ملحق (ج): قائمة التحديثات

يوضح الجدول ٤ أدناه التحديثات التي تم إجراؤها على النسخة السابقة من وثيقة الضوابط الأساسية للأمن السيبراني (ECC – 1 : 2018).

جدول ٤: قائمة التحديثات

النسخة	التاريخ			
ECC – 2 : 2024	2024			
نوع التحديث	القسم	النص السابق	النص بعد التحديث	سبب التحديث
تعديل	نطاق عمل الضوابط	تُطبَّق هذه الضوابط على الجهات الحكومية في المملكة العربية السعودية (وتشمل الوزارات والهيئات والمؤسسات وغيرها) والجهات والشركات التابعة لها	تُطبَّق هذه الضوابط على الجهات الحكومية في المملكة العربية السعودية (وتشمل الوزارات والهيئات والمؤسسات وغيرها) والجهات والشركات التابعة لها (داخل المملكة وخارجها)	إيضاح للنص
حذف	قابلية التطبيق داخل الجهة	الضوابط ضمن المكون الرئيسي رقم (٥) المتعلقة بالأمن السيبراني لأنظمة التحكم الصناعي (Industrial Control Systems Cybersecurity) تكون قابلة التطبيق وملزمة على الجهة التي تستخدم حالياً أنظمة التحكم الصناعي أو تخطط لاستخدامها.		حذف المكون الأساسي الخامس تم نقل الضوابط ضمن المكون الأساسي الخامس إلى وثيقة ضوابط الأمن السيبراني للأنظمة التشغيلية
تعديل	الضابط ١-٢-٢	يجب أن يشغل رئاسة الإدارة المعنية بالأمن السيبراني والوظائف الإشرافية والحساسة بها مواطنون متفرغون وذو كفاءة عالية في مجال الأمن السيبراني.	يجب شغل جميع وظائف الأمن السيبراني من قبل مواطنين متفرغين وذوي كفاءة في مجال الأمن السيبراني.	تعزيز الأمن السيبراني
حذف	الضابط ١-٧-١	يجب على الجهة الالتزام بالمتطلبات التشريعية والتنظيمية الوطنية المتعلقة بالأمن السيبراني.		النضج التنظيمي للأمن السيبراني ودعم التزام الجهات
تعديل	الضابط ١-٧-٢	في حال وجود اتفاقيات أو التزامات دولية معتمدة محلياً تتضمن متطلبات خاصة بالأمن السيبراني، فيجب على الجهة الالتزام بتلك المتطلبات.	في حال وجود اتفاقيات أو التزامات دولية معتمدة محلياً تتضمن متطلبات خاصة بالأمن السيبراني، فيجب على الجهة حصر تلك المتطلبات والالتزام بها.	إيضاح النص

