المحددة في عملية إدارة الوصول.
97	Translated (0%)	The requirements for e-mail and web browser protection, (e.g., email filtering for spam and phishing protection, multi-factor authentication, backup and archive for emails, protection against advanced persistent threats, and untrusted websites) shall be implemented.	يجب تنفيذ متطلبات حماية البريد الإلكتروني ومتصفح الويب، (على سبيل المثال، تصفية البريد الإلكتروني للحماية من الرسائل غير المرغوب فيها والتصيد الاحتيالي، والمصادقة متعددة العوامل، والنسخ الاحتياطي والأرشفة لرسائل البريد الإلكتروني، والحماية من التهديدات المستمرة المتقدمة، ومواقع الويب غير الموثوقة).
98	Translated (0%)	The access to unauthorized web-based email services, (e.g. through firewall rules, network-based URL filters) shall be restricted.	يجب تقييد الوصول إلى خدمات البريد الإلكتروني غير المصرح بها المستندة إلى الويب، (على سبيل المثال من خلال قواعد جدار الحماية، وعوامل تصفية عناوين URL المستندة إلى الشبكة).
99	Translated (0%)	The requirements for e-mail and web browser protection shall be measured, reviewed, and optimized, periodically.	يجب قياس متطلبات حماية البريد الإلكتروني ومتصفح الويب ومراجعتها وتحسينها بشكل دوري.
100	Translated (0%)	The email service domains shall be validated using the sender policy framework.	يجب التحقق من صحة نطاقات خدمة البريد الإلكتروني باستخدام إطار سياسة المرسل.
101	Translated (0%)	Email traffic shall be encrypted during transit.	يجب تشفير حركة مرور البريد الإلكتروني أثناء النقل.
102	Translated (0%)	All email services (on-premises and cloud-based) must be secured against unauthorized access, interception, or compromise.	يجب تأمين جميع خدمات البريد الإلكتروني (المحلية والسحابية) ضد الوصول غير المصرح به أو الاعتراض أو الاختراق.
103	Translated (0%)	Al Hammadi Holding shall secure email services by implementing controls such as Sender Policy Framework (SPF), DMARC, and DKIM.	يجب على شركة الحمادي القابضة تأمين خدمات البريد الإلكتروني من خلال تنفيذ الضوابط مثل إطار سياسة المرسل (SPF) و DMARC و DKIM.
104	Translated (0%)	Electronic signatures shall be implemented wherever required legally and contractually.	يتم تنفيذ التوقيعات الإلكترونية حيثما كان ذلك مطلوبًا من الناحية القانونية والتعاقدية.
105	Translated (0%)	Email systems shall be configured in accordance with cybersecurity hardening standards approved by the Al Hammadi holding's cybersecurity governance.	يجب تكوين أنظمة البريد الإلكتروني وفقًا لمعايير تشديد الأمن السيبراني المعتمدة من قبل حوكمة الأمن السيبراني في شركة الحمادي القابضة.
106	Translated	Stronger levels of authentication shall be implemented to	يجب تنفيذ مستويات أقوى من المصادقة للتحكم في الوصول إلى خدمات المراسلة

	(0%)	control access to electronic messaging services from publicly accessible networks (remote and webmail access) for example restrictions based on geographical location etc.	الإلكترونية من الشبكات المتاحة للجمهور (الوصول عن بعد والبريد الإلكتروني) على سبيل المثال القيود القائمة على الموقع الجغرافي وما إلى ذلك.
107	Translated (0%)	Advanced filtering mechanisms must be used to detect and block:	يجب استخدام آليات تصفية متقدمة للكشف عن وحظر:
108	Translated (0%)	Phishing attempts	محاولات التصيد الاحتيالي
109	Translated (0%)	Malware and ransomware attachments	مرفقات البرامج الضارة وبرامج الفدية
110	Translated (0%)	Spoofed sender domains	نطاقات المرسل المنتحلة
111	Translated (0%)	Spam and promotional bulk messages	الرسائل غير المرغوب فيها والرسائل الترويجية المجمعة
112	Translated (0%)	AI/ML-based threat intelligence platforms may be integrated for real-time scanning.	يمكن دمج منصات استخبارات التهديدات القائمة على الذكاء الاصطناعي/غسل الأموال للمسح في الوقت الفعلي.
113	Translated (0%)	Authentication and Access Control	المصادقة والتحكم في الوصول
114	Translated (0%)	Multi-Factor Authentication (MFA) must be implemented for all remote or webmail access.	لجميع عمليات الوصول عن بُعد أو (MFA) يجب تنفيذ المصادقة متعددة العوامل بريد الويب.
