الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

ضوابط الأمن السيبراني
للأحداث والمناسبات الوطنية

National Events Cybersecurity Controls
(NECC -1:2026)

إشارة المشاركة: شفاف
تصنيف الوثيقة: عام

تنويه: لمواكبة المتغيرات بشأن تحديثات الوثائق الصادرة عن الهيئة الوطنية للأمن السيبراني، تود الهيئة الوطنية للأمن السيبراني التنويه على أهمية الاعتماد الدائم على نسخ الوثائق المنشورة في الموقع الإلكتروني للهيئة https://nca.gov.sa

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 أكان ذلك من داخل الجهة أم خارجها؛ خارج النطاق المحدد للاستلام.

برتقالى + مشدد (مشاركة فى نفس الجهة)

المستلم يمكنه مشاركة المعلومات في الجهة نفسها مع الأشخاص المعنيين فحسب.

برتقالي (مشاركة محدودة)

المستلم يمكنه مشاركة المعلومات في الجهة نفسها مع الأشخاص المعنيين فحسب. ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

أخضر (مشاركة في نفس المجتمع)

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

شفاف (غير محدود)

قائمة المحتويات

قائمة الجداول

قائمة الأشكال والرسوم التوضيحية

الملخص التنفيذي

استهدفت رؤية المملكة العربية السعودية ٢٠٣٠ إلى تعزيز مكانة المملكة إقليميًا ودوليًا، وتنويع الاقتصاد الوطني، وتحسين جودة الحياة. ويُعد قطاع استضافة الأحداث والفعاليات والمؤتمرات أحد المكنات الرئيسة لتحقيق هذه الأهداف، نظرًا لدوره في تنشيط الاقتصاد، وتعزيز السياحة، وجذب الاستثمارات، ونقل المعرفة، إلى جانب إبراز الهوية الوطنية والثقافية للمملكة على المستويين المحلي والدولي.

وقد شهدت المملكة خلال الأعوام الماضية تطورًا متسارعًا في منظومة استضافة الأحداث والمناسبات؛ شمل البنية التحتية، والمرافق المتخصصة، والكوادر الوطنية، والقدرات التنظيمية والتقنية؛ بما يواكب أفضل الممارسات العالمية، في إدارة الأحداث الكبرى، والمعارض، والمؤتمرات، والمواسم الترفيهية، والفعاليات الثقافية والرياضية، وتنظيمها.

إن هذا التحول يتطلب انسيابية المعلومات، وأمانها، وتكامل أنظمتها، ويستوجب المحافظة على الأمن السيبراني للمملكة العربية السعودية، وتعزيزه؛ حمايةً للمصالح الحيوية للدولة، وأمنها الوطني والبنى التحتية الحساسة، والقطاعات ذات الأولوية، والخدمات، والأنشطة الحكومية. لهذا أُسست الهيئة الوطنية للأمن السيبراني، وجرت الموافقة على تنظيمها، بموجب الأمر الملكي الكريم ذي الرقم ٦٨٠١ والتاريخ ١٤٣٩/٢/١١هـ فأصبحت الجهة المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه.

ومن هذا المنطلق، قامت الهيئة الوطنية للأمن السيبراني، بوضع ضوابط الأمن السيبراني للأحداث والمناسبات الوطنية National Events Cybersecurity Controls (NECC -1:2026) بهدف تحقيق الحد الأدنى من متطلبات الأمن السيبراني للأحداث، والمناسبات الوطنية، واستنادًا إلى اختصاصها في وضع السياسات، وآليات الحوكمة، والأطر والمعايير، والضوابط، والإرشادات المتعلقة بالأمن السيبراني، وتعميمها على الجهات ذات العلاقة ومتابعة الالتزام بها، بما يضمن تحقيق مستهدفات رؤية المملكة، وتعظيم الأثر الإيجابي للفعاليات على الاقتصاد والمجتمع للمملكة.

وعلى مختلف الجهات الوطنية تنفيذ ما يحقق الالتزام الدائم والمستمر بهذه الضوابط؛ تحقيقًا لما ورد في الفقرة الثالثة من المادة العاشرة، في تنظيم الهيئة الوطنية للأمن السيبراني، وكذلك ما ورد في الأمر السامي الكريم ذي الرقم ٥٧٢٣١ والتاريخ ١٤٣٩/١١/١٠ هـ.

