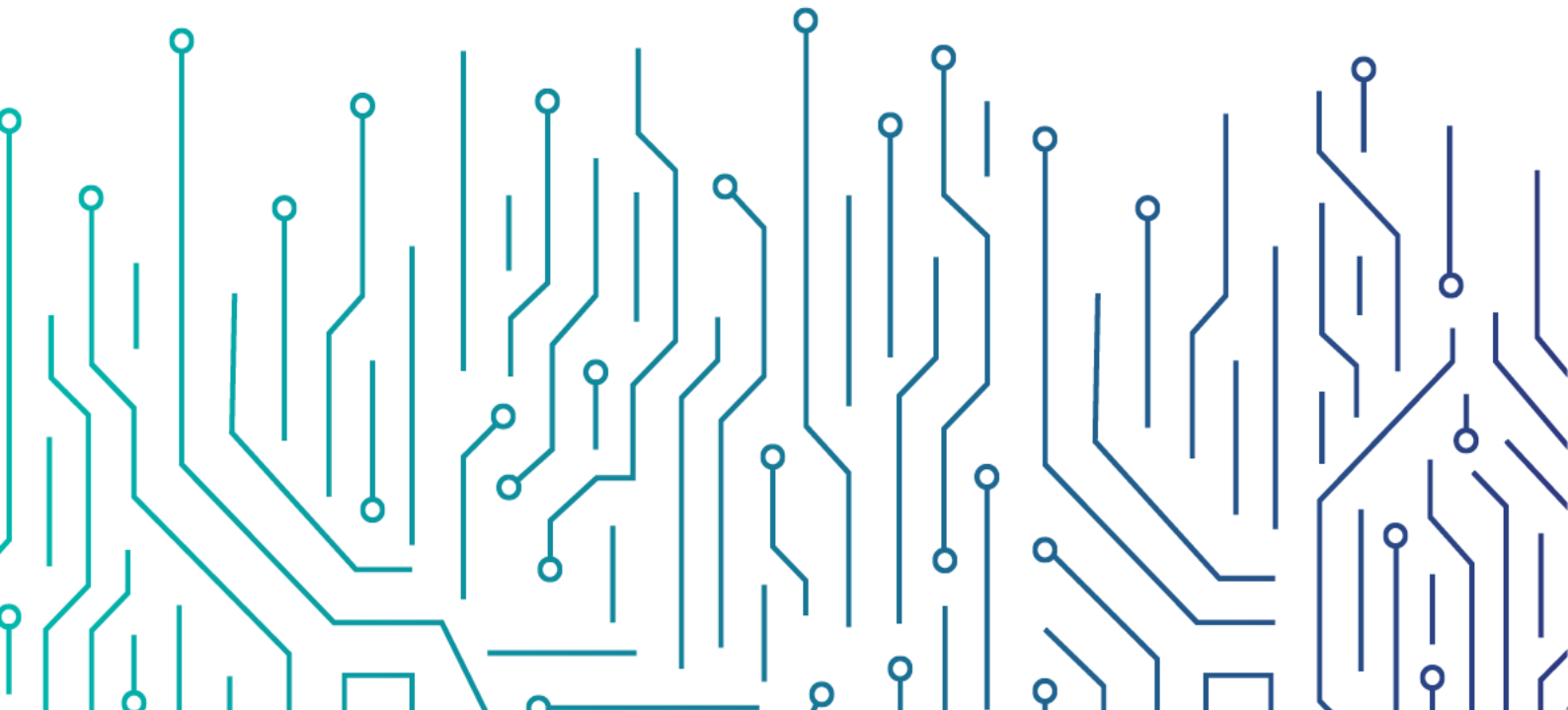
الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

مسودة ضوابط الأمن السيبراني للبيانات

Data Cybersecurity Controls
(DCC -1: 2021)

إشارة المشاركة: أبيض
تصنيف الوثيقة: عام



تصنيف الوثيقة: عام

متاح

بسم الله الرحمن الرحيم

تصنيف الوثيقة: عام

متاح

قائمة المحتويات

قائمة المحتويات ٤
الملخص التنفيذي ٥
المقدمة ٦
الأهداف ٧
نطاق العمل وقابلية التطبيق ٨
نطاق عمل الضوابط ٨
قابلية التطبيق داخل الجهة (Statement of Applicability) ٨
التنفيذ والالتزام ٩
التحديث والمراجعة ٩
مكونات وهيكلية ضوابط الأمن السيبراني للبيانات ١٠
المكونات الأساسية والفرعية لضوابط الأمن السيبراني للبيانات ١٠
الهيكلية ١١
ضوابط الأمن السيبراني للبيانات ١٢
ملاحق ١٨
ملحق (أ): العلاقة مع الضوابط الأساسية للأمن السيبراني ١٨
ملحق (ب): مصطلحات وتعريفات ٢٠
ملحق (ج): قائمة الاختصارات ٢١

