

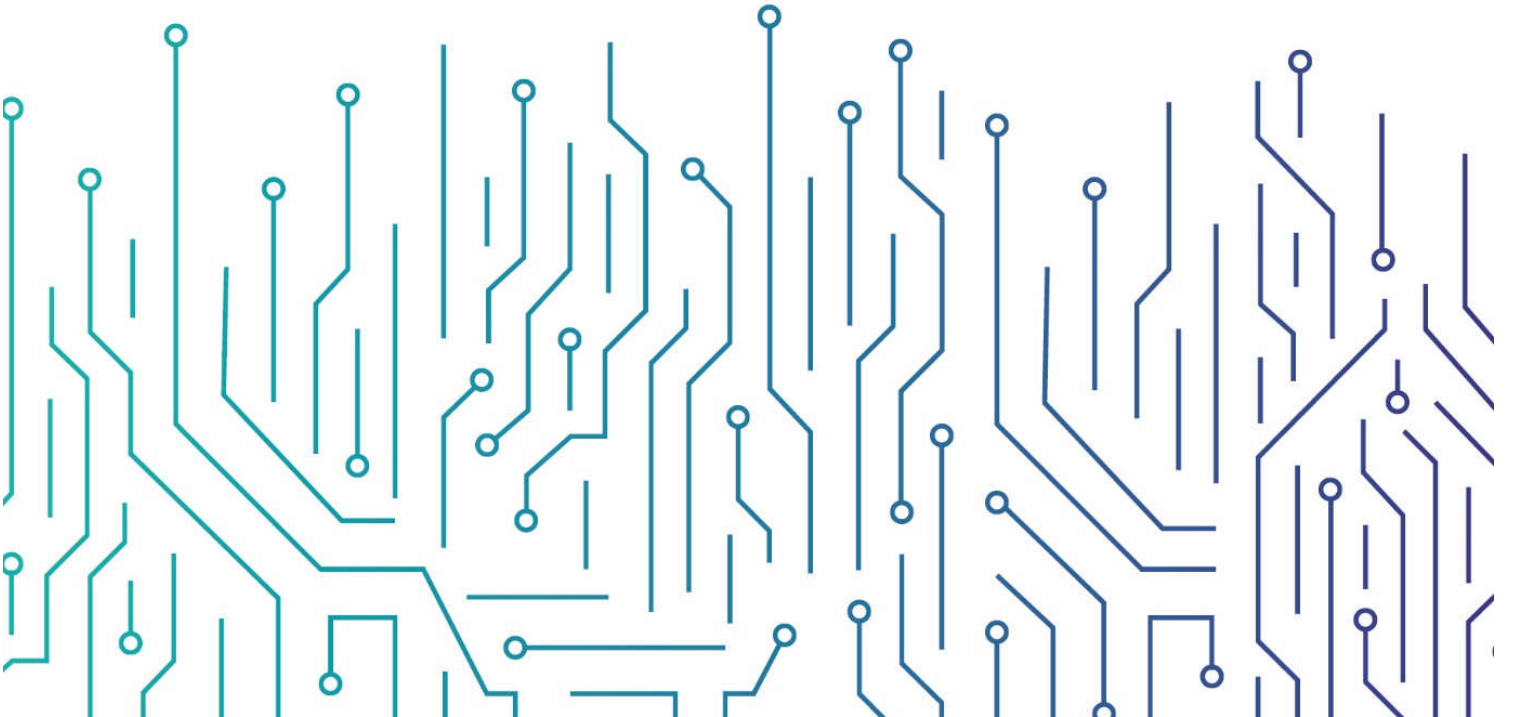


الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

ضوابط الأمن السيبراني للبينات

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 للاستلام.

