



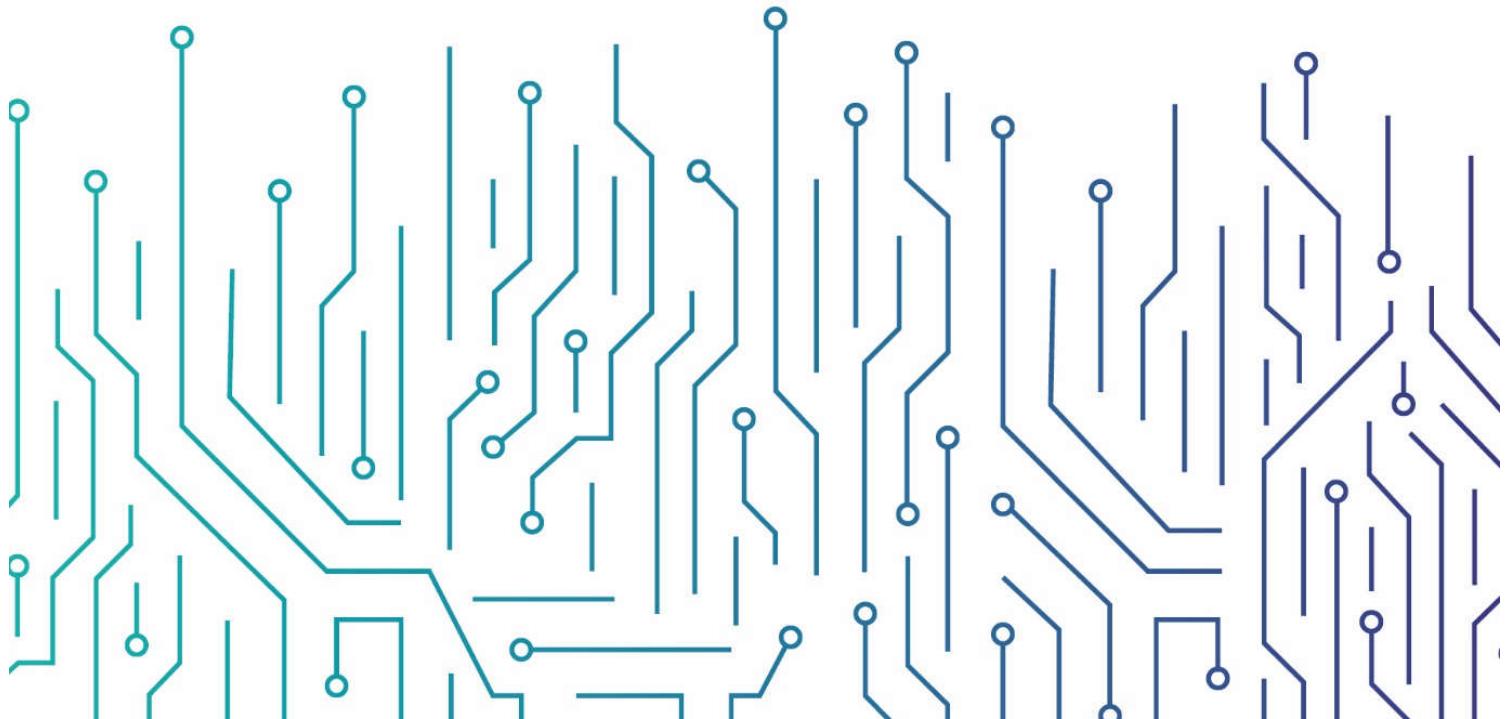
الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

ضوابط الأمان السيبراني

للبيانات

Data Cybersecurity Controls
(DCC -1: 2022)

إشارة المشاركة: أبيض
تصنيف الوثيقة: عام



بسم الله الرحمن الرحيم

بروتوكول الإشارة الضوئية (TLP):

يستخدم هذا البروتوكول على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية):

أحمر - شخصي وسري للمستلم فقط

المستلم لا يحق له مشاركة المصنف بالإشارة الحمراء مع أي فرد، سواء من داخل أو خارج الجهة خارج النطاق المحدد للإسلام.

برتقالي - مشاركة محددة

المستلم يمكنه مشاركة المعلومات في نفس الجهة مع الأشخاص المعنيين فقط، ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

أخضر - مشاركة في نفس المجتمع

المستلم يمكنه مشاركة المعلومات مع آخرين في نفس الجهة أو جهة أخرى على علاقة معهم أو في نفس القطاع، ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

أبيض - غير محدود

قائمة المحتويات

٠	الملخص التنفيذي
١	المقدمة
٧	الأهداف
٧	نطاق العمل وقابلية التطبيق
٧	نطاق عمل الضوابط
٧	قابلية التطبيق داخل الجهة
٨	التنفيذ والالتزام
٨	التحديث والمراجعة
٩	مكونات وهيكلية ضوابط الأمان السيبراني للبيانات
٩	المكونات الأساسية والفرعية لضوابط الأمان السيبراني للبيانات
١٠	الهيكلية
١١	ضوابط الأمان السيبراني للبيانات
١٩	ملحق
١٩	ملحق (أ): العلاقة مع الضوابط الأساسية للأمان السيبراني
٢٢	ملحق (ب): مصطلحات وتعريفات
٢٣	ملحق (ج): قائمة الاختصارات
٢٤	ملحق (د): العلاقة مع دورة حياة البيانات

قائمة الجداول

١٠	جدول ١ : هيكلية ضوابط الأمان السيبراني للبيانات
٢٢	جدول ٢ : مصطلحات وتعريفات
٢٣	جدول ٣ : قائمة الاختصارات
٢٤	جدول ٤ : العلاقة مع دورة حياة البيانات

قائمة الأشكال والرسوم التوضيحية

٩	شكل ١ : المكونات الأساسية والفرعية لضوابط الأمان السيبراني للبيانات
١٠	شكل ٢ : معنى رموز ضوابط الأمان السيبراني للبيانات
١٠	شكل ٣ : هيكلية ضوابط الأمان السيبراني للبيانات
١٩	شكل ٤ : دليل ألوان المكونات الفرعية في الشكل ٥
٢٠	شكل ٥ : مكونات الضوابط الأساسية للأمان السيبراني، وضوابط الأمان السيبراني للبيانات

الملخص التنفيذي

تسعى المملكة في ظل رؤية ٢٠٣٠ إلى تحقيق عدد من الأهداف الاقتصادية والتنموية والأمنية مما يعزز أداء الجهات الوطنية، ويشجع على تنوع الاقتصاد والاستفادة من الخدمات المعتمدة على البيانات. وتعتبر البيانات الوطنية أحد أهم الأصول التي تسهم في تحقيق الأهداف الاستراتيجية لرؤية المملكة العربية السعودية ٢٠٣٠ من خلال دعم صناعة القرار، وتعد ذلك مورداً اقتصادياً لدعم المقومات التنافسية على المستوى الوطني، حيث تقوم الجهات الوطنية بجمع ومعالجة كميات هائلة من البيانات الوطنية التي قد تكون عرضة للتهديدات والمخاطر السيبرانية المؤثرة سلبياً على الأمن الوطني واقتصاد المملكة أو سمعتها أو علاقاتها الخارجية، أو على سلامة البنية التحتية الوطنية الحساسة. مما يستوجب وضع متطلبات الأمن السيبراني للحد من هذه التهديدات والمخاطر.