قائمة الجداول

جدول ١ : هيكلية ضوابط الأمن السيبراني للبيانات ١١
جدول ٢ : مصطلحات وتعريفات ٢٠
جدول ٣ : قائمة الاختصارات ٢١

قائمة الأشكال والرسوم التوضيحية

شكل ١ : المكونات الأساسية والفرعية لضوابط الأمن السيبراني للبيانات ١٠
شكل ٢ : معنى رموز ضوابط الأمن السيبراني للبيانات ١١
شكل ٣ : هيكلية ضوابط الأمن السيبراني للبيانات ١١
شكل ٤ : مكونات الضوابط الأساسية للأمن السيبراني، وضوابط الأمن السيبراني للبيانات ١٩

الملخص التنفيذي

تسعى المملكة في ظل رؤية ٢٠٣٠ إلى تحقيق عدد من الأهداف الاقتصادية والتنموية والأمنية مما يعزز أداء الجهات الوطنية ويزيد من مستوى شفافيتها ومسؤوليتها، ويشجع على تنويع الاقتصاد والاستفادة من الخدمات المعتمدة على البيانات. وتعتبر البيانات الوطنية أحد أهم الأصول التي تسهم في تحقيق الأهداف الاستراتيجية للرؤية، وتعدُ موردًا اقتصاديًا لدعم المقومات التنافسية على المستوى الوطني، حيث تقوم الجهات الوطنية بجمع ومعالجة كميات هائلة من البيانات التي قد تكون عرضة للتهديدات والمخاطر السيبرانية المؤثرة سلبياً على الأمن الوطني واقتصاد المملكة أو سمعتها أو علاقاتها الخارجية، أو على البنى التحتية الوطنية الحساسة.

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 ومهماتها وضع السياسات، وآليات الحوكمة، والأطر والمعايير، والضوابط، والإرشادات المتعلقة بالأمن السيبراني وتحديثها، 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 يُخلي 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".

إن البيانات أصبحت عنصراً أساسياً ولها دور بارز في تدوير عجلة الاقتصاد والتنمية. ويعد الاهتمام بالبيانات ضرورياً لتحقيق الفعالية في دعم صناعة القرار والمساهمة في تحقيق رؤية المملكة العربية السعودية ٢٠٣٠، ومع تزايد اعتماد الجهات على الوسائل التقنية لإعداد وتخزين ومشاركة البيانات، تزداد التهديدات والمخاطر السيبرانية على البيانات، مما يستوجب وضع متطلبات الأمن السيبراني للحد من هذه التهديدات والمخاطر.

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: 2021) لوضع الحد الأدنى من متطلبات الأمن السيبراني لتمكين الجهات من حماية بياناتها خلال دورة حياتها الكاملة. وتوضح هذه الوثيقة تفاصيل ضوابط الأمن السيبراني للبيانات، وأهدافها، ونطاق العمل، وآلية الالتزام والمتابعة. ويستوجب على الجهة الأخذ في الاعتبار متطلبات ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC – 1:2019) في حال التعامل مع البيانات المصنفة على مستوى سري وسري للغاية. وعلى الجهة 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.

المقدمة

قامت الهيئة الوطنية للأمن السيبراني (ويشار لهـــا في هذه الوثيقة بـ "الهيئة") بإصـــــدار ضوابط الأمن السيبراني للبيـانات (DCC-1:2021)؛ بعد دراسة عدد من المعايير، والأطر والضوابط، ذات الأهداف المماثلة لدى جهات ومنظمات دولية. ومراعاة متطلبات التشريعات، والتنظيمات والقرارات الوطنية 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.