برتقالي - مشاركة محدودة 

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

0	الملخص التنفيذي
٦	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 الأمن السيبراني للبيانات
٩	المكونات الأساسية والفرعية لضوابط الأمن السيبراني للبيانات
١٠	الهيكليّة
١١	ضوابط الأمن السيبراني للبيانات
١٩	ملاحق
١٩	ملحق (أ): العلاقة مع الضوابط الأساسية للأمن 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 الأمن 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 الأمن السيبراني للبيانات
١٠	شكل ٢ : معنى رموز ضوابط الأمن السيبراني للبيانات
١٠	شكل ٣ : هيكلية ضوابط الأمن السيبراني للبيانات
١٩	شكل ٤ : دليل ألوان المكونات الفرعية في الشكل ٥
٢٠	شكل ٥ : مكونات الضوابط الأساسية للأمن السيبراني، وضوابط الأمن 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 تنويع 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 سلباً على الأمن الوطني واقتصاد المملكة أو سمعتها أو علاقاتها الخارجية، أو على سلامة البنى 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 ١٤٣٩/٢/١١هـ على كونها الجهة المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه. وتشمل اختصاصاتها ومهامها وضع السياسات، وآليات الحوكمة، والأطر والمعايير، والضوابط، والإرشادات المتعلقة بالأمن السيبراني، وتعميمها 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 يُخلى أي جهة عامة أو خاصة، أو غيرها من مسؤوليتها تجاه أمنها السيبراني؛ وهو ما تضمنه الأمر السامي الكريم رقم (٥٧٢٣١) وتاريخ ١٤٣٩/١١/١٠هـ 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، وضوابط وإرشادات بهذا الشأن". وبهدف الوصول إلى فضاء سيبراني سعودي آمن وموثوق يُمكن النمو والازدهار؛ وامتداداً للضوابط الأساسية للأمن السيبراني (ECC - 1: 2018)، قامت الهيئة الوطنية للأمن السيبراني بإعداد ضوابط الأمن السيبراني للبيانات (DCC - 1: 2022) لوضع الحد الأدنى من متطلبات الأمن السيبراني لتمكين الجهات من حماية بياناتها خلال جميع مراحل دورة حياة البيانات. وتوضح هذه الوثيقة تفاصيل ضوابط الأمن 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 وآليات الحوكمة والأطر وتطبيق المعايير والضوابط التي تقرها الهيئة. وما تضمنه الأمر السامي الكريم رقم (٥٧٢٣١) وتاريخ ١٤٣٩/١١/١٠هـ.

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 والبنى 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، مقيد، سري، سري للغاية.

تتكون 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 الأمن السيبراني للبيانات إلى:
- رفع مستوى الأمن السيبراني لحماية البيانات الوطنية.
- تعزيز الأمن 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 والرقمية، 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 الأمن السيبراني لحماية البيانات.

قابلية التطبيق داخل الجهة

تم إعداد هذه الضوابط بحيث تكون ملائمة لمتطلبات الأمن 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

تحقيقًا لما ورد في الفقرة الثالثة من المادة العاشرة من تنظيم الهيئة الوطنية للأمن السيبراني، وكذلك ما ورد في الأمر السامي الكريم رقم (٥٧٢٣١) وتاريخ ١٤٣٩/١١/١٠ هـ، يجب على جميع الجهات ضمن نطاق عمل هذه الضوابط تنفيذ 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) وفقًا لقابلية تطبيقها في الجهة بحسب طبيعة أعمالها.

وتقوم الهيئة بتقييم التزام الجهات بما ورد في هذه الضوابط بطرق متعددة، منها: التقييم الذاتي للجهات، و/أو التقييم الخارجي، وذلك وفقًا 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 الأمن السيبراني للبيانات

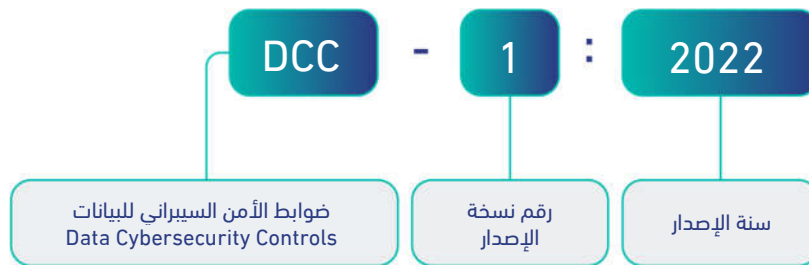
المكونات الأساسية والفرعية، لضوابط الأمن السيبراني للبيانات