115	Translated (0%)	All user access to email services shall be role-based and follow the principle of least privilege.	يجب أن يكون وصول جميع المستخدمين إلى خدمات البريد الإلكتروني قائمًا على الأدوار وأن يتبع مبدأ الحد الأدنى من الامتيازات.
116	Translated (0%)	User sessions must be automatically logged out after a period of inactivity.	يجب تسجيل خروج المستخدم تلقائيًا بعد فترة من عدم النشاط.
117	Translated (0%)	Al Hammadi Holding retains the right to access employee e-mail if it has reasonable grounds to do so as required by law.	تحتفظ شركة الحمادي القابضة بالحق في الوصول إلى البريد الإلكتروني للموظفين إذا كان لديها أسباب معقولة للقيام بذلك كما هو مطلوب بموجب القانون.
118	Translated (0%)	Prohibited Use of E-Mail	الاستخدام المحظور للبريد الإلكتروني
119	Translated (0%)	The use of the E-Mail system is prohibited for the following:	يحظر استخدام نظام البريد الإلكتروني في الحالات التالية:
120	Translated (0%)	Charitable fundraising campaigns, political advocacy efforts, confidential business activities or personal amusement and entertainment.	حملات جمع التبرعات الخيرية، وجهود الدعوة السياسية، والأنشطة التجارية السرية أو التسلية الشخصية والترفيه.
121	Translated (0%)	Creating or distributing any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs, and practice, political beliefs, or national origin.	إنشاء أو توزيع أي رسائل تخريبية أو مسيئة، بما في ذلك التعليقات المسيئة حول العرق أو الجنس أو لون الشعر أو الإعاقة أو العمر أو التوجه الجنسي أو المواد الإباحية أو المعتقدات الدينية أو الممارسة أو المعتقدات السياسية أو الأصل القومي.
122	Translated (0%)	Forwarding or sending messages that have racial or sexual slurs, political or religious solicitations or any other message that could damage the reputation of Al Hammadi Holding.	إعادة توجيه أو إرسال رسائل تحتوي على افتراءات عرقية أو جنسية أو استدراج سياسي أو ديني أو أي رسالة أخرى يمكن أن تضر بسمعة شركة الحمادي القابضة.

123	Translated (0%)	Transmitting any material that potentially contains viruses, trojan horses, worms, time bombs or any other harmful or malicious program.	نقل أي مواد يحتمل أن تحتوي على فيروسات أو أحصنة طروادة أو ديدان أو قنابل موقوتة أو أي برنامج ضار أو ضار آخر.
124	Translated (0%)	User Accountability	مساءلة المستخدم
125	Translated (0%)	All messages originated/ received by the Al Hammadi Holding E-Mail system are considered to be the property of Al Hammadi Holding.	تعتبر جميع الرسائل التي تم إنشاؤها/ استلامها بواسطة نظام البريد الإلكتروني لشركة الحمادي القابضة ملكًا لشركة الحمادي القابضة.
126	Translated (0%)	The e-mail system shall be used for business purposes only.	يجب استخدام نظام البريد الإلكتروني لأغراض العمل فقط.
127	Translated (0%)	Users shall not use any unauthorized web-mail services or portals from the Al Hammadi Holding network.	لا يجوز للمستخدمين استخدام أي خدمات بريد إلكتروني أو بوابات غير مصرح بها من شبكة الحمادي القابضة.
128	Translated (0%)	Users shall regularly move their important e-mail messages to archive files at the e-mail client end.	يجب على المستخدمين نقل رسائل البريد الإلكتروني المهمة الخاصة بهم بانتظام لأرشفة الملفات في نهاية عميل البريد الإلكتروني.
129	Translated (0%)	The server end of the e-mail system is not intended for archival storage of the information.	نهاية الخادم لنظام البريد الإلكتروني غير مخصصة لتخزين المعلومات في الأرشيف.
130	Translated (0%)	It shall be the responsibility of users to regularly back up their pst and other important files in the designated shared folder in the file server.	وغيرها PST تقع على عاتق المستخدمين مسؤولية النسخ الاحتياطي المنتظم لملفات من الملفات المهمة في المجلد المشترك المعين في خادم الملفات.