وعليه تم تصنيف البيانات بناءً على الأدوات التنظيمية الصادرة من مكتب إدارة البيانات الوطنية إلى أربعة تصنيفات بناءً على حساسيتها ومدى الحاجة إلى حمايتها من المخاطر، وهذه التصنيفات هي: عام، مقيد، سري، سري للغاية. مما يتطلب وجود ضوابط أمن سيبراني تساعد على تفادي 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 –وفقا لقابلية تطبيقها عليها- في المقام الأول كما تعد مرتبطة مع المتطلبات التشريعية، والتنظيمية الوطنية ذات العلاقة.

تتكون ضوابط الأمن السيبراني للبيانات من:

- ٣ مكونات أساسية (3 Main Domains)
- ١١ مكونات فرعية (11 Subdomains)
- ١٧ ضابطاً أساسياً (17 Main Controls)
- ٣٣ ضابطاً فرعياً (33 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 اشكال البيانات المادية والرقمية، والتي تشمل البيانات المهيكلة مثل قواعد البيانات وجداول البيانات والبيانات غير المهيكلة مثل الوثائق والمستندات.

كما تشجع الهيئة الجهات الأخرى في المملكة وبشدة على الاستفادة من هذه الضوابط لتطبيق أفضل الممارسات فيما يتعلق بتحسين الأمن السيبراني وتطويره داخل الجهة.

قابلية التطبيق داخل الجهة (Statement of Applicability)

تم إعداد هذه الضوابط بحيث تكون ملائمة لمتطلبات الأمن السيبراني لجميع الجهات والقطاعات في المملكة العربية السعودية بتنوع طبيعة أعمالها، ويجب على الجهة 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 (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) وفقاً 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 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 الأمن السيبراني للبيانات

المكونات الأساسية والفرعية، لضوابط الأمن السيبراني للبيانات

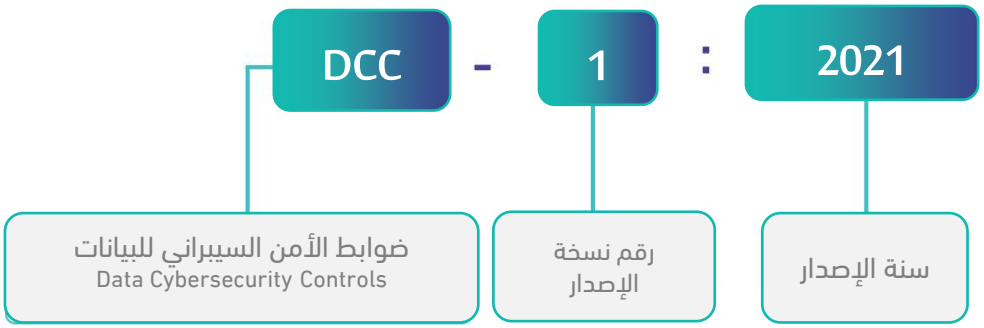
يوضح الشكل (١) أدناه، المكونات الأساسية والفرعية، لضوابط الأمن السيبراني للبيانات. كما يوضح ملحق (أ) العلاقة مع الضوابط الأساسية للأمن السيبراني.

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

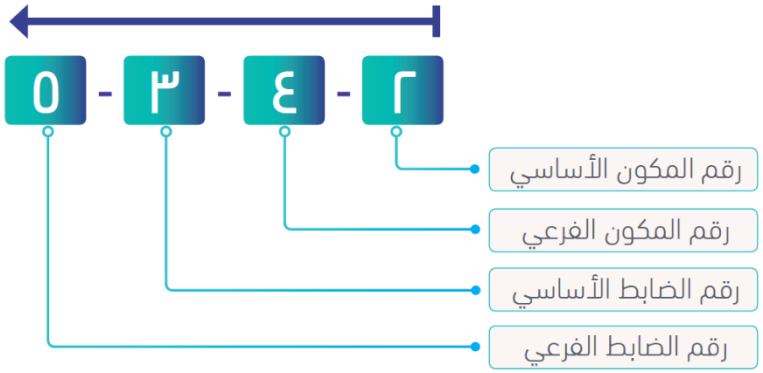
شكل ١ : المكونات الأساسية والفرعية لضوابط الأمن السيبراني للبيانات

الهيكلية

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



شكل ٢ : معنى رموز ضوابط الأمن السيبراني للبيانات



شكل ٣ : هيكلية ضوابط الأمن السيبراني للبيانات

يوضح الجدول ١ طريقة هيكلية ضوابط الأمن السيبراني للبيانات.