لقد نص تنظيم الهيئة الوطنية للأمن السيبراني الصادر بالأمر الملكي الكريم رقم (٦٨٠١) وتاريخ ١٤٣٩/٢/١١ على كونها الجهة المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه. وتشمل اختصاصاتها ومهامها وضع السياسات، وأليات الحكومة، والأطر ومعايير، والضوابط، والإرشادات المتعلقة بالأمن السيبراني، وتعزيزها على الجهات، ومتابعة الالتزام بها وتحديثها؛ بما يعزز دور الأمن السيبراني، وأهميته؛ والحاجة الملحة له التي ازدادت مع ازدياد التهديدات، والمخاطر السيبرانية، أكثر من أي وقت مضى. كما أن دور الهيئة التنظيمي لا يُخلي أي جهة عامة أو خاصة، أو غيرها من مسؤوليتها تجاه أنها السiberian؛ وهو ما تضمنه الأمر السامي الكريم رقم (٥٧٢٣١) وتاريخ ١٤٣٩/١١/١٠ هـ بأن "على جميع الجهات الحكومية رفع مستوى أمنها السيبراني؛ لحماية شبكاتها وأنظمتها وبياناتها الإلكترونية، والالتزام بما تصدره الهيئة الوطنية للأمن السيبراني من سياسات وأطر ومعايير، ضوابط وإرشادات بهذا الشأن".

وبهدف الوصول إلى فضاء سيريرياني سعودي آمن وموثوق يمكن النمو والازدهار؛ وامتداداً للضوابط الأساسية للأمن السيبراني (ECC)، قامت الهيئة الوطنية للأمن السيبراني بإعداد ضوابط الأمان السيبراني للبيانات (DCC - 1: 2022) لوضع الحد الأدنى من متطلبات الأمان السيبراني لتمكن الجهات من حماية بياناتها خلال جميع مراحل دورة حياة البيانات. وتوضح هذه الوثيقة تفاصيل ضوابط الأمان السيبراني للبيانات، وأهدافها، ونطاق العمل، وآلية الالتزام والمتابعة.

وعلى الجهات تنفيذ ما يحقق الالتزام الدائم والمستمر بهذه الضوابط؛ تحقيقاً لما ورد في الفقرة الثالثة من المادة العاشرة، في تنظيم الهيئة الوطنية للأمن السيبراني؛ والتي نصت على أن تلتزم كافة الجهات ذات العلاقة بتنفيذ السياسات وأليات الحكومة والأطر وتطبيق المعايير والضوابط التي تقرها الهيئة. وما تضمنه الأمر السامي الكريم رقم (٥٧٢٣١) وتاريخ ١٤٣٩/١١/١٠ هـ.

المقدمة

قامت الهيئة الوطنية للأمن السيبراني (ويشار لها في هذه الوثيقة بـ "الهيئة") بإصدار ضوابط الأمن السيبراني للبيانات (DCC-1:2022)؛ بعد دراسة عدد من المعايير، والأطر والضوابط، ذات الأهداف المماثلة لدى جهات ومنظمات دولية، ومراعاة متطلبات التشريعات والتنظيمات ذات العلاقة، وبعد الاطلاع على أفضل الممارسات والتجارب في مجال الأمن السيبراني، والاستفادة منها، وتحليل ما تم رصده من مخاطر وتهديدات وحوادث سيبرانية على المستوى الوطني. وتساعد هذه الضوابط الجهات على مواجهة التهديدات السيبرانية المتزايدة والخروج منها بأقل ضرر في حال حدوثها بما يحافظ على المصالح الحيوية للدولة وأمنها الوطني والبني التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية.

وقد حرصت الهيئة في إعدادها لضوابط الأمن السيبراني للبيانات، على مواءمة مكوناتها مع مكونات الضوابط الأساسية للأمن السيبراني التي تعد متطلباً أساسياً لها، ولا يمكن للجهات تحقيق الالتزام بها إلا من خلال تحقيق الالتزام المستمر بالضوابط الأساسية للأمن السيبراني في المقام الأول – وفقاً لقابلية تطبيقها عليها. كما ترتبط ضوابط الأمن السيبراني للبيانات مع المتطلبات التشريعية، والتنظيمية الوطنية ذات العلاقة. واستناداً إلى الأدوات التنظيمية الصادرة من الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) تم تصنيف البيانات إلى أربعة مستويات بناءً على حساسيتها ومدى الحاجة إلى حمايتها من المخاطر، وهذه التصنيفات هي: عام، مقييد، سري، سري للغاية.

ت تكون ضوابط الأمن السيبراني للبيانات من:

- ٣ مكونات أساسية (3 Main Domains)
- ١١ مكون فرعياً (11 Subdomains)
- ١٩ ضابطاً أساسياً (19 Main Controls)
- ٤٧ ضابطاً فرعياً (47 Subcontrols)

الأهداف

تهدف ضوابط الأمان السيبراني للبيانات إلى:

- رفع مستوى الأمان السيبراني لحماية البيانات الوطنية.
- تعزيز الأمان السيبراني للجهات خلال مراحل دورة حياة البيانات، وذلك لضمان حماية بياناتها والأصول المعلوماتية من التهديدات والمخاطر السيبرانية.
- رفع مستوى الوعي حول التعامل الآمن مع البيانات.

نطاق العمل وقابلية التطبيق

نطاق عمل الضوابط

تطبق هذه الضوابط على الجهات الحكومية في المملكة العربية السعودية (وتشمل الوزارات والهيئات والمؤسسات وغيرها) والجهات والشركات التابعة لها، وتطبق على جهات القطاع الخاص التي تمتلك بنى تحتية وطنية حساسة أو تقوم بتشغيلها أو استضافتها، ويشار لها جميعاً في هذه الوثيقة بـ (الجهة)، كما تطبق الضوابط على جميع أشكال البيانات المادية وال الرقمية، والتي تشمل البيانات المهيكلة (مثل قواعد البيانات وجداول البيانات) والبيانات غير المهيكلة (مثل الوثائق والمستندات).
كما تشجع الهيئة وبشدة الجهات الأخرى في المملكة على الاستفادة من هذه الضوابط لتطبيق أفضل ممارسات الأمان السيبراني لحماية البيانات.

قابلية التطبيق داخل الجهة

تم إعداد هذه الضوابط بحيث تكون ملائمة لمتطلبات الأمان السيبراني للجهات والقطاعات في المملكة العربية السعودية بتنوع طبيعة أعمالها، ويجب على الجهات ضمن نطاق هذه الضوابط الالتزام بجميع الضوابط القابلة للتطبيق عليها.

التنفيذ والالتزام

تحقيقاً لما ورد في الفقرة الثالثة من المادة العاشرة من تنظيم الهيئة الوطنية للأمن السيبراني، وكذلك ما ورد في الأمر السامي الكريم رقم (٥٧٣١) وتاريخ ١٤٣٩/١١/١٠ هـ يجب على جميع الجهات ضمن نطاق عمل هذه الضوابط تفزيذ ما يحقق الالتزام الدائم والمستمر بهذه الضوابط، ولا يمكن تحقيق ذلك إلا من خلال تحقيق الالتزام الدائم والمستمر بالضوابط الأساسية للأمن السيبراني (ECC - 1: 2018) وفقاً لقابلية تطبيقها في الجهة بحسب طبيعة أعمالها.

وتقوم الهيئة بتقييم التزام الجهات بما ورد في هذه الضوابط بطرق متعددة، منها: التقييم الذاتي للجهات، وأو التقييم الخارجي، وذلك وفقاً للآلية المناسبة التي تراها الهيئة.

التحديث والمراجعة

تتولى الهيئة المراجعة الدورية لضوابط الأمن السيبراني للبيانات حسب متطلبات الأمن السيبراني والمستجدات ذات العلاقة وتحديثها متى ما دعت الحاجة لذلك.

مكونات وهيكلية ضوابط الأمان السيبراني للبيانات

المكونات الأساسية والفرعية، لضوابط الأمان السيبراني للبيانات

يوضح الشكل (١) أدناه، المكونات الأساسية والفرعية، لضوابط الأمان السيبراني للبيانات. كما يوضح ملحق (آ) العلاقة مع الضوابط الأساسية للأمن السيبراني.

الأمن السيبراني المتعلق بـالموارد البشرية Cybersecurity in Human Resources	٢-١	المراجعة والتدقير الدوري للأمن السيبراني Periodical Cybersecurity Review and Audit	١-١	١ - حوكمة الأمان السيبراني Cybersecurity Governance
برنامج التوعية والتدريب بالأمن السيبراني Cybersecurity Awareness and Training Program			٣-١	
حماية الأنظمة وأجهزة معالجة المعلومات Information System and Information Processing Facilities Protection	٢-٢	إدارة هويات الدخول والصلاحيات Identity and Access Management	١-٢	
حماية البيانات والمعلومات Data and Information Protection	٤-٢	أمن الأجهزة المحمولة Mobile Devices Security	٣-٢	٢ - تعزيز الأمان السيبراني Cybersecurity Defense
الإتلاف الآمن للبيانات Secure Data Disposal	٦-٢	التشفيير Cryptography	٥-٢	
الأمن السيبراني للطابعات ولماسحات الضوئية وآلات التصوير Cybersecurity for Printers, Scanners and Copy Machines			٧-٢	
الأمن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity			١-٣	٣ - الأمان السيبراني المتعلق بالأطراف الخارجية والموسبية السطانية Third-Party and Cloud Computing Cybersecurity

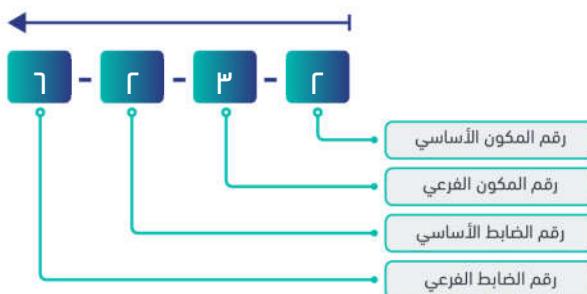
شكل ١ : المكونات الأساسية والفرعية لضوابط الأمان السيبراني للبيانات

الهيكلية

يوضح الشكلان (٢) و (٣) أدناه معنى رموز ضوابط الأمان السيبراني للبيانات.



شكل ٢ : معنى رموز ضوابط الأمان السيبراني للبيانات



شكل ٣ : هيكلية ضوابط الأمان السيبراني للبيانات

يوضح الجدول ١ طريقة هيكلية ضوابط الأمان السيبراني للبيانات.

اسم المكون الأساسي	١
رقم مرجعي للمكون الأساسي	
رقم مرجعي للمكون الفرعي	
الهدف	
مستوى تصنيف البيانات	الضوابط
عام	
سري للغاية	
سري	
مقيد	
عام	
مستوى تصنيف البيانات	
بنود الضابط	
رقم مرجعي للضابط	

جدول ١ : هيكلية ضوابط الأمان السيبراني للبيانات

ضوابط الأمان السيبراني للبيانات

حوكمة الأمان السيبراني (Cybersecurity Governance)



				الهدف								
				الضوابط								
				الهدف								
المراجعة والتدقق الدوري للأمن السيبراني (Periodical Cybersecurity Review and Audit)				١-١								
<p>ضمان التأكيد من أن ضوابط الأمان السيبراني لدى الجهة مطبقة وتعمل وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المقرة تنظيمياً على الجهة.</p>				الهدف								
<table border="1" style="width: 100%; text-align: center;"> <tr> <td style="background-color: #e6f2ff; width: 25%;">مستوى تصنيف البيانات</td> <td style="width: 25%;"></td> <td style="width: 25%;"></td> <td style="width: 25%;"></td> </tr> <tr> <td style="background-color: #e6f2ff;">سري للغاية</td> <td style="background-color: #ffcc00;">سري</td> <td style="background-color: #ffd700;">مقيد</td> <td style="background-color: #2e8b57;">عام</td> </tr> </table>				مستوى تصنيف البيانات				سري للغاية	سري	مقيد	عام	الضوابط
مستوى تصنيف البيانات												
سري للغاية	سري	مقيد	عام									
<p>رجوعاً للضابط ١-٨-١ في الضوابط الأساسية للأمن السيبراني، فإنه يجب على الإدارة المعنية بالأمن السيبراني في الجهة مراجعة تطبيق ضوابط الأمان السيبراني للبيانات حسب المدة المحددة لكل مستوى.</p>				١-١-١								
<p>كل سنة على الأقل</p>				رجوعاً للضابط ٢-٨-١ في الضوابط الأساسية للأمن السيبراني، فإنه يجب أن تتم مراجعة تطبيق ضوابط الأمان السيبراني للبيانات من قبل أطراف مستقلة عن الإدارة المعنية بالأمن السيبراني من داخل الجهة حسب المدة المحددة لكل مستوى.	٢-١-١							
الأمن السيبراني المتعلق بالموارد البشرية (Cybersecurity in Human Resources)				٢-١								
<p>ضمان التأكيد من أن مخاطر ومتطلبات الأمان السيبراني المتعلقة بالعاملين (موظفين ومتعاقدين) في الجهة تعالج بفعالية قبل وأثناء وعند انتهاء/ إنهاء عملهم، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.</p>				الهدف								
<table border="1" style="width: 100%; text-align: center;"> <tr> <td style="background-color: #e6f2ff; width: 25%;">مستوى تصنيف البيانات</td> <td style="width: 25%;"></td> <td style="width: 25%;"></td> <td style="width: 25%;"></td> </tr> <tr> <td style="background-color: #e6f2ff;">سري للغاية</td> <td style="background-color: #ffcc00;">سري</td> <td style="background-color: #ffd700;">مقيد</td> <td style="background-color: #2e8b57;">عام</td> </tr> </table>				مستوى تصنيف البيانات				سري للغاية	سري	مقيد	عام	الضوابط
مستوى تصنيف البيانات												
سري للغاية	سري	مقيد	عام									
<p>بالإضافة للضوابط الفرعية ضمن الضابط ٣-٩-١ في الضوابط الأساسية للأمن السيبراني يجب أن تغطي متطلبات الأمان السيبراني المتعلق بالموارد البشرية لتشمل خلال وبعد إنتهاء/ إنهاء العلاقة الوظيفية في الجهة بحد أدنى ما يلي:</p>				١-٢-١								
<p>✓ ✓ ✓</p>				إجراء المسح الأمني (Screening and vetting) للعاملين في الوظائف ذات العلاقة بالتعامل مع البيانات.	١-١-٢-١							
<p>✓ ✓ ✓</p>				تعهد العاملين في الجهة بعدم استخدام تطبيقات التراسل أو التواصل الاجتماعي أو خدمات التخزين السحابية الشخصية لإنشاء أو تخزين أو مشاركة البيانات الخاصة بالجهة، باستثناء تطبيقات التراسل الآمنة المعتمدة من الجهات ذات العلاقة.	٢-١-٢-١							
برنامج التوعية والتدريب بالأمن السيبراني (Cybersecurity Awareness and Training Program)				٣-١								
<p>ضمان التأكيد من أن العاملين بالجهة لديهم التوعية الأمنية الازمة وعلى دراية بمسؤولياتهم في مجال الأمان السيبراني. والتأكد من تزويد العاملين بالجهة بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمان السيبراني لحماية الأصول المعلوماتية والتقنية للجهة والقيام بمسؤولياتهم تجاه الأمان السيبراني.</p>				الهدف								

مستوى تصنيف البيانات					الضوابط
سري للغاية	سري	مقييد	عام		1-٣-١
				بالإضافة للضوابط الفرعية ضمن الضابط ٣-١٠-١ في الضوابط الأساسية للأمن السيبراني، فإنه يجب أن يغطي برنامج التوعية بالأمن السيبراني المحاور المتعلقة بحماية البيانات، بما في ذلك:	
✓	✓	✓	✓	مخاطر التسريب والوصول غير المصرح به للبيانات خلال دورة حياتها.	١-١-٣-١
✓	✓	✓		التعامل الآمن مع البيانات المصنفة خلال السفر والتواجد خارج مكان العمل.	٢-١-٣-١
✓	✓	✓		التعامل الآمن مع البيانات خلال الاجتماعات (الافتراضية والحضورية).	٣-١-٣-١
✓	✓	✓		الاستخدام الآمن للطبعات والماسحات الضوئية وآلات التصوير.	٤-١-٣-١
✓	✓	✓		إجراءات الإتلاف الآمن للبيانات.	٥-١-٣-١
✓	✓	✓	✓	مخاطر مشاركة الوثائق والمعلومات من خلال قنوات تواصل غير مؤمنة.	٦-١-٣-١
✓	✓	✓	✓	المخاطر السيبرانية المتعلقة باستخدام وسائل التخزين الخارجية.	٧-١-٣-١

تعزيز الأمان السيبراني (Cybersecurity Defense)



إدارة هويات الدخول والصلاحيات (Identity and Access Management)					١-٢
ضمان حماية الأمن السيبراني للوصول المنطقي (Logical Access) إلى الأصول المعلوماتية والتكنولوجية للجهة؛ من أجل منع الوصول غير المصرح به، وتقييد الوصول إلى ما هو مطلوب؛ لإنجاز الأعمال المتعلقة بالجهة.					الهدف
مستوى تصنيف البيانات					الضوابط
سري للغاية	سري	مقييد	عام	بالإضافة للضوابط الفرعية ضمن الضابط ٣-٢-٢ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمان السيبراني المتعلقة بإدارة هويات الدخول والصلاحيات، بحد أدنى، ما يلي:	
✓	✓			التقييد الحازم بالسماح للحد الأدنى من العاملين للوصول والاطلاع ومشاركة البيانات بناءً على قوائم صلاحيات مقتصرة على موظفين سعوديين إلا بوجب استثناء من قبل صاحب الصلاحية (رئيس الجهة أو من يفوضه) وعلى أن يتم إعتماد هذه القوائم من قبل صاحب الصلاحية.	
✓	✓	✓		منع مشاركة قوائم الصلاحيات المعتمدة مع الأشخاص غير المصرح لهم.	
✓	✓	✓		إدارة هويات الدخول وصلاحيات الاطلاع على البيانات باستخدام أنظمة إدارة الصلاحيات (Privileged Access Management).	
كل ٣ أشهر على الأقل	كل سنة على الأقل	بالإضافة للضابط الفرعي ٥-٣-٢-٢ في الضوابط الأساسية للأمن السيبراني، يجب مراجعة قوائم الصلاحيات المعتمدة والصلاحيات المستخدمة للتعامل مع البيانات حسب المدة المحددة لكل مستوى.			
حماية الأنظمة وأجهزة معالجة المعلومات (Information System and Information Processing Facilities Protection)					٢-٢
ضمان حماية الأنظمة وأجهزة معالجة المعلومات بما في ذلك أجهزة المستخدمين والبني التحتية للجهة من المخاطر السيبرانية.					الهدف
مستوى تصنيف البيانات					الضوابط
سري للغاية	سري	مقييد	عام	بالإضافة للضوابط الفرعية ضمن الضابط ٣-٣-٢ في الضوابط الأساسية للأمن السيبراني، يجب أن تشمل متطلبات الأمان السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات، بحد أدنى، ما يلي:	
فوري		كل شهر على الأقل		تطبيق حزم التحديثات، والإصلاحات الأمنية من وقت إطلاقها للأنظمة المستخدمة للتعامل مع البيانات حسب المدة المحددة لكل مستوى.	
كل ٦ أشهر على الأقل		كل سنة على الأقل		مراجعة إعدادات الحماية والتحصين للأنظمة المستخدمة للتعامل مع البيانات (Security Configuration and Hardening) حسب المدة المحددة لكل مستوى.	
✓	✓	✓	✓	مراجعة وتحصين الإعدادات المصطنعة (مثل كلمات المرور الثابتة، والخلفية الافتراضية) للأصول التقنية المستخدمة للتعامل مع البيانات.	