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

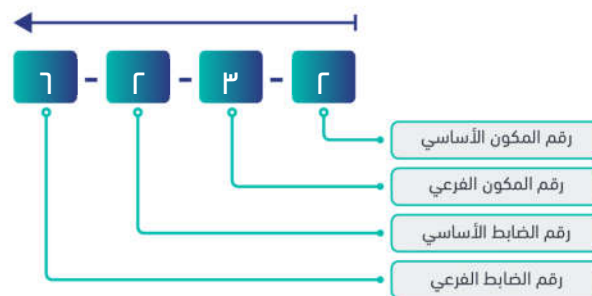
المراجعة والتدقيق الدوري للأمن السيبراني Periodical Cybersecurity Review and Audit	٢-١	الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources	١-١	١ - حوكمة الأمن السيبراني Cybersecurity Governance
برنامج التوعية والتدريب بالأمن السيبراني Cybersecurity Awareness and Training Program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

شكل ١ : المكونات الأساسية والفرعية لضوابط الأمن السيبراني للبيانات

يوضح الشكلان (٢) و (٣) أدناه معنى رموز ضوابط الأمن السيراني للبيانات.



شكل ٢ : معنى رموز ضوابط الأمن السيراني للبيانات



شكل ٣ : هيكلية ضوابط الأمن السيبراني للبيانات

يوضح الجدول ١ طريقة هيكلية ضوابط الأمن السيبراني للبيانات.

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

جدول ١ : هيكلية ضوابط الأمن السيبراني للبيانات

ضوابط الأمن السيبراني للبيانات

حوكمة الأمن السيبراني (Cybersecurity Governance)



المراجعة والتدقيق الدوري للأمن السيبراني (Periodical Cybersecurity Review and Audit)						١-١
ضمان التأكد من أن ضوابط الأمن السيبراني لدى الجهة مطبقة وتعمل وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المقررة تنظيمياً على الجهة.						الهدف
مستوى تصنيف البيانات				الضوابط		
عام	مقيد	سري	سري للغاية			
كل سنة على الأقل		رجوعاً للضابط ١-٨-١ في الضوابط الأساسية للأمن السيبراني، فإنه يجب على الإدارة المعنية بالأمن السيبراني في الجهة مراجعة تطبيق ضوابط الأمن السيبراني للبيانات حسب المدة المحددة لكل مستوى.				١-١-١
كل سنتين على الأقل	كل سنتين على الأقل	رجوعاً للضابط ٢-٨-١ في الضوابط الأساسية للأمن السيبراني، فإنه يجب أن تتم مراجعة تطبيق ضوابط الأمن 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
ضمان التأكد من أن مخاطر ومتطلبات الأمن السيبراني المتعلقة بالعاملين (موظفين ومتقاعدين) في الجهة تعالج بفعالية قبل وأثناء وعند انتهاء/إنهاء عملهم، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.						الهدف
مستوى تصنيف البيانات				الضوابط		
عام	مقيد	سري	سري للغاية			
		بالإضافة للضوابط الفرعية ضمن الضابط ٣-٩-١ في الضوابط الأساسية للأمن السيبراني يجب أن تغطي متطلبات الأمن السيبراني المتعلق بالموارد البشرية لتشمل خلال وبعد إنتهاء/إنهاء العلاقة الوظيفية في الجهة بحد أدنى ما يلي:				١-٢-١
✓	✓			١-١-٢-١ إجراء المسح الأمني (Screening and vetting) للعاملين في الوظائف ذات العلاقة بالتعامل مع البيانات.		
✓	✓	✓		٢-١-٢-١ 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.		
برنامج التوعية والتدريب بالأمن السيبراني (Cybersecurity Awareness and Training Program)						٣-١
ضمان التأكد من أن العاملين بالجهة لديهم التوعية الأمنية اللازمة وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني. والتأكد من تزويد العاملين بالجهة بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة والقيام بمسؤولياتهم تجاه الأمن السيبراني.						الهدف

مستوى تصنيف البيانات				الضوابط	
سري للغاية	سري	مقيد	عام	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:	١-٣-١
✓	✓	✓	✓	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 للطابعات والمساحات الضوئية وآلات التصوير.	٤-١-٣-١
✓	✓	✓		إجراءات الإلتلاف للأمن للبيانات.	٥-١-٣-١
✓	✓	✓	✓	مخاطر مشاركة الوثائق والمعلومات من خلال قنوات تواصل غير مؤمنة.	٦-١-٣-١
✓	✓	✓	✓	المخاطر السيبرانية المتعلقة باستخدام وسائط التخزين الخارجية.	٧-١-٣-١

تعزيز الأمن السيبراني (Cybersecurity Defense)