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

جدول ١ : هيكلية ضوابط الأمن السيبراني للبيانات

ضوابط الأمن السيبراني للبيانات

تفاصيل ضوابط الأمن السيبراني للبيانات

١. حوكمة الأمن السيبراني (Cybersecurity Governance)						
١-١	المراجعة والتدقيق الدوري للأمن السيبراني(Cybersecurity Periodical Assessment and Audit)					
الهدف	ضمان التأكد من أن ضوابط الأمن السيبراني لدى الجهة مطبقة وتعمل وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المقرة تنظيمياً على الجهة.					
الضوابط		مستوى تصنيف البيانات				
		عام	مقيد	سري	سري للغاية	
١-١-١	رجوعا 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.		كل ٣ سنوات على الأقل		كل سنة على الأقل	
١-١-٢	رجوعا للضابط ١ - ٨ -٢ في الضوابط الأساسية للأمن السيبراني ،فإنه يجب أن تتم مراجعة تطبيق ضوابط الأمن السيبراني البيانات من قبل أطراف مستقلة عن الإدارة المعنية بالأمن السيبراني من داخل الجهة حسب المدة المحددة لكل مستوى.		كل 5 سنوات على الأقل		كل ثلاث سنوات	
١-٢	الأمن السيبراني المتعلق بالموارد البشرية (Cybersecurity in Human Resources)					
الهدف	ضمان التأكد من أن مخاطر ومتطلبات الأمن 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.					
الضوابط		مستوى تصنيف البيانات				
١-٢-١	بالإضافة للضوابط الفرعية ضمن الضابط ١ -٩-٣ 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 مايلي:	عام	مقيد	سري	سري للغاية	
١-٢-١-١	إجراء المسح الأمني (Screening or vetting) للعاملين في الوظائف ذات العلاقة بالتعامل مع البيانات.			✓	✓	
١-٢-١-٢	تعهد العاملين في الجهة بعدم استخدام تطبيقات التواصل والتراسل الإجتماعي لإنشاء أو تخزين أو مشاركة البيانات الخاصة بالجهة، باستثناء تطبيقات الاتصال الآمنة المعتمدة من الجهات ذات العلاقة.		✓	✓	✓	
١-٣	برنامج التوعية والتدريب بالأمن السيبراني (Cybersecurity Awareness and Training Program)					
الهدف	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.					
الضوابط		مستوى تصنيف البيانات				
	بالإضافة للضوابط الفرعية ضمن الضابط ١ - ١٠- ٣ في الضوابط الأساسية للأمن السيبراني، فإنه يجب أن يغطي برنامج التوعية بالأمن السيبراني المحاور المتعلقة بحماية البيانات، بما في ذلك:	عام	مقيد	سري	سري للغاية	
١-٣-١	١-١-٣-١ مخاطر التسريب والوصول غير المصرح به للبيانات خلال دورة حياتها.	✓	✓	✓	✓	
	٢-١-٣-١ التعامل الآمن مع البيانات المصنفة خلال السفر والتواجد خارج مكان العمل.	✓	✓	✓	✓	

	١-٣-١-٣	التعامل الآمن مع البيانات خلال الاجتماعات (الافتراضية والحضورية).	✓	✓	✓	✓
	١-٣-١-٤	التعامل الآمن عند استخدام الطابعات والماسحات الضوئية وآلات التصوير.	✓	✓	✓	✓
	١-٣-١-٥	إجراءات الإتلاف الآمن للبيانات.	✓	✓	✓	✓
	١-٣-١-٦	مخاطر مشاركة الوثائق والمعلومات من خلال قنوات غير معتمدة.	✓	✓	✓	✓
	١-٣-١-٧	المخاطر المتعلقة باستخدام وحدات التخزين المتنقلة.	✓	✓	✓	✓