✓	✓			(Print Screen or Screen Capture) تعطيل خاصية تصوير الشاشة للأجهزة التي تنشئ أو تعالج الوثائق.	٤-١-٢-٢	
أمن الأجهزة المحمولة (Mobile Devices Security)					٣-٢	
ضمان حماية أجهزة الجهة المحمولة (بما في ذلك أجهزة الحاسب المحمول والهواتف الذكية والأجهزة الذكية اللوحية) من المخاطر السيبرانية. وضمان التعامل بشكل آمن مع المعلومات الحساسة والمعلومات الخاصة بأعمال الجهة وحمايتها أثناء النقل والتخزين والمعالجة عند استخدام الأجهزة الشخصية للعاملين في الجهة (مبدأ BYOD).					الهدف	
مستوى تصنيف البيانات					الضوابط	
سري للغاية	سري	مقيد	عام	بالإضافة للضوابط الفرعية ضمن الضابط ٣-٦-٢ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة، بحد أدنى، ما يلي:	١-٣-٢	
✓	✓	✓	✓	إدارة الأجهزة المحمولة المملوكة للجهة مركزياً باستخدام نظام إدارة الأجهزة المحمولة (MDM) - Mobile Device Management وتفعيل خاصية الحذف عن بعد.	١-١-٣-٢	
يمكن استخدام أجهزة (BYOD)	✓	✓		إدارة أجهزة (BYOD) مركزياً باستخدام نظام إدارة الأجهزة المحمولة (MDM) - Mobile Device Management وتفعيل خاصية الحذف عن بعد.	٢-١-٣-٢	
حماية البيانات والمعلومات (Data and Information Protection)					٤-٢	
ضمان حماية السرية وسلامة بيانات ومعلومات الجهة ودقتها وتوافرها، وذلك وفقاً لسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.					الهدف	
مستوى تصنيف البيانات					الضوابط	
سري للغاية	سري	مقيد	عام	بالإضافة للضوابط الفرعية ضمن الضابط ٣-٧-٢ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بحماية البيانات والمعلومات، بحد أدنى، ما يلي:	١-٤-٢	
✓	✓			استخدام خاصية العلامات المائية لتميز كامل الوثيقة عند الإنشاء والتخزين والطباعة وعلى الشاشة وعلى كل نسخة بحيث يكون الرمز يمكن تتبعه على مستوى المستخدم أو الجهاز.	١-١-٤-٢	
✓	✓	✓		استخدام تقنيات منع تسريب البيانات (Data Leakage Prevention) وتقنيات إدارة الصلاحيات (Rights Management).	٢-١-٤-٢	
✓	✓	✓		حظر استخدام البيانات في أي بيئة غير بيئة الإنتاج (Production Environment) إلا بعد إجراء تقييم للمخاطر وتطبيق ضوابط لحماية تلك البيانات، مثل تقنيات تعتيم البيانات (Data Masking) أو تقنيات مزج البيانات (Data Scrambling).	٣-١-٤-٢	
✓	✓	✓	✓	استخدام خدمة حماية العلامة التجارية لحماية هوية الجهة من الانتهاك .(Brand Protection)	٤-١-٤-٢	