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

✓	✓			تعطيل خاصية تصوير الشاشة (Print Screen or Screen Capture) للأجهزة التي تنشئ أو تعالج الوثائق.	٤-١-٢-٢	
أمن الأجهزة المحمولة (Mobile Devices Security)						
الهدف						
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).						
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 (Mobile Device Management - MDM) وتفعيل خاصية الحذف عن بعد.	١-١-٣-٢	
يمنع استخدام أجهزة (BYOD)				إدارة أجهزة (BYOD) مركزياً باستخدام نظام إدارة الأجهزة المحمولة (Mobile Device Management - MDM) وتفعيل خاصية الحذف عن بعد.	٢-١-٣-٢	
حماية البيانات والمعلومات (Data and Information Protection)						
الهدف						
ضمان حماية السرية وسلامة بيانات ومعلومات الجهة ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.						
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 لترميز 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 تعقيم البيانات (Data Masking) أو تقنيات مزج البيانات (Data Scrambling).	٣-١-٤-٢	
✓	✓	✓	✓	استخدام خدمة حماية العلامة التجارية لحماية هوية الجهة من الانتحال (Brand Protection).	٤-١-٤-٢	

التشفير (Cryptography)					٥-٢	
الهدف					ضمان الاستخدام السليم والفعال للتشفير؛ لحماية الأصول المعلوماتية الإلكترونية للجهة، وذلك وفقاً للسياسات، والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.	
مستوى تصنيف البيانات				الضوابط		
عام	مقيد	سري	سري للغاية	١-٥-٢	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٨-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني للتشفير في الجهة، بحد أدنى، ما يلي:	
		✓	✓	١-١-٥-٢	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 – 1:2020).	
	✓			٢-١-٥-٢	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 – 1:2020).	
الإتلاف الآمن للبيانات (Secure Data Disposal)					٦-٢	
الهدف					ضمان تنفيذ عمليات إتلاف البيانات بشكل آمن، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.	
مستوى تصنيف البيانات				الضوابط		
عام	مقيد	سري	سري للغاية	١-٦-٢	يجب أن تغطي متطلبات الإتلاف الآمن للبيانات في الجهة بحد أدنى، ما يلي:	
	✓	✓	✓	١-١-٦-٢	تحديد التقنيات والأدوات والإجراءات لتنفيذ عمليات الإتلاف الآمن للبيانات حسب مستوى تصنيف البيانات.	
	✓	✓	✓	٢-١-٦-٢	عند انتهاء الحاجة لاستخدام وسائط التخزين بشكل نهائي، يجب أن يتم الإتلاف الآمن (Secure Disposal) لوسائط التخزين وذلك باستخدام التقنيات والأدوات واتباع الإجراءات التي تم تحديدها في الضابط رقم ٦-٢-١.	
	✓	✓	✓	٣-١-٦-٢	عند الحاجة لإعادة استخدام وسائط التخزين، يجب أن يتم الحذف الآمن للبيانات (Secure Erasure)، بحيث لا يمكن استرجاعها.	
	✓	✓	✓	٤-١-٦-٢	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.	
	✓	✓	✓	٥-١-٦-٢	الاحتفاظ بسجل لعمليات الإتلاف أو الحذف الآمن للبيانات التي تم تنفيذها.	
كل سنة على الأقل	كل ٦ أشهر على الأقل				٢-٦-٢	يجب مراجعة تطبيق متطلبات الإتلاف الآمن للبيانات في الجهة حسب المدة المحددة لكل مستوى.
الأمن السيبراني للطابعات والماسحات الضوئية وآلات التصوير (Cybersecurity for Printers, Scanners and Copy Machines)					٧-٢	
الهدف					ضمان التعامل الآمن مع البيانات عند استخدام الطابعات والماسحات الضوئية وآلات التصوير.	
مستوى تصنيف البيانات				الضوابط		
عام	مقيد	سري	سري للغاية	١-٧-٢	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية الطابعات والماسحات الضوئية وآلات التصوير في الجهة.	
	✓	✓	✓			