المقدمة

قامت الهيئة الوطنية للأمن السيبراني (ويشار لها في هذه الوثيقة بـ "الهيئة") بتطوير ضوابط الأمن السيبراني للأحداث والمناسبات الوطنية؛ بعد دراسة أفضل الممارسات والتجارب في مجال الأمن السيبراني، والاستفادة منها، وتحليل ما جرى رصده من حوادث وهجمات سيبرانية، على مستوى الجهات الحكومية وأحداثها ومناسباتها، وخبرات الهيئة في تعزيز أمن الأحداث، والمناسبات الوطنية.

تتكون ضوابط الأمن السيبراني للأحداث والمناسبات الوطنية من:

- ٤ مكونات أساسية (Main Domains) لضوابط الأمن السيبراني.
- ١٧ مكوناً فرعياً (Subdomains) لضوابط الأمن السيبراني.
- ٣٥ ضابطاً أساسياً (Controls) للأمن السيبراني.

الأهداف

تهدف هذه الضوابط إلى توفير الحد الأدنى، من متطلبات الأمن السيبراني، للأحداث والمناسبات الوطنية؛ وذلك لرفع الجاهزية السيبرانية، للأحداث والمناسبات الوطنية، ضمن نطاق عمل هذه الضوابط، وحماية الأنظمة المتعلقة بها (ويشار لها في هذه الوثيقة بـ "أنظمة الفعالية") ويعنى بها جميع المواقع أو الخدمات الإلكترونية الخاصة بالحدث، أو المناسبة الوطنية، والبنى التحتية؛ مثل المواقع الإلكترونية، والبريد الإلكتروني، وقواعد البيانات، وحسابات التواصل الاجتماعي، الخاصة بالحدث أو بالمناسبة وغيرها.

نطاق العمل وقابلية التطبيق

نطاق عمل الضوابط

تُطَبّق هذه الضوابط على الأحداث، والمناسبات التي تحظى برعاية ملكية كريمة، أو برعاية سمو ولي العهد، أو برعاية حكومية، أو مناسبات وفعاليات على مستوى وطني. ومسؤولية تطبيق هذه الضوابط والالتزام بها، تقع على الجهة الوطنية، المسؤولة عن الحدث، أو المناسبة. كما تُشجع الهيئة الجهات الأخرى في المملكة وبشدة على الاستفادة من هذه الضوابط؛ لتطبيق أفضل الممارسات فيما يتعلق بتعزيز الأمن السيبراني لفعالياتها.

قابلية التطبيق داخل الجهة

أعدت هذه الضوابط لتكون ملائمة لاحتياجات الأمن السيبراني في الأحداث والمناسبات الوطنية في المملكة العربية السعودية، بتنوع طبيعتها. ويجب على كل جهة وطنية، مسؤولة عن حدث، أو مناسبة، الالتزام بجميع الضوابط، القابلة للتطبيق عليها.

من الأمثلة على الضوابط، التي تتفاوت فيها قابلية التطبيق، من حدث أو مناسبة إلى أخرى، حسب طبيعتها، واستخدامها للتقنيات المذكورة، الضوابط ضمن المكون الفرعي رقم (٤-٢) المتعلقة بالأمن السيبراني للحوسبة السحابية والاستضافة (Cloud Computing and Hosting Cybersecurity) فإنها تكون قابلة التطبيق، وملزمة للأحداث والمناسبات الوطنية، التي تستخدم حاليًا خدمات الحوسبة السحابية، والاستضافة، أو تخطط لاستخدامها.

التنفيذ والالتزام

تحقيقًا لما ورد في الفقرة الثالثة، من المادة العاشرة، في تنظيم الهيئة الوطنية للأمن السيبراني، وكذلك ما ورد في الأمر السامي الكريم ذي الرقم ٥٧٢٣١ والتاريخ ١٤٣٩/١١/١٠ هـ، فإنه يجب على جميع الجهات، ضمن نطاق عمل هذه الضوابط؛ تنفيذ ما يحقق الالتزام الدائم، والمستمر بهذه الضوابط.