تعديل	الضابط ١-٩-٥	يجب مراجعة وإلغاء الصلاحيات للعاملين مباشرة بعد انتهاء/إنهاء الخدمة المهنية لهم بالجهة.	يجب مراجعة وإلغاء الصلاحيات للعاملين مباشرة بعد انتهاء/إنهاء العلاقة الوظيفية مع الجهة.	إيضاح النص
تعديل	الضابط الفرعي ١-٣-٢-٢	التحقق من هوية المستخدم (User Authentication) بناءً على إدارة تسجيل المستخدم، وإدارة كلمة المرور.	التحقق من الهوية أحادي العنصر (Single-factor authentication) بناءً على إدارة تسجيل المستخدم، وإدارة كلمة المرور.	إيضاح للنص
تعديل	الضابط الفرعي ٢-٣-٢-٢	التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) لعمليات الدخول عن بعد.	التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) وتحديد عناصر التحقق المناسبة وعددها وكذلك تقنيات التحقق المناسبة بناء على نتائج تقييم الأثر المحتمل لفشل عملية التحقق وتخطيها، وذلك لعمليات الدخول عن بعد والحسابات ذات الصلاحيات الهامة والحساسة.	إيضاح للنص
تعديل	الضابط الفرعي ٢-٣-٤-٢	التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) للدخول عن بعد والدخول عن طريق صفحة موقع البريد الإلكتروني (Webmail).	التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) وتحديد عناصر التحقق المناسبة وعددها وكذلك تقنيات التحقق المناسبة بناء على نتائج تقييم الأثر المحتمل لفشل عملية التحقق وتخطيها، وذلك للدخول عن بعد والدخول عن طريق صفحة موقع البريد الإلكتروني (Webmail).	إيضاح للنص
تعديل	الضابط الفرعي ٢-٣-٤-٥	توثيق مجال البريد الإلكتروني للجهة بالطرق التقنية، مثل طريقة إطار سياسة المرسل (Sender Policy Framework).	توثيق مجال البريد الإلكتروني للجهة باستخدام إطار سياسة المرسل (Sender Policy Framework "SPF") والبريد المعرّف بمفاتيح النطاق (Domain Keys Identified Mail "DKIM") وسياسة مصادقة الرسائل والإبلاغ عنها (Domain Message Authentication Reporting and Conformance "DMARC").	إيضاح للنص

إضافة	الضابط الفرعي ٢-٥-٣-٩	لا يوجد	الحماية من هجمات تعطيل الشبكات (Distributed Denial of Service Attack "DDoS") للحد من المخاطر السيبرانية الناتجة عن هجمات تعطيل الشبكات.	تعزيز الأمن السيبراني
تعديل	الضابط ٢-٧-٢	يجب تطبيق متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجهة.	يجب تطبيق متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجهة، حسب مستوى تصنيفها.	إيضاح النص
حذف	الضابط ٢-٧-٣	يجب أن تغطي متطلبات الأمن السيبراني لحماية البيانات والمعلومات بحد أدنى ما يلي: ٢-٧-٣-١ ملكية البيانات والمعلومات ٢-٧-٣-٢ تصنيف البيانات والمعلومات وآلية ترميزها (Classification and Labeling Mechanisms). ٢-٧-٣-٣ خصوصية البيانات والمعلومات.		للاختصاص التنظيمي، يجب على الجهات الرجوع إلى مكتب إدارة البيانات الوطنية بالهيئة السعودية للبيانات والذكاء الاصطناعي فيما يخص تصنيف وخصوصية البيانات قبل اتخاذ أي إجراء في هذا الشأن.
تعديل	الهدف من المكون الفرعي ٢-٨	ضمان الاستخدام السليم والفعال للتشفير لحماية الأصول المعلوماتية الإلكترونية للجهة، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.	ضمان الاستخدام السليم والفعال للتشفير لحماية الأصول المعلوماتية الإلكترونية للجهة، وذلك وفقاً للمعايير الوطنية للتشفير الصادرة من الهيئة، وللسياسات والإجراءات التنظيمية للجهة، وبناء على تقييم المخاطر، وبحسب المتطلبات التشريعية والتنظيمية ذات العلاقة.	
تعديل	الضابط ٢-٨-٣	يجب أن تغطي متطلبات الأمن السيبراني للتشفير بحد أدنى ما يلي:	يجب أن تغطي متطلبات الأمن السيبراني للتشفير بحد أدنى المتطلبات المذكورة في المعايير الوطنية للتشفير الصادرة من الهيئة، مع تطبيق مستوى التشفير المناسب، وذلك بحسب طبيعة ومستوى حساسية البيانات والأنظمة والشبكات وبناءً على تقييم المخاطر من قبل الجهة وحسب المتطلبات التشريعية والتنظيمية ذات العلاقة، وفقاً لما يلي:	إيضاح للنص