٢. تعزيز الأمن السيبراني (Cybersecurity Defense)						
٢-١	إدارة هويات الدخول والصلاحيات (Identity and Access Management)					
الهدف	ضمان حماية الأمن السيبراني للوصول المنطقي (Logical Access) إلى الأصول المعلوماتية والتقنية للجهة؛ من أجل منع الوصول غير المصرح به، وتقييد الوصول إلى ماهو مطلوب؛ لإنجاز الأعمال المتعلقة بالجهة.					
الضوابط		مستوى تصنيف البيانات				
٢-١-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٢-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني المتعلقة بإدارة هويات الدخول والصلاحيات، بحد أدنى، مايلي:	عام	مقيد	سري	سري للغاية
٢-١-١-١	التقييد الحازم للوصول والاطلاع ومشاركة البيانات بناء على قوائم صلاحيات معتمدة من صاحب الصلاحية (رئيس الجهة أو من ينيبه).			✓	✓
٢-١-١-٢	يمنع 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).		✓	✓	✓
٢-١-٣	رجوعاً للضابط الفرعي ٢-٢-٣-٥ في الضوابط الأساسية للأمن السيبراني، يجب مراجعة هويات الدخول والصلاحيات المستخدمة للتعامل مع البيانات.	كل سنة على الأقل		كل٦ أشهر على الأقل	
٢-٢	حماية الأنظمة وأجهزة معالجة المعلومات (Information System and 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				
٢-٢-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٣-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تشمل متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات، بحد أدنى، مايلي:	عام	مقيد	سري	سري للغاية
٢-٢-١-١	تطبيق حزم التحديثات، والإصلاحات الأمنية للأنظمة والخدمات المستخدمة للتعامل مع البيانات.	كل ستة أشهر على الأقل		كل ثلاثة أشهر على الأقل	
٢-٢-١-٢	مراجعة إعدادات الحماية والتحصين للأنظمة والخدمات المستخدمة للتعامل مع البيانات (Secure Configuration and Hardening).	كل سنة على الأقل		كل ٦ أشهر على الأقل	
٢-٢-١-٣	مراجعة وتحصين الإعدادت المصنعية (Default Configuration) للأصول التقنية للأنظمة والخدمات المستخدمة للتعامل مع البيانات، ومنها وجود كلمات مرور ثابتة، وخلفية افتراضية.	✓	✓	✓	✓
٢-٢-١-٤	تعطيل خاصية التصوير(Print Screen or Screen Capture) للأجهزة التي تنشئ أو تعالج الوثائق.			✓	✓
٢-٣	أمن الأجهزة المحمولة (Mobile Device 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 Bring Your Own Device (BYOD).					
الضوابط		مستوى تصنيف البيانات				
٢-٣-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٦-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة ، بحد أدنى، مايلي:	عام	مقيد	سري	سري للغاية
٢-٣-١-١	إدارة الأجهزة المحمولة المملوكة للجهة مركزياً باستخدام نظام إدارة الأجهزة المحمولة (Mobile Device Management – MDM) وتفعيل خاصية الحذف عن بعد.	✓	✓	✓	✓
٢-٣-١-٢	إدارة أجهزة (BYOD) مركزياً باستخدام نظام إدارة الأجهزة المحمولة (Mobile Device Management – MDM) وتفعيل خاصية الحذف عن بعد.	✓	✓	يمنع إستخدام أجهزة (BYOD)	