الهدف					الصوابط		
مستوى تصنيف البيانات					الصوابط		
<p>ضمان الاستخدام السليم والفعال للتشفير؛ لحماية الأصول المعلوماتية الإلكترونية للجهة، وذلك وفقاً للسياسات، والإجراءات التنظيمية للجهة، والمطلبات التشريعية والتنظيمية ذات العلاقة.</p>					٥-٢		
<table border="1"> <thead> <tr> <th>الصوابط</th> </tr> </thead> <tbody> <tr> <td>١-٥-٢</td> </tr> </tbody> </table>					الصوابط	١-٥-٢	
الصوابط							
١-٥-٢							
<p>بالإضافة للضوابط الفرعية ضمن الضابط ٣-٨-٢ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي مطلوبات الأمن السيبراني للتشفير في الجهة، بحد أدنى، ما يلي:</p>					١-٥-٢		
<p>استخدام طرق وخوارزميات محدثة وأمنة للتشفير عند الإنشاء والتخزين والمشاركة وعلى كامل الاتصال الشبكي المستخدم لنقل البيانات وفقاً للمستوى المتقدم (Advanced) ضمن المعايير الوطنية للتشفير (NCS - ١:٢٠٢٠).</p>					١-٥-٢		
<p>استخدام طرق وخوارزميات محدثة وأمنة للتشفير عند الإنشاء والتخزين والمشاركة وعلى كامل الاتصال الشبكي المستخدم لنقل البيانات وفقاً للمستوى الأساسي (Moderate) ضمن المعايير الوطنية للتشفير (NCS - ١:٢٠٢٠).</p>					٢-١-٥-٢		
<p>الإتلاف الآمن للبيانات (Secure Data Disposal)</p>					٦-٢		
<p>ضمان تنفيذ عمليات إتلاف البيانات بشكل آمن، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمطلبات التشريعية والتنظيمية ذات العلاقة.</p>					الهدف		
<table border="1"> <thead> <tr> <th>الصوابط</th> </tr> </thead> <tbody> <tr> <td>١-٦-٢</td> </tr> </tbody> </table>					الصوابط	١-٦-٢	
الصوابط							
١-٦-٢							
<p>يجب أن تغطي مطلوبات الإتلاف الآمن للبيانات في الجهة بحد أدنى، ما يلي:</p>					١-٦-٢		
<p>تحديد التقنيات والأدوات والإجراءات لتنفيذ عمليات الإتلاف الآمن للبيانات حسب مستوى تصنيف البيانات.</p>					١-٦-٢		
<p>عند انتهاء الحاجة لاستخدام وسائل التخزين بشكل نهائي، يجب أن يتم الإتلاف الآمن (Secure Disposal) لوسائل التخزين وذلك باستخدام التقنيات والأدوات وإتباع الإجراءات التي تم تحديدها في الضابط رقم ٦-٢-١.</p>					٢-١-٦-٢		
<p>عند الحاجة لإعادة استخدام وسائل التخزين، يجب أن يتم الحذف الآمن للبيانات (Secure Erasure)، بحيث لا يمكن استرجاعها.</p>					٣-١-٦-٢		
<p>يجب أن يتم التحقق من تنفيذ عمليات الإتلاف أو الحذف الآمن للبيانات المشار إليها في الضابطين رقم ٢-١-٦-٢ و ٣-١-٦-٢.</p>					٤-١-٦-٢		
<p>الاحتفاظ بسجل لعمليات الإتلاف أو الحذف الآمن للبيانات التي تم تنفيذها.</p>					٥-١-٦-٢		
<p>يجب مراجعة تطبيق مطلوبات الإتلاف الآمن للبيانات في الجهة حسب المدة المحددة لكل مستوى.</p>					٢-٦-٢		
<p>الأمن السيبراني للطبعات والماسحات الضوئية وآلات التصوير (Cybersecurity for Printers, Scanners and Copy Machines)</p>					٧-٢		
<p>ضمان التعامل الآمن مع البيانات عند استخدام الطبعات والماسحات الضوئية وآلات التصوير.</p>					الهدف		
<table border="1"> <thead> <tr> <th>الصوابط</th> </tr> </thead> <tbody> <tr> <td>١-٧-٢</td> </tr> </tbody> </table>					الصوابط	١-٧-٢	
الصوابط							
١-٧-٢							
<table border="1"> <thead> <tr> <th>مستوى تصنيف البيانات</th> </tr> </thead> <tbody> <tr> <td>١-٧-٢</td> </tr> </tbody> </table>					مستوى تصنيف البيانات	١-٧-٢	١-٧-٢
مستوى تصنيف البيانات							
١-٧-٢							
<p>يجب تحديد وتوثيق واعتماد مطلوبات الأمن السيبراني لحماية الطبعات والماسحات الضوئية وآلات التصوير في الجهة.</p>							

✓	✓	✓		يجب تطبيق متطلبات الأمان السيبراني للطبعات ولما سحات الضوئية وآلات التصوير في الجهة.	٢-٧-٢
				يجب أن تغطي متطلبات الأمان السيبراني للطبعات ولما سحات الضوئية وآلات التصوير بحد أدنى، ما يلي:	٣-٧-٢
✓	✓			تعطيل خاصية التخزين المؤقت.	١-٣-٧-٢
✓	✓			تفعيل خاصية التحقق من الهوية في الطابعات ولما سحات الضوئية والآت التصوير المركزية قبل بدء عمليات الطباعة والتصوير والممسح الضوئي.	٢-٣-٧-٢
✓	✓			الاحتفاظ بطريقة آمنة بسجل الكتروني للعمليات الخاصة باستخدام الطابعات ولما سحات الضوئية والآت التصوير، لفترة لا تقل عن ١٢ شهراً.	٣-٣-٧-٢
✓	✓			تفعيل وحماية سجلات المراقبة لأنظمة CCTV على موقع أجهزة الطباعة المركزية ولما سحات الضوئية والآت التصوير.	٤-٣-٧-٢
✓	✓			استخدام أجهزة تمزيق الوثائق الورقية (Cross Shredding)، لإتلاف الوثائق في حال الانتهاء من استخدامها نهائياً.	٥-٣-٧-٢
كل سنة على الأقل		كل ٣ سنوات على الأقل		يجب مراجعة تطبيق متطلبات الأمان السيبراني للطبعات ولما سحات الضوئية وآلات التصوير في الجهة حسب المدة المحددة لكل مستوى.	٤-٧-٢

الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية (Third-Party and Cloud Computing Cybersecurity)



٣

				الأمن السيبراني المتعلق بالأطراف الخارجية	١-٣
				الصوابط	
مستوى تصنيف البيانات	الهدف				
سري للغاية	سري	مقيد	عام		
				بالإضافة للضوابط ضمن المكون الفرعى ٤ في الضوابط الأساسية للأمن السيبراني يجب أن تشمل متطلبات الأمان السيبراني المتعلقة بالأطراف الخارجية، بحد أدنى، ما يلى:	١-١-٣
✓	✓			إجراء المسح الأمني (Screening or Vetting) لموظفي الأطراف الخارجية الذين لديهم صلاحيات الاطلاع على البيانات.	١-١-١-٣
✓	✓	✓		وجود ضمانات تعاقدية على حذف بيانات الجهة بطرق آمنة لدى الطرف الخارجي عند الانتهاء/إنهاء العلاقة التعاقدية مع تقديم الأدلة على ذلك.	٢-١-١-٣
✓	✓	✓		توثيق كافة عمليات مشاركة البيانات مع الأطراف الخارجية، على أن يشمل ذلك مبررات مشاركة البيانات.	٣-١-١-٣
✓	✓	✓		عند مشاركة البيانات خارج المملكة يجب التتحقق من قدرة الجهة المستضيفة على حماية تلك البيانات والحصول على موافقة صاحب الصلاحية بالإضافة إلى الالتزام بالمتطلبات التشريعية والتنظيمية ذات العلاقة.	٤-١-١-٣
✓	✓	✓		إلزام الأطراف الخارجية بإبلاغ الجهة مباشرةً عند حدوث حادثة أمن سيبراني قد تؤثر على البيانات التي تمت مشاركتها أو إنشائها.	٥-١-١-٣
✓	✓	✓		إعادة تصفيف البيانات إلى أقل مستوى يحقق الهدف، قبل مشاركتها مع الأطراف الخارجية وذلك باستخدام تقنيات تعليم البيانات (Data Masking) أو تقنيات مزج البيانات (Data Scrambling).	٦-١-١-٣
				بما ينواتق مع المتطلبات التشريعية والتنظيمية ذات العلاقة، وبالإضافة إلى ما ينطبق من الضوابط الأساسية للأمن السيبراني والضوابط ضمن المكونات الرئيسية رقم (١) و (٢) و (٣) من هذه الوثيقة، يجب أن تخفي متطلبات الأمان السيبراني عند التعامل مع الجهات الاستشارية للمشاريع الاستراتيجية ذات الحساسية العالية على المستوى الوطني بحد أدنى، ما يلى:	٢-١-٣
✓	✓			إجراء المسح الأمني (Screening or Vetting) لموظفي شركات الخدمات الاستشارية الذين لديهم صلاحيات الاطلاع على البيانات.	١-٢-١-٣
✓	✓	✓		وجود ضمانات تعاقدية تشمل إلزام موظفي الخدمات الاستشارية بعدم إفشاء المعلومات وكذلك القدرة على حذف بيانات الجهة بطرق آمنة لدى شركات الخدمات الاستشارية عند الانتهاء/إنهاء العلاقة التعاقدية مع تقديم الأدلة على ذلك.	٢-٢-١-٣
✓	✓	✓		توثيق كافة عمليات مشاركة البيانات مع شركات الخدمات الاستشارية، على أن يشمل ذلك مبررات مشاركة البيانات.	٣-٢-١-٣
✓	✓	✓		إلزام شركات الخدمات الاستشارية بإبلاغ الجهة مباشرةً عند حدوث حادثة أمن سيبراني قد تؤثر على البيانات التي تمت مشاركتها أو إنشائها.	٤-٢-١-٣