تعديل	الضابط الفرعي ٢-١٠-٣-٤	إدارة حزم التحديثات والإصلاحات الأمنية لمعالجة الثغرات.	إدارة حزم التحديثات والإصلاحات الأمنية لمعالجة الثغرات، على أن يتم التحقق من سلامة وفعالية تلك التحديثات والإصلاحات الأمنية على بيئة غير بيئة الإنتاج قبل تطبيقها.	إيضاح للنص
تعديل	الضابط الفرعي ٢-١٥-٣-٥	التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) لعمليات دخول المستخدمين.	التحقق من الهوية على أن يتم تحديد عناصر التحقق المناسبة وعددها وكذلك تقنيات التحقق المناسبة بناء على نتائج تقييم الأثر المحتمل لفشل عملية التحقق وتخطيها، وذلك لعمليات دخول المستخدمين.	إيضاح للنص
تعديل	الهدف من المكون الفرعي ٤-١	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.	ضمان حماية أصول الجهة من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية (بما في ذلك خدمات الإسناد للأمن السيبراني أو لتقنية المعلومات "Outsourcing" والخدمات المدارة "Managed Services"). وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.	إيضاح النص
تعديل	الضابط ٤-١-٣	يجب أن تغطي متطلبات الأمن السيبراني مع الأطراف الخارجية التي تقدم خدمات إسناد لتقنية المعلومات، أو خدمات مدارة بحد أدنى ما يلي:	يجب أن تغطي متطلبات الأمن السيبراني مع الأطراف الخارجية التي تقدم خدمات الإسناد للأمن السيبراني أو لتقنية المعلومات، أو الخدمات المدارة بحد أدنى ما يلي:	إيضاح النص
تعديل	الضابط الفرعي ٤-٢-٣-١	تصنيف البيانات قبل استضافتها لدى مقدمي خدمات الحوسبة السحابية والاستضافة، وإعادتها للجهة (بصيغة قابلة للاستخدام) عند انتهاء الخدمة.	حماية بيانات الجهة من قبل مقدمي خدمات الحوسبة السحابية والاستضافة بما يتوافق مع مستوى تصنيفها، وإعادتها للجهة (بصيغة قابلة للاستخدام) عند انتهاء الخدمة.	تعزيز الأمن السيبراني
حذف	الضابط الفرعي ٤-٢-٣-٣	موقع استضافة وتخزين معلومات الجهة يجب أن يكون داخل المملكة.		تم نقل الضوابط ذات العلاقة بتوطين وسيادة البيانات من الوثيقة إلى الهيئة السعودية للبيانات والذكاء الاصطناعي

				للاختصاص التنظيمي، ويجب على الجهات الرجوع إلى مكتب إدارة البيانات الوطنية بالهيئة السعودية للبيانات والذكاء الاصطناعي فيما يخص توطين وسيادة البيانات قبل اتخاذ أي إجراء في هذا الشأن.
حذف	المكون الأساسي الخامس	الأمن السيبراني لأنظمة التحكم الصناعي		تم نقل الضوابط ضمن المكون الأساسي الخامس إلى وثيقة ضوابط الأمن السيبراني للأنظمة التشغيلية
تعديل	مصطلحات وتعريفات	**المعلومات (أو البيانات) الحساسة Confidential Data/Information**	**المعلومات (أو البيانات) الحساسة Sensitive Data/Information**	تحديث الترجمة
تعديل	مصطلحات وتعريفات	**البنية التحتية الوطنية الحساسة Critical National Infrastructure** تلك العناصر الأساسية للبنية التحتية (أي الأصول، والمرافق، والنظم، والشبكات، والعمليات، والعاملون الأساسيون الذين يقومون بتشغيلها ومعالجتها)، والتي قد يؤدي فقدانها أو تعرضها لانتهاكات أمنية إلى: • أثر سلبي كبير على توافر الخدمات الأساسية أو تكاملها أو تسليمها -بما في ذلك الخدمات التي يمكن أن تؤدي في حال تعرضت سلامتها للخطر إلى خسائر كبيرة في الممتلكات و/أو الأرواح و/أو الإصابات- مع مراعاة الآثار الاقتصادية و/أو الاجتماعية الكبيرة. • تأثير كبير على الأمن القومي و/أو الدفاع الوطني و/أو اقتصاد الدولة أو مقدراتها الوطنية.	**البنية التحتية الوطنية الحساسة Critical National Infrastructure** تلك العناصر الأساسية للبنية التحتية (أي الأصول، والمرافق، والنظم، والشبكات، والعمليات، والعاملون الأساسيون الذين يقومون بتشغيلها ومعالجتها)، والتي قد يؤدي فقدانها أو تعرضها لانتهاكات أمنية إلى: • أثر سلبي كبير على توافر الخدمات الأساسية أو تكاملها أو تسليمها -بما في ذلك الخدمات التي يمكن أن تؤدي في حال تعرضت سلامتها للخطر إلى خسائر كبيرة في الممتلكات و/أو الأرواح و/أو الإصابات- مع مراعاة الآثار الاقتصادية و/أو الاجتماعية على المستوى الوطني.	إيضاح للنص