٢-٤	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.					
الضوابط		مستوى تصنيف البيانات				
٢-٤-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٧-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بحماية البيانات والمعلومات، بحد أدنى، مايلي:	عام	مقيد	سري	سري للغاية	
٢-٤-١-١	استخدام خاصية العلامات المائية لترميز كامل الوثيقة عند الإنشاء والحفظ والطباعة وعلى الشاشة وعلى كل نسخة (رقم تسلسلي يمكن تتبعه).			✓	✓	
٢-٤-١-٢	استخدام تقنيات منع تسريب البيانات (Data Leakage Prevention).		✓	✓	✓	
٢-٤-١-٣	عدم استخدام البيانات في غير بيئة الإنتاج (Production Enviroment) إلا بعد استخدام ضوابط مشددة لحماية تلك البيانات مثل تقنيات تعتيم البيانات (Data Masking) أو تقنيات مزج البيانات (Data Scrambling).		✓	✓	✓	
٢-٥	التشفير (Cryptography)					
الهدف	ضمان الاستخدام السليم والفعال للتشفير؛ لحماية الأصول المعلوماتية الإلكترونية للجهة، وذلك وفقاً للسياسات، والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.					
الضوابط		مستوى تصنيف البيانات				
٢-٥-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٨-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني للتشفير في الجهة، بحد أدنى، مايلي:	عام	مقيد	سري	سري للغاية	
٢-٥-١-١	استخدام طرق وخوارزميات محدثة وآمنة للتشفير عند الإنشاء والحفظ والنقل وعلى كامل الاتصال الشبكي المستخدم لنقل البيانات وفقاً للمستوى المتقدم (Advanced) ضمن المعايير الوطنية للتشفير (NCS – 1:2020).			✓	✓	
٢-٥-١-٢	استخدام طرق وخوارزميات محدثة وآمنة للتشفير عند الإنشاء والحفظ والنقل وعلى كامل الاتصال الشبكي المستخدم لنقل البيانات وفقاً للمستوى المتوسط (Moderate) ضمن المعايير الوطنية للتشفير (NCS – 1:2020).		✓			
٢-٦	الأمن المادي					
الهدف	ضمان حماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب.					
الضوابط		مستوى تصنيف البيانات				
٢-٦-١	رجوعاً للضابط الفرعي ٢-١٤-٣-٤ في الضوابط الأساسية للأمن السيبراني، يجب أن يغطي أمن اتلاف وإعادة استخدام الأصول المادية التي تحوي معلومات مصنفة (وتشمل: الوثائق الورقية ووسائط الحفظ والتخزين)، بحد أدنى مايلي:	عام	مقيد	سري	سري للغاية	
٢-٦-١-١	الحذف الكلي (Wiping) بإستخدام طرق وبرامج الحذف الآمنه للبيانات المحفوظة على وحدات التخزين.		✓	✓	✓	
٢-٦-١-٢	الإتلاف الكلي لوحدات التخزين الثابتة والمحمولة ، في حال الانتهاء من استخدامها نهائياً.			✓	✓	
٢-٦-١-٣	الاحتفاظ بسجل لعمليات الإتلاف والحذف التي تم تنفيذها.		✓	✓	✓	
٢-٦-١-٤	استخدام أجهزة تمزيق الوثائق الورقية (cross shredding).			✓	✓	
٢-٦-١-٥	تفعيل وحماية سجلات المراقبة لأنظمة CCTV على مواقع أجهزة الطباعة المركزية والماسحات الضوئية والآت التصوير.			✓	✓	

٢-7	الأمن السيبراني للطابعات والماسحات الضوئية وآلات التصوير (Cybersecurity for printers and scanners and copy machiense)				
الهدف	ضمان التعامل الآمن مع البيانات عند استخدام الطابعات والماسحات الضوئية وآلات التصوير.				
الضوابط		مستوى تصنيف البيانات			
		عام	مقيد	سري	سري للغاية
١-٧-٢	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية الطابعات والماسحات الضوئية في الجهة.		✓	✓	✓
٢-٧-٢	يجب تطبيق متطلبات الأمن السيبراني للطابعات والماسحات الضوئية وآلات التصوير في الجهة.		✓	✓	✓
٣-٧-٢	يجب أن تغطي متطلبات الأمن السيبراني للطابعات والماسحات الضوئية وآلات التصوير بحد أدنى، مايلي:				
١-٣-٧-٢	تعطيل خاصية التخزين المؤقت في الطابعات والماسحات الضوئية والآت التصوير المستخدمة للتعامل مع الوثائق والبيانات.		✓	✓	✓
٢-٣-٧-٢	تفعيل خاصية التحقق من الهوية في الطابعات والماسحات الضوئية والآت التصوير المركزية قبل عمليات الطباعة والتصوير والمسح الضوئي.		✓	✓	✓
٣-٣-٧-٢	الاحتفاظ بطريقة آمنة بسجل الكتروني للعمليات الخاصة باستخدام الطابعات والماسحات الضوئية والآت التصوير، لفترة لا تقل عن ١٨ شهراً.			✓	✓
٤-٧-٢	يجب مراجعة تطبيق متطلبات الأمن السيبراني للطابعات والماسحات الضوئية وآلات التصوير في الجهة	كل سنة على الأقل		كل ثلاثة أشهر على الأقل	

٣. الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية (Third-Party and Cloud Computing Cybersecurity)						
٣-١	الأمن السيبراني المتعلق بالأطراف الخارجية					
الهدف	ضمان حماية أصول الجهة من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية (بما في ذلك خدمات الإسناد لتقنية المعلومات "Outsourcing" والخدمات المدارة "Managed Services") وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.					
الضوابط			مستوى تصنيف البيانات			
			عام	مقيد	سري	سري للغاية
٣-١-١	بالإضافة للضوابط ضمن المكون الفرعي ١-٤ في الضوابط الأساسية للأمن السيبراني، يجب أن تشمل متطلبات الأمن السيبراني المتعلقة بالأطراف الخارجية، بحد أدنى، مايلي:					
	٣-١-١-١	إجراء المسح الأمني (Screening or Vetting) لموظفي خدمات الإسناد والخدمات المدارة الذين لديهم صلاحيات الاطلاع على البيانات.			✓	✓
	٣-١-١-٢	أن تكون خدمات الإسناد، والخدمات المدارة التي تتعامل مع البيانات، عن طريق شركات وجهات وطنية وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.			✓	✓
	٣-١-١-٣	وجود ضمانات تعاقدية للقدرة على حذف بيانات الجهة بطرق آمنة لدى الطرف الخارجي عند الانتهاء/إنهاء العلاقة التعاقدية مع تقديم الأدلة على ذلك.		✓	✓	✓