✓	✓	✓		إعادة تصنيف البيانات إلى أقل مستوى يتحقق الهدف، قبل مشاركتها مع شركات الخدمات الاستشارية وذلك باستخدام تقنيات تعتمد على تغيير البيانات (Data Masking) أو تقنيات مزج البيانات (Data Scrambling).	٥-٢-١-٣
✓	✓			تحصيص قاعة مغلقة لموظفي شركات الخدمات الاستشارية لأداء أعمالهم، مع توفير أجهزة مخصصة مملوكة للجهة يتم من خلالها مشاركة البيانات ومعالجتها.	٦-٢-١-٣
✓	✓			تفعيل أنظمة التحكم بالدخول والخروج من القاعة المغلقة، على أن يكون للمصرح لهم فقط.	٧-٢-١-٣
✓	✓			منع خروج الأجهزة ووحدات التخزين والوثائق من القاعة المغلقة، ومنع إدخال أي أجهزة إلكترونية للقاعة.	٨-٢-١-٣

ملاحق

ملحق (أ): العلاقة مع الضوابط الأساسية للأمان السيبراني

تُعد ضوابط الأمان السيبراني للبيانات؛ امتداداً للضوابط الأساسية للأمان السيبراني (ECC- 1: 2018) كما هو موضح في الشكلين (٤) و (٥)، من خلال الآتي:

- تسعه مكونات فرعية، أضيفت لها ضوابط خاصة بالأمان السيبراني للبيانات.
- عشرون مكوناً فرعياً، لم يضاف لها ضوابط خاصة بالأمان السيبراني للبيانات.
- مكونان فرعيان جديدان، أضيفت لها ضوابط خاصة بالأمان السيبراني للبيانات.

مكونات فرعية أضيفت لها ضوابط خاصة للبيانات	
مكونات فرعية لم يضاف لها ضوابط خاصة للبيانات	
مكون فرعي جديد بضوابط الأمان السيبراني للبيانات	

شكل ٤: دليل ألوان المكونات الفرعية في الشكل ٥

ادارة الأمن السيبراني Cybersecurity Management		إستراتيجية الأمن السيبراني Cybersecurity Strategy		١ - حوكمة الأمن السيبراني Cybersecurity Governance	
أدوار ومسؤوليات الأمن السيبراني Cybersecurity Roles and Responsibilities		سياسات وإجراءات الأمن السيبراني Cybersecurity Policies and Procedures			
الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية Cybersecurity in Information Technology Projects		إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management			
المراجعة والتدقير الدوري للأمن السيبراني Periodical Cybersecurity Review and Audit	١ - ١	الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني Cybersecurity Regulatory Compliance			
برنامج التوعية والتدريب بالأمن السيبراني Cybersecurity Awareness and Training Program	٣ - ١	الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources	٢ - ١		
ادارة هويات الدخول والصلاحيات Identity and Access Management	١ - ٢	ادارة الأصول Asset Management		٢ - تعزيز الأمن السيبراني Cybersecurity Defense	
حماية البريد الإلكتروني Email Protection		حماية الأنظمة وأجهزة معالجة المعلومات Information System and Information Processing Facilities Protection			
أمن الأجهزة المحمولة Mobile Devices Security	٣ - ٢	ادارة أمن الشبكات Networks Security Management			
التشفير Cryptography	٥ - ٢	حماية البيانات والمعلومات Data and Information Protection	٤ - ٢		
ادارة الثغرات Vulnerabilities Management		ادارة النسخ الاحتياطية Backup and Recovery Management			
ادارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management		اختبار الاختراق Penetration Testing			
الأمن المادي Physical Security		ادارة حوادث وتهديدات الأمن السيبراني Cybersecurity Incident and Threat Management			
الإتلاف الآمن للبيانات Secure Data Disposal	٦ - ٢	حماية تطبيقات الويب Web Application Security			

الأمن السيبراني للطبعات ولماسحات الضوئية وآلات التصوير Cybersecurity for printers and scanners and copy machines	٧ - ٢	٣ - صمود الأمان السيبراني Cybersecurity Resilience
صمود الأمن السيبراني في إدارة استمرارية الأعمال Cybersecurity Resilience aspects of Business Continuity Management (BCM)	١-٣	٤ - الأمان السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية Third-Party and Cloud Computing Cybersecurity
الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة Cloud Computing and Hosting Cybersecurity	الأمن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity	٥ - الأمان السيبراني لأنظمة التحكم الصناعي ICS Cybersecurity
حماية أجهزة وأنظمة التحكم الصناعي Industrial Control Systems (ICS) Protection		

شكل ٥: مكونات الضوابط الأساسية للأمن السيبراني، وضوابط الأمان السيبراني للبيانات

ملحق (ب): مصطلحات وتعريفات

يوضح الجدول (٢) أدناه بعض المصطلحات وتعريفاتها، التي ورد ذكرها في هذه الضوابط.