تقوم الهيئة بتقييم التزام الجهات، بما ورد في هذه الضوابط؛ من خلال بوابة حصين وكذلك القيام بالزيارات الميدانية للتدقيق؛ وفق الآلية التي تراها الهيئة مناسبة لذلك.

التحديث والمراجعة

تتولى الهيئة التحديث والمراجعة الدورية، لضوابط الأمن السيبراني، للأحداث والمناسبات الوطنية؛ حسب متطلبات الأمن السيبراني، والمستجدات ذات العلاقة. كما تتولى الهيئة إعلان الإصدار المحدث من الضوابط.

مكونات وهيكلية ضوابط الأمن السيبراني للأحداث والمناسبات الوطنية

المكونات الأساسية والفرعية لضوابط الأمن السيبراني للأحداث والمناسبات الوطنية

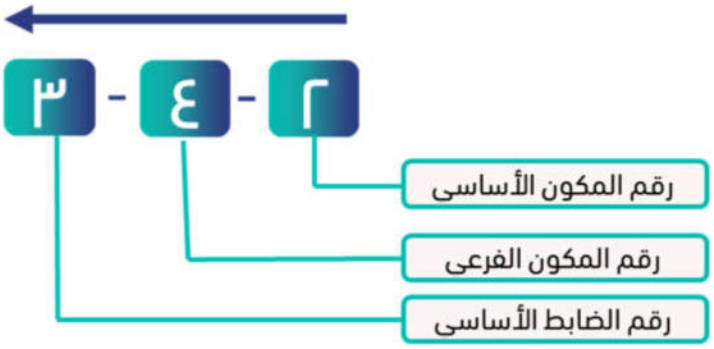
يبين الشكل (١) الآتي، المكونات الأساسية والفرعية لضوابط الأمن السيبراني للأحداث والمناسبات الوطنية.

١- حوكمة الأمن السيبراني Cybersecurity Governance	١ - ١	صلاحية اتخاذ القرارات Decision Making Authority	١-١	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management
٢ - تعزيز الأمن السيبراني Cybersecurity Defense	٢ – ١	إدارة الأصول Asset Management	٢ - ٢	إدارة هويات الدخول والصلاحيات Identity and Access Management
	٢ – ٣	حماية البريد الإلكتروني Email Protection	٢ - ٤	إدارة أمن الشبكات Networks Security Management
	٢ - ٥	حماية البيانات والمعلومات Data and Information Protection	٢-٦	إدارة الثغرات Vulnerabilities Management
	٢-٧	اختبار الاختراق Penetration Testing	٢-٨	إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management
	٢-٩	إدارة حوادث وتهديدات الأمن السيبراني Cybersecurity Incident and Threat Management	٢-١٠	الأمن المادي Physical Security
	٢-١١	إدارة حسابات التواصل الاجتماعي Social Media Accounts Management	٢-١٢	حماية التطبيقات Application Security
٣ - صمود الأمن السيبراني Cybersecurity Resilience	٣-١	صمود الأمن السيبراني في إدارة استمرارية الأعمال Cybersecurity Resilience In Business Continuity Management (BCM)		
٤ - الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية Third-Party and Cloud Computing Cybersecurity	٤ - ١	الأمن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity	٤-٢	الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة Cloud Computing and Hosting Cybersecurity

شكل ١: المكونات الأساسية والفرعية لضوابط الأمن السيبراني للأحداث والمناسبات الوطنية

الهيكلية

يوضح الشكل (٢) الآتي معنى رموز ضوابط الأمن السيبراني، للأحداث والمناسبات الوطنية.