✓	✓	✓	يجب تطبيق متطلبات الأمن السيبراني للطابعات والماسحات الضوئية وآلات التصوير في الجهة.	٢-٧-٢
			يجب أن تغطي متطلبات الأمن السيبراني للطابعات والماسحات 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 والماسحات الضوئية والآلات التصوير المركزية قبل بدء عمليات الطباعة والتصوير والمسح الضوئي.	٢-٣-٧-٢
✓	✓		الاحتفاظ بطريقة آمنة بسجل الكتروني للعمليات الخاصة باستخدام الطابعات والماسحات الضوئية والآلات التصوير، لفترة لا تقل عن ١٢ شهرًا.	٣-٣-٧-٢
✓	✓		تفعيل وحماية سجلات المراقبة لأنظمة CCTV على مواقع أجهزة الطباعة المركزية والماسحات الضوئية والآلات التصوير.	٤-٣-٧-٢
✓	✓		استخدام أجهزة تمزيق الوثائق الورقية (Cross Shredding)، لإتلاف الوثائق في حال الانتهاء من استخدامها نهائيًا.	٥-٣-٧-٢
كل سنة على الأقل		كل ٣ سنوات على الأقل	يجب مراجعة متطلبات الأمن السيبراني للطابعات والماسحات 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)



الأمن السيبراني المتعلق بالأطراف الخارجية					١-٣
ضمان حماية أصول الجهة من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية بما في ذلك خدمات الإي ساند لتقنية المعلومات "Outsourcing" والخدمات المدارة "Managed Services" والخدمات الاستشارية "Consultancy Services" وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.					الهدف
مستوى تصنيف البيانات				الضوابط	
سري للغاية	سري	مقيد	عام	بالإضافة للضوابط ضمن المكون الفرعي ١-٤ في الضوابط الأساسية للأمن السيبراني، يجب أن تشمل متطلبات الأمن السيبراني المتعلقة بالأطراف الخارجية، بحد أدنى، ما يلي:	١-١-٣
✓	✓			١-١-٣ إجراء المسح الأمني (Screening or Vetting) لموظفي الأطراف الخارجية الذين لديهم صلاحيات الاطلاع على البيانات.	
✓	✓	✓		٢-١-٣ وجود ضمانات تعاقدية للقدرة على حذف بيانات الجهة بطرق آمنة لدى الطرف الخارجي عند الانتهاء/إنهاء العلاقة التعاقدية مع تقديم الأدلة على ذلك.	
✓	✓	✓		٣-١-٣ توثيق كافة عمليات مشاركة البيانات مع الأطراف الخارجية، على أن يشمل ذلك مبررات مشاركة البيانات.	
✓	✓	✓		٤-١-٣ عند مشاركة البيانات خارج المملكة يجب التحقق من قدرة الجهة المستضيفة على حماية تلك البيانات والحصول على موافقة صاحب الصلاحية بالإضافة إلى الالتزام بالمتطلبات التشريعية والتنظيمية ذات العلاقة.	
✓	✓	✓		٥-١-٣ إلزام الأطراف الخارجية بإبلاغ الجهة مباشرة عند حدوث حادثة أمن سيبراني قد تؤثر على البيانات التي تمت مشاركتها أو إنشائها.	
✓	✓	✓		٦-١-٣ إعادة تصنيف البيانات إلى أقل مستوى يحقق الهدف، قبل مشاركتها مع الأطراف الخارجية وذلك باستخدام تقنيات تعقيم البيانات (Data Masking) أو تقنيات مزج البيانات (Data Scrambling).	
				بما يتوافق 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 تغطي متطلبات الأمن السيبراني عند التعامل مع الجهات الاستشارية للمشاريع الاستراتيجية ذات الحساسية العالية على المستوى الوطني بحد أدنى، ما يلي:	٢-١-٣
✓	✓			١-٢-٣ إجراء المسح الأمني (Screening or Vetting) لموظفي شركات الخدمات الاستشارية الذين لديهم صلاحيات الاطلاع على البيانات.	
✓	✓	✓		٢-٢-٣ 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.	
✓	✓	✓		٣-٢-٣ توثيق كافة عمليات مشاركة البيانات مع شركات الخدمات الاستشارية، على أن يشمل ذلك مبررات مشاركة البيانات.	
✓	✓	✓		٤-٢-٣ إلزام شركات الخدمات الاستشارية بإبلاغ الجهة مباشرة عند حدوث حادثة أمن سيبراني قد تؤثر على البيانات التي تمت مشاركتها أو إنشائها.	