			• تأثير كبير على الأمن الوطني و/أو الدفاع الوطني و/أو اقتصاد الدولة أو مقدراتها الوطنية.	
تعديل	مصطلحات وتعريفات	**الهجوم السيبراني** **Cyber-Attack** الاستغلال المتعمّد لأنظمة الحاسب الآلي والشبكات والجهات التي يعتمد عملها على تقنية المعلومات والاتصالات الرقمية بهدف إحداث أضرار.	**الهجوم السيبراني** **Cyber-Attack** محاولة متعمدة للتأثير السلبي على الأمن السيبراني، سواءً نجحت في ذلك أو لم تنجح.	إيضاح للنص
تعديل	مصطلحات وتعريفات	**حدث** **Event** شيء يحدث في مكان محدد (مثل الشبكة والأنظمة والتطبيقات وغيرها) وفي وقت محدد.	**حدث** **Event** حدث ذو علاقة بحالة الأمن السيبراني الخاصة بشبكة، أو نظام، أو خدمة، أو بيانات، أو أي جهاز تقني آخر.	إيضاح للنص
تعديل	مصطلحات وتعريفات	**حادثة** **Incident** انتهاك أمني بمخالفة سياسات الأمن السيبراني أو سياسات الاستخدام المقبول أو ممارسات أو ضوابط أو متطلبات الأمن السيبراني.	**حادثة** **Incident** حدث متعمد أو غير متعمد تسبب في التأثير السلبي على الأمن السيبراني.	إيضاح للنص
تعديل	مصطلحات وتعريفات	**المتطلبات الوطنية والدولية** **(Inter)National Requirements** المتطلبات الوطنية هي متطلبات طورتها جهة تشريعية في المملكة العربية السعودية للاستخدام بشكل تنظيمي (مثل: الضوابط الأساسية للأمن السيبراني "ECC – 1 : 2018"). المتطلبات الدولية هي متطلبات طورتها جهة أو منظمة دولية عالمية للاستخدام بشكل تنظيمي في جميع أنحاء العالم (مثل:SWIFT ، PCI، وغيرها).	**المتطلبات الدولية** **International Requirements** المتطلبات الدولية هي متطلبات طورتها جهة أو منظمة دولية عالمية للاستخدام بشكل تنظيمي في جميع أنحاء العالم (مثل:SWIFT ، PCI، وغيرها).	إيضاح للنص