شكل (٢): هيكلية ضوابط الأمن السيبراني للأحداث والمناسبات الوطنية

يوضح الجدول (١) طريقة هيكلية ضوابط الأمن السيبراني للأحداث والمناسبات الوطنية

١	اسم المكون الأساسي
رقم مرجعي للمكون الأساسي	
رقم مرجعي للمكون الفرعي	اسم المكون الفرعي
الهدف	
الضوابط	
رقم مرجعي للضابط	بنود الضابط

جدول (١): هيكلية ضوابط الأمن السيبراني للأحداث والمناسبات الوطنية

ضوابط الأمن السيبراني للأحداث والمناسبات الوطنية

١ حوكمة الأمن السيبراني (Cybersecurity Governance)

١-١	صلاحية اتخاذ القرارات (Decision Making Authority)
الهدف	ضمان الوصول المباشر لمتخذ القرار، وصاحب الصلاحية؛ للتعامل المناسب مع المهمات المتعلقة بالأمن السيبراني.
الضوابط	
١-١-١	يجب تحديد صاحب الصلاحية في الجهة؛ لاتخاذ القرارات المهمة، المتعلقة بالأمن السيبراني، الخاص بأنظمة الفعالية.
١-١-٢	يجب تحديد الأدوار والمسؤوليات، الخاصة بالأمن السيبراني في أنظمة الفعالية، وتوثيقها واعتمادها. وتكليف الأشخاص المعنيين بها. كما يجب تقديم الدعم اللازم، لإنفاذ ذلك؛ مع الأخذ في الحسبان، عدم تعارض المصالح.
١-١-٣	يجب تحديد ضابط اتصال، أساسي واحتياطي، وتسجيل بيانات كل منهما لدى الهيئة.
١-٢	إدارة مخاطر الأمن السيبراني (Cybersecurity Risk Management)
الهدف	ضمان إدارة مخاطر الأمن السيبراني، على نحو ممنهج؛ يهدف إلى حماية الأصول المعلوماتية، والتقنية للأحداث، والمناسبات؛ وذلك وفقاً للسياسات، والإجراءات التنظيمية للحدث أو المناسبة، والمتطلبات التشريعية، والتنظيمية ذات العلاقة.
الضوابط	
١-٢-١	يجب تنفيذ إجراءات إدارة مخاطر الأمن السيبراني بحد أدنى في الحالات الآتية: ١-٢-١-١ في مرحلة مبكرة، من التخطيط للحدث أو المناسبة. ١-٢-١-٢ قبل إجراء تغيير جوهري، في البنية التقنية. ١-٢-١-٣ عند التخطيط؛ للحصول على خدمات طرف خارجي. ١-٢-١-٤ عند التخطيط، وقبل إطلاق منتجات، وخدمات تقنية جديدة.

٢ تعزيز الأمن السيبراني (Cybersecurity Defense)

٢-١	إدارة الأصول (Asset Management)
الهدف	للتأكد من أن إدارة الأحداث والمناسبات، لديها قائمة جرد دقيقة، وحديثة للأصول، تشمل التفاصيل ذات العلاقة، لجميع الأصول المعلوماتية، والتقنية المتاحة لأنظمة الفعالية؛ من أجل دعم العمليات التشغيلية للحدث، أو المناسبة، ومتطلبات الأمن السيبراني؛ لتحقيق سرية الأصول المعلوماتية والتقنية لأنظمة الفعالية وسلامتها ودقتها وتوافرها.
الضوابط	
٢-١-١	يجب حصر الأصول، وتحديث جميع بيانات أنظمة الفعالية (الأنظمة والخدمات والمعرفات الرقمية، المرتبطة تقنيًا، والمتصلة بالإنترنت) للحدث أو المناسبة، ومشاركتها مع الهيئة الوطنية للأمن السيبراني باستمرار.
٢-١-٢	يجب تصنيف أنظمة الفعالية وترميزها (Labeling) والتعامل معها، وفقًا للمتطلبات التشريعية، والتنظيمية ذات العلاقة.
٢-١-٣	يجب إتمام التحقق من الجاهزية الأمنية، لأنظمة الفعالية، لتلك الأنظمة، والخدمات والمعرفات الرقمية، التي جرى حصرها، ومن ثم تزويد الهيئة الوطنية للأمن السيبراني، بالوثائق والمعلومات والبيانات، والتقارير ذوات العلاقة.
٢-١-٤	يجب تحديد سياسة الاستخدام المقبولة للأصول المعلوماتية والتقنية لأنظمة الفعالية، والعمل على توثيقها، واعتمادها، ونشرها