التعريف	المصطلح
هي تقنيات تستخدم للحفاظ على البيانات المهمة، من الأشخاص غير المصرح لهم بالاطلاع عليها، ومنع تداولها خارج نطاق المنظمة في أي صورة تكون عليه هذه البيانات، ومكانها؛ سواءً كانت مخزنة على وحدات التخزين (In-rest) أو أجهزة المستخدمين، والحوادم (In-Use) أو متنقلة من خلال الشبكة (In-transit).	تقنيات منع تسريب البيانات
هو نظام تقني يستخدم لإدارة الأجهزة المحمولة للعاملين، ومراقبتها، وحمايتها بتطبيق سياسات الأمن السيبراني.	Data Leakage Prevention Technologies (DLP)
هي تقنيات تستخدم للحفاظ على البيانات المهمة، من الأشخاص غير المصرح لهم بالاطلاع عليها، وقصر معالجتها وفق الصلاحيات المحددة للمستخدم المصرح له.	نظام إدارة الأجهزة المحمولة Mobile Device Management (MDM) System
خدمات يتم تقديمها من قبل فريق استشاري متخصص حيث يقوم المستشارون بالاطلاع على بيانات ووثائق مختلفة للعميل، وقد تحوي بيانات سرية وحساسة، بغرض دراستها وتحليلها، والاستفادة من خبراتهم لتقديم المشورة ودراسات المقارنة والتوصية بأفضل الممارسات بما يتواكب مع احتياجات ومتطلبات العملاء. ويستثنى من نطاق الخدمات الاستشارية ما يتعلق بالخدمات الاحترافية للأمن السيبراني.	تقنيات إدارة الصلاحيات Rights Management Technologies
أمثلة:	الخدمات الاستشارية Consulting Services
• استشارات التحول الرقمي.	
• تحليل وتطوير الاستراتيجيات والتشريعات.	
خدمات يتم تقديمها من قبل مقدم خدمة مرخص/معتمد وفق ما يصدر من الهيئة بناءً على نطاق عمل محدد في مجال الأمن السيبراني، وترتजك تحديداً على مختلف أعمال التقييم والاستجابة.	الخدمات الاحترافية للأمن السيبراني Professional Cybersecurity Services
أمثلة :	
• تقييم الثغرات السيبرانية.	
• الاستجابة للحوادث السيبرانية.	
• تقييم المخاطر السيبرانية.	
خدمات احترافية تقدم بنموذج الاشتراك مع مقدم خدمات مرخص/معتمد وفق ما يصدر من الهيئة لإسناد بعض أعمال إدارة وتشغيل تقنية المعلومات والأمن السيبراني، وتشمل المنتجات والحلول والبرامج والأجهزة.	الخدمات المدارة Managed Services
أمثلة:	
• مراكز عمليات الأمن السيبراني المدارة (SOC).	
• خدمات تقنية المعلومات المدارة.	

جدول ٢ : مصطلحات وتعريفات

ملحق (ج): قائمة الاختصارات

يوضح الجدول (٣) أدناه، معنى الاختصارات التي ورد ذكرها في هذه الضوابط.

الاختصار	معنى
BYOD	Bring Your Own Device أحضر الجهاز الخاص بك
ECC	Essential Cybersecurity Controls الضوابط الأساسية للأمن السيبراني
MDM	Mobile Device Management إدارة الأجهزة المحمولة
NCS	National Cryptographic Standards المعايير الوطنية للتشифر
TLP	Traffic Light Protocol بروتوكول الإشارة الضوئية

جدول ٣ : قائمة الاختصارات

ملحق (د): العلاقة مع دورة حياة البيانات

يوضح الجدول (٤) أدناه العلاقة بين ضوابط الأمان السيبراني للبيانات ومراحل دورة حياة البيانات:

دورة حياة البيانات					الضوابط	
الإتلاف	الاستخدام	المشاركة	التخزين	الإنشاء	الضابط الفرعي	الضابط الأساسي
✓	✓	✓	✓	✓	_____	1-1-1
✓	✓	✓	✓	✓	_____	2-1-1
✓	✓	✓	✓	✓	1-1-2-1	1-2-1
	✓	✓	✓	✓	2-1-2-1	
✓	✓	✓	✓	✓	1-1-3-1	1-3-1
	✓	✓	✓		2-1-3-1	
	✓	✓	✓		3-1-3-1	
	✓	✓	✓		4-1-3-1	
✓					5-1-3-1	
	✓	✓	✓		6-1-3-1	
✓	✓	✓	✓		7-1-3-1	
	✓	✓			1-1-1-2	1-1-2
	✓	✓			2-1-1-2	
	✓	✓			_____	2-1-2
	✓	✓			_____	3-1-2
	✓	✓	✓	✓	1-1-2-2	
	✓	✓	✓	✓	2-1-2-2	1-2-2
	✓	✓	✓	✓	3-1-2-2	
	✓	✓	✓	✓	4-1-2-2	
✓	✓	✓	✓	✓	1-1-3-2	1-3-2
✓	✓	✓	✓	✓	2-1-3-2	
	✓	✓	✓	✓	1-1-4-2	
✓	✓	✓	✓	✓	2-1-4-2	1-4-2
	✓	✓	✓		3-1-4-2	
✓	✓	✓	✓	✓	4-1-4-2	
	✓	✓	✓	✓	1-1-0-2	1-0-2

دورة حياة البيانات					الضوابط	
الإتلاف	الاستخدام	المشاركة	التخزين	الإنشاء	الضابط الفرعي	الضابط الأساسي
	✓	✓	✓	✓	٢-١-٥-٢	
✓					١-١-٦-٢	١-٦-٢
✓					٢-١-٦-٢	
✓					٣-١-٦-٢	
✓					٤-١-٦-٢	
✓					٥-١-٦-٢	
	✓	✓			_____	١-٧-٢
	✓	✓			_____	٢-٧-٢
	✓	✓	✓		١-٣-٧-٢	٣-٧-٢
	✓	✓			٢-٣-٧-٢	
	✓	✓			٣-٣-٧-٢	
	✓	✓			٤-٣-٧-٢	
✓					٥-٣-٧-٢	
	✓	✓			_____	٤-٧-٢
	✓	✓	✓		١-١-١-٣	١-١-٣
✓	✓	✓	✓	✓	٢-١-١-٣	
	✓	✓			٣-١-١-٣	
	✓	✓	✓	✓	٤-١-١-٣	
	✓	✓	✓	✓	٥-١-١-٣	
	✓	✓	✓	✓	٦-١-١-٣	
	✓	✓	✓		١-١-٢-٣	١-٢-٣
✓	✓	✓	✓	✓	٢-١-٢-٣	
	✓	✓			٣-١-٢-٣	
	✓	✓	✓	✓	٤-١-٢-٣	
	✓	✓	✓	✓	٥-١-٢-٣	
	✓	✓	✓	✓	٦-١-٢-٣	
	✓	✓	✓	✓	٧-١-٢-٣	

جدول ٤: العلاقة مع دورة حياة البيانات



الهيئة الوطنية للذكاء الاصطناعي
National Cybersecurity Authority