131	Translated (0%)	The IT Operations & Infrastructure function shall take back-up of the file server at regular intervals (as per their documented process) or at the user's request, whichever is earlier.	يجب أن تأخذ وظيفة عمليات تكنولوجيا المعلومات والبنية التحتية نسخة احتياطية من خادم الملفات على فترات منتظمة (وفقًا للعملية الموثقة) أو بناءً على طلب المستخدم، أيهما أسبق.
132	Translated (0%)	If users receive any offensive or unsolicited material from external or internal sources, they shall not forward/ redistribute it to either other employees or third-party staff except to the reporting authority.	إذا تلقى المستخدمون أي مواد مسيئة أو غير مرغوب فيها من مصادر خارجية أو داخلية، فلا يجوز لهم إرسالها/ إعادة توزيعها على أي من الموظفين الآخرين أو موظفي الجهات الخارجية باستثناء الجهة القائمة بالإبلاغ.
133	Translated (0%)	If users are concerned by an excessive amount of spam from a particular organization or electronic mail address, they shall inform the IT helpdesk.	إذا كان المستخدمون قلقين بشأن كمية مفرطة من البريد العشوائي من منظمة معينة أو عنوان بريد إلكتروني معين، فيجب عليهم إبلاغ مكتب مساعدة تكنولوجيا المعلومات.
134	Translated (0%)	It is the responsibility of users to maintain accountability.	تقع على عاتق المستخدمين مسؤولية الحفاظ على المساءلة.
135	Translated (0%)	Al Hammadi Holding shall not be held responsible, nor does it accept any liability for the consequences of improper usage.	لا تتحمل شركة الحمادي القابضة المسؤولية، ولا تقبل أي مسؤولية عن عواقب الاستخدام غير السليم.
136	Translated (0%)	Attachments and Virus Protection	المرفقات والحماية من الفيروسات
137	Translated (100%)	Information involved in electronic messaging shall be appropriately protected.	يجب حماية المعلومات المتعلقة بالرسائل الإلكترونية بشكل مناسب.
138	Translated (0%)	Electronic messages shall be protected from unauthorized access, modification, or denial of service commensurate with	يجب حماية الرسائل الإلكترونية من الوصول غير المصرح به أو التعديل أو الحرمان من الخدمة بما يتناسب مع نظام التصنيف المعتمد من قبل شركة الحمادي القابضة.

		the classification scheme adopted by Al Hammadi Holding.	
139	Translated (0%)	Controls shall be implemented to ensure the correct addressing and transportation of electronic messages and the reliability and availability of the electronic messaging service.	يجب تنفيذ الضوابط لضمان صحة معالجة الرسائل الإلكترونية ونقلها وموثوقية خدمة المراسلة الإلكترونية وتوافرها.
140	Translated (0%)	All malicious attachments shall be quarantined and deleted at the e-mail gateway/ server end.	يجب عزل جميع المرفقات الضارة وحذفها في بوابة البريد الإلكتروني/نهاية الخادم.
141	Translated (0%)	The e-mail administrator shall maintain malicious file extensions that shall be blocked at the e-mail gateway/ server level and ensure that these are blocked.	يجب على مسؤول البريد الإلكتروني الاحتفاظ بامتدادات الملفات الضارة التي يجب حظرها على مستوى بوابة البريد الإلكتروني/ الخادم والتأكد من حظرها.
142	Translated (0%)	They shall regularly update this list and review it at least once a quarter.	يجب عليهم تحديث هذه القائمة بانتظام ومراجعتها مرة واحدة على الأقل كل ثلاثة أشهر.
143	Translated (0%)	The e-mail administrator shall implement e-mail content filtering and virus protection software at the e-mail gateway/ server using advanced and up-to-date email protection techniques.	يجب على مسؤول البريد الإلكتروني تنفيذ برنامج تصفية محتوى البريد الإلكتروني والحماية من الفيروسات في بوابة/ خادم البريد الإلكتروني باستخدام تقنيات حماية البريد الإلكتروني المتقدمة والحديثة.
144	Translated (0%)	Archival Storage and Backup	التخزين الأرشيفي والنسخ الاحتياطي
145	Translated (0%)	If an electronic mail message contains information relevant to the completion of a business transaction or could be produced as evidence for a critical decision, it shall be appropriately retained for future reference.	إذا كانت رسالة البريد الإلكتروني تحتوي على معلومات ذات صلة بإنجاز معاملة تجارية أو يمكن تقديمها كدليل على قرار حاسم، فيجب الاحتفاظ بها بشكل مناسب للرجوع إليها في المستقبل.
146	Translated (0%)	Backup of the e-mail server shall be taken by the backup and restore process.	يجب أخذ نسخة احتياطية من خادم البريد الإلكتروني عن طريق عملية النسخ الاحتياطي والاستعادة.
147	Translated (0%)	Auditing and Logging	التدقيق والتسجيل
148	Translated (0%)	Auditing and logging shall be enabled on the e-mail server.	يجب تمكين التدقيق والتسجيل على خادم البريد الإلكتروني.
149	Translated (0%)	Logs shall be reviewed as a routine process daily and any suspicious activity shall be monitored.	يجب مراجعة السجلات كعملية روتينية يوميًا ومراقبة أي نشاط مشبوه.
150	Translated (0%)	Audit trial shall be maintained and reviewed at least once a year.	يجب الحفاظ على تجربة التدقيق ومراجعتها مرة واحدة على الأقل في السنة.
151	Translated (0%)	The review report shall be submitted to the cybersecurity Steering committee.	يجب تقديم تقرير المراجعة إلى اللجنة التوجيهية للأمن السيبراني.
152	Translated (0%)	Systems supporting email services shall be regularly reviewed for compliance with Al Hammadi Holding's cyber security policies and standards.	يجب مراجعة الأنظمة الداعمة لخدمات البريد الإلكتروني بانتظام للتأكد من امتثالها لسياسات ومعايير الأمن السيبراني لشركة الحمادي القابضة.
153	Translated (0%)	Where possible, technical compliance shall be reviewed with the assistance of automated tools, which generate technical reports for subsequent interpretation by a technical specialist.	حيثما أمكن، يجب مراجعة الامتثال الفني بمساعدة الأدوات الآلية، التي تنتج تقارير فنية للتفسير اللاحق من قبل أخصائي تقني.

154	Translated (0%)	Manual reviews supported by appropriate software tools, if necessary, by an experienced security engineer shall be performed.	يجب إجراء مراجعات يدوية مدعومة بأدوات برمجية مناسبة، إذا لزم الأمر، من قبل مهندس أمن متمرس.
155	Translated (0%)	If penetration evaluations or vulnerability assessments are used, caution shall be exercised as such activities could lead to a compromise of the security of the system.	في حالة استخدام تقييمات الاختراق أو تقييمات الضعف، يجب توخي الحذر لأن هذه الأنشطة يمكن أن تؤدي إلى المساس بأمن النظام.
156	Translated (0%)	Such tests shall be planned, documented and repeatable.	يجب أن تكون هذه الاختبارات مخططة وموثقة وقابلة للتكرار.
157	Translated (0%)	Any technical compliance review shall only be conducted by competent, authorized persons or under the supervision of such persons.	لا يجوز إجراء أي مراجعة للامتثال الفني إلا من قبل أشخاص مختصين أو مفوضين أو تحت إشراف هؤلاء الأشخاص.
158	Translated (0%)	Penetration tests shall cover Internet-facing services and their technical components including infrastructure, websites, web applications, mobile apps, email, and remote access and shall be conducted periodically.	يجب أن تغطي اختبارات الاختراق الخدمات التي تواجه الإنترنت ومكوناتها الفنية بما في ذلك البنية التحتية ومواقع الويب وتطبيقات الويب وتطبيقات الهاتف المحمول والبريد الإلكتروني والوصول عن بُعد ويجب إجراؤها بشكل دوري.
159	Translated (100%)	Compliance and Adherence	الامتثال والالتزام
160	Translated (100%)	Al Hammadi Holding CEO shall ensure compliance with the cybersecurity policies and standards.	يضمن الرئيس التنفيذي لشركة الحمادي القابضة الامتثال لسياسات ومعايير الأمن السيبراني.
161	Translated (100%)	To ensure compliance, the Cybersecurity department will establish regular reporting by the Cybersecurity Manager, conduct periodic audits, or form a Cybersecurity Steering Committee for oversight.	لضمان الامتثال، سينشئ قسم الأمن السيبراني نظامًا لتقديم تقارير منتظمة يُعدّها مدير الأمن السيبراني، ويجري عمليات تدقيق دورية، أو يشكل لجنة توجيهية للأمن السيبراني للإشراف.
162	Translated (100%)	The CS manager shall ensure adherence to this policy.	يتعين على مدير الأمن السيبراني ضمان الالتزام بهذه السياسة.
163	Translated (100%)	All employees of Al Hammadi Holding must adhere to this policy.	على جميع موظفي شركة الحمادي القابضة الالتزام بهذه السياسة.
164	Translated (100%)	Violations of this policy may result in legal action in any jurisdiction or other measures as deemed appropriate by the Al Hammadi Holding.	قد تؤدي انتهاكات هذه السياسة إلى اتخاذ إجراءات قانونية في أي ولاية قضائية أو غيرها من التدابير التي تراها شركة الحمادي القابضة مناسبة.
165	Translated (100%)	Exceptions	الاستثناءات
166	Translated (100%)	Violation of cybersecurity policies and standards is prohibited unless a prior justified exception is obtained from the Cybersecurity Department or the Cybersecurity Steering Committee.	يُحظر انتهاك سياسات ومعايير الأمن السيبراني ما لم يتم الحصول على استثناء مبرر مسبق من إدارة الأمن السيبراني أو اللجنة التوجيهية للأمن السيبراني.
167	Translated (100%)	In case of a conflict, applicable legislative and regulatory requirements overrule Al Hammadi Holding policies and standards.	في حالة وجود تعارض، فإن المتطلبات التشريعية والتنظيمية المعمول بها تسود على سياسات ومعايير شركة الحمادي القابضة.

168	Translated (100%)	Revision	المراجعة
169	Translated (100%)	This policy is reviewed annually, or after major changes in Al Hammadi Holding's organizational chart or infrastructure, and more frequently whenever required, to ensure it remains appropriate and current for Al Hammadi Holding, ISO 27001, and NCA requirements.	تخضع هذه السياسة لمراجعة سنوية، أو لإعادة التقييم بعد أي تغييرات جوهرية في الهيكل التنظيمي أو البنية التحتية لشركة الحمادي القابضة، إضافة إلى مراجعات دورية إضافية عند الضرورة، وذلك لضمان توافقها المستمر مع متطلبات شركة الحمادي القابضة، ISO 27001:2022 وإرشادات الهيئة الوطنية للأمن السيبراني.
170	Translated (100%)	Approval Section	قسم الاعتماد
171	Translated (100%)	Prepared by:	إعداد:
172	Translated (100%)	Mr. Mohammed Alamer	السيد/ محمد العامر
173	Translated (100%)	GRC Cybersecurity Specialist	أخصائي حوكمة ومخاطر وامتثال في الأمن السيبراني
174	Translated (100%)	Name	الاسم
175	Translated (100%)	Designation	المسمى الوظيفي
176	Translated (100%)	Signature	التوقيع
177	Translated (100%)	Date	التاريخ
178	Translated (100%)	Reviewed by:	راجعها:
179	Translated (100%)	Mr. Deepak Dasan	السيد/ ديباك داسان
180	Translated (100%)	IT Manager	مدير تكنولوجيا المعلومات
181	Translated (100%)	Name	الاسم
182	Translated (100%)	Designation	المسمى الوظيفي
183	Translated (100%)	Signature	التوقيع
184	Translated (100%)	Date	التاريخ
185	Translated (100%)	Reviewed by:	راجعها:

186	Translated (100%)	Ms. Mashael Alotaibi	السيدة/ مشاعل العتيبي
187	Translated (100%)	<873>Cybersecurity </873>Manager	<مدير <873>الأمن السيبراني<873/>
188	Translated (100%)	Name	الاسم
189	Translated (100%)	Designation	المسمى الوظيفي
190	Translated (100%)	Signature	التوقيع
191	Translated (100%)	Date	التاريخ
192	Translated (100%)	Approved by:	:اعتمدها
193	Translated (100%)	Dr. Abdulaziz Al Hammadi	الحمادي<Bold></Bold> د./ عبد العزيز<Bold><Bold><Bold><Bold></Bold></Bold>
194	Translated (100%)	Chief Operating Officer	الرئيس التنفيذي للعمليات
195	Translated (100%)	Name	الاسم
196	Translated (100%)	Designation	المسمى الوظيفي
197	Translated (100%)	Signature	التوقيع
198	Translated (100%)	Date	التاريخ
199	Translated (100%)	Approved by:	:اعتمدها
200	Translated (100%)	Mr. Mohammad Al Hammadi	السيد/ محمد الحمادي
201	Translated (100%)	Chief Executive Officer	الرئيس التنفيذي
202	Translated (100%)	Name	الاسم
203	Translated (100%)	Designation	المسمى الوظيفي
204	Translated (100%)	Signature	التوقيع
205	Translated	Date	التاريخ

	(100%)		