ملاحق

ملحق (أ): العلاقة مع الضوابط الأساسية للأمن السيبراني

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

- عشر مكونات فرعية، أضيفت لها ضوابط خاصة بالأمن السيبراني للبيانات.
- تسعة عشر مكوناً فرعياً، لم يضف لها ضوابط خاصة بالأمن السيبراني للبيانات.

	مكونات فرعية أضيف لها ضوابط خاصة للبيانات
	مكونات فرعية لم يضف لها ضوابط خاصة للبيانات

شكل٤: دليل ألوان المكونات الفرعية في الشكل 0

١ - حوكمة الأمن السيبراني Cybersecurity Governance	إستراتيجية الأمن السيبراني Cybersecurity Strategy		إدارة الأمن السيبراني Cybersecurity Management
	سياسات وإجراءات الأمن السيبراني Cybersecurity Policies and Procedures		أدوار ومسؤوليات الأمن السيبراني Cybersecurity Roles and Responsibilities
	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management		الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية Cybersecurity in Information Technology Projects
	الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني Cybersecurity Regulatory Compliance	١-١	المراجعة والتدقيق الدوري للأمن السيبراني Cybersecurity Periodical Assessment and Audit
	الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources	١-٣	برنامج التوعية والتدريب بالأمن السيبراني Cybersecurity Awareness and Training Program
	٢-١		
٢ - تعزيز الأمن السيبراني Cybersecurity Defense	إدارة الأصول Asset Management	٢ - ١	إدارة هويات الدخول والصلاحيات Identity and Access Management
	حماية الأنظمة وأجهزة معالجة المعلومات Information System and Processing Facilities Protection	٢ - ٢	حماية البريد الإلكتروني Email Protection
	إدارة أمن الشبكات Networks Security Management	٢ - ٣	أمن الأجهزة المحمولة Mobile Devices Security
	حماية البيانات والمعلومات Data and Information Protection	٢ - ٥	التشفير Cryptography
	٢-٤		
	إدارة النسخ الاحتياطية Backup and Recovery Management		إدارة الثغرات Vulnerabilities Management
	اختبار الاختراق Penetration Testing		إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management
	إدارة حوادث وتهديدات الأمن السيبراني Cybersecurity Incident and Threat Management	٢-٦	الأمن المادي Physical Security
	حماية تطبيقات الويب Web Application Security	٢-٧	الأمن السيبراني للطابعات والماسحات الضوئية وآلات التصوير (Cybersecurity for printers and scanners and copy machiense
٣ - صمود الأمن السيبراني Cybersecurity Resilience	صمود الأمن السيبراني في إدارة استمرارية الأعمال Cybersecurity Resilience aspects of Business Continuity Management (BCM)		
٤ - الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية Third-Party and Cloud Computing Cybersecurity	الأمن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity	٣-١	الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة Cloud Computing and Hosting Cybersecurity
٥ - الأمن السيبراني لأنظمة التحكم الصناعي ICS Cybersecurity	حماية أجهزة وأنظمة التحكم الصناعي Industrial Control Systems (ICS) Protection		

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.

جدول ٢ : مصطلحات وتعريفات

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.

ملحق (ج): قائمة الاختصارات

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

جدول ٣ : قائمة الاختصارات

الاختصار	معناه
BYOD	Bring Your Own Device سياسة أحضر الجهاز الخاص بك
DDoS	Distributed Denial of Service Attack هجمات تعطيل الخدمات الموزعة
ECC	Essential Cybersecurity Controls الضوابط الأساسية للأمن السيبراني
MDM	Mobile Device Management إدارة الأجهزة المحمولة
TLP	Traffic Light Protocol بروتوكول الإشارة الضوئية