✓	✓	✓	إعادة تصنيف البيانات إلى أقل مستوى يحقق الهدف، قبل مشاركتها مع شركات الخدمات الاستشارية وذلك باستخدام تقنيات تعقيم البيانات (Data Masking) أو تقنيات مزج البيانات (Data Scrambling).	٥-٢-١-٣	
✓	✓		تخصيص 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 للأمن السيبراني

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

- تسعة مكونات فرعية، أضيفت لها ضوابط خاصة بالأمن السيبراني للبيانات.
- عشرون مكوناً فرعياً، لم يضاف لها ضوابط خاصة بالأمن السيبراني للبيانات.
- مكونان فرعيان جديداً، أضيفت لها ضوابط خاصة بالأمن السيبراني للبيانات.

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

شكل ٤: دليل ألوان المكونات الفرعية في الشكل ٥

إدارة 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 والتدقيق 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	
إدارة هويات الدخول والصلاحيات Identity and Access Management	١ - ٢	إدارة 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	٢ - ٢	
أمن الأجهزة المحمولة Mobile Devices Security	٣ - ٢	إدارة أمن الشبكات Networks Security Management		
التشفير Cryptography	٥ - ٢	حماية البيانات والمعلومات Data and Information Protection	٤ - ٢	
إدارة الثغرات Vulnerabilities Management		إدارة النسخ الاحتياطية Backup and Recovery Management		
إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management		اختبار الاختراق Penetration Testing		
الأمن المادي Physical Security		إدارة 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 للطابعات والماسحات الضوئية وآلات التصوير Cybersecurity for printers and scanners and copy machines		٧ - ٢	
صمود الأمن السيبراني في إدارة استمرارية الأعمال Cybersecurity Resilience aspects of Business Continuity Management (BCM)			٣ - صمود الأمن السيبراني Cybersecurity Resilience
الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة Cloud Computing and Hosting Cybersecurity	الأمن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity	١-٣	٤ - الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية Third-Party and Cloud Computing Cybersecurity
حماية أجهزة وأنظمة التحكم الصناعي Industrial Control Systems (ICS) Protection			٥ - الأمن السيبراني لأنظمة التحكم الصناعي ICS Cybersecurity

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

ملحق (ب): مصطلحات وتعريفات

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

المصطلح	التعريف
تقنيات منع تسريب البيانات Data Leakage Prevention Technologies (DLP)	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؛ سواء أكانت مخزنة على وحدات التخزين (In-rest) أو أجهزة المستخدمين، والخوادم (In-Use) أو متنقلة من خلال الشبكة (In-transit).
نظام إدارة الأجهزة المحمولة Mobile Device Management (MDM) System	هو نظام تقني يستخدم لإدارة الأجهزة المحمولة للعاملين، ومراقبتها، وحمايتها بتطبيق سياسات الأمن السيبراني.
تقنيات إدارة الصلاحيات Rights Management Technologies	هي تقنيات تستخدم للحفاظ على البيانات المهمة، من الأشخاص غير المصرح لهم بالاطلاع عليها، وقصر معالجتها وفق الصلاحيات المحددة للمستخدم المصرح له.
الخدمات الاستشارية Consulting Services	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 يتواءم مع احتياجات ومتطلبات العملاء. ويستثنى من نطاق الخدمات الاستشارية ما يتعلق بالخدمات الاحترافية للأمن السيبراني. أمثلة: <ul style="list-style-type: none"> استشارات التحول الرقمي. تحليل وتطوير الاستراتيجيات والتشريعات.
الخدمات الاحترافية للأمن السيبراني Professional Cybersecurity Services	خدمات يتم تقديمها من قبل مقدم خدمة مرخص/معتمد وفق ما يصدر من الهيئة بناءً على نطاق عمل محدد في مجال الأمن السيبراني، وترتكز تحديداً على مختلف أعمال التقييم والاستجابة. أمثلة: <ul style="list-style-type: none"> تقييم الثغرات السيبرانية. الاستجابة للحوادث السيبرانية. تقييم المخاطر السيبرانية.
الخدمات المدارة Managed Services	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. أمثلة: <ul style="list-style-type: none"> 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	معناه
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 للتشفير
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 الأمن السيبراني للبيانات ومراحل دورة حياة البيانات:

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

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 للأمن السيبراني
National Cybersecurity Authority