تعديل	مصطلحات وتعريفات	**التحقق من الهوية متعدد العناصر Multi-Factor Authentication (MFA)** نظام أمني يتحقق من هوية المستخدم، يتطلب استخدام عدة عناصر مستقلة من آليات التحقق من الهوية. تتضمن آليات التحقق عدة عناصر: • المعرفة (شيء يعرفه المستخدم فقط "مثل كلمة المرور"). • الحيازة (شيء يملكه المستخدم فقط "مثل برنامج أو جهاز توليد أرقام عشوائية أو الرسائل القصيرة المؤقتة لتسجيل الدخول"، ويطلق عليها "One-Time-Password"). • الملازمة (صفة أو سمة حيوية متعلقة بالمستخدم نفسه فقط "مثل بصمة الإصبع").	**التحقق من الهوية متعدد العناصر Multi-Factor Authentication (MFA)** نظام أمني يتحقق من هوية المستخدم، باستخدام عدة عناصر من خلال تقنيات التحقق من الهوية. عناصر التحقق من الهوية هي: • المعرفة (شيء يعرفه المستخدم فقط "مثل استخدام تقنية كلمة المرور"). • الحيازة (شيء يملكه المستخدم فقط "مثل استخدام تقنية برنامج أو جهاز توليد أرقام عشوائية أو الرسائل القصيرة المؤقتة لتسجيل الدخول"، ويطلق عليها "One-Time-Password"). • الملازمة (صفة أو سمة حيوية متعلقة بالمستخدم نفسه فقط "مثل استخدام تقنية بصمة الإصبع أو الوجه").	إيضاح للنص
حذف	مصطلحات وتعريفات	**الخصوصية Privacy** الحرية من التدخل غير المصرح به أو الكشف عن معلومات شخصية حول فرد.		للاختصاص التنظيمي، يجب على الجهات الرجوع إلى مكتب إدارة البيانات الوطنية بالهيئة السعودية للبيانات والذكاء الاصطناعي فيما يخص خصوصية البيانات قبل اتخاذ أي إجراء في هذا الشأن.

تعديل	مصطلحات وتعريفات	**تهديد** **Threat** أي ظرف أو حدث من المحتمل أن يؤثر سلباً على أعمال الجهة (بما في ذلك مهمتها أو وظائفها أو مصداقيتها أو سمعتها) أو أصولها أو منسوبيها مستغلاً أحد أنظمة المعلومات عن طريق الوصول غير المصرح به إلى المعلومات أو تدميرها أو كشفها أو تغييرها أو حجب الخدمة. وأيضاً قدرة مصدر التهديد على النجاح في استغلال أحد نقاط الضعف الخاصة بنظام معلومات معين. وهذا التعريف يشمل التهديدات السيبرانية.	**تهديد** **Threat** أي شيء قد يؤثر سلبًا على الأمن السيبراني.	إيضاح للنص
تعديل	مصطلحات وتعريفات	**الثغرة** **Vulnerability** أي نوع من نقاط الضعف في نظام الحاسب الآلي، أو برامجه أو تطبيقاته، أو في مجموعة من الإجراءات، أو في أي شيء يجعل الأمن السيبراني عرضة للتهديد.	**الثغرة** **Vulnerability** ضعف في أي أصل تقنية معلومات (مثال: برنامج، نظام)، أو إجراء، أو ضابط، أو أي شيء؛ يمكن استغلاله للتأثير السلبي على الأمن السيبراني.	إيضاح للنص
إضافة	قائمة الاختصارات		DDoS :Distributed Denial of Service Attack هجمات تعطيل الشبكات DKIM :Domain Keys Identified Mail البريد المعرّف بمفاتيح النطاق DMARC :Domain Message Authentication Reporting and Conformance سياسة مصادقة الرسائل والإبلاغ عنها SPF: Sender Policy Framework إطار سياسة المرسل	إضافة اختصارات تمت إضافتها للوثيقة
حذف	قائمة الاختصارات	ICS :Industrial Control System نظام التحكم الصناعي SIS :Safety Instrumented System نظام معدات السلامة		تم نقل الضوابط ضمن المكون الأساسي الخامس إلى وثيقة ضوابط الأمن السيبراني للأنظمة التشغيلية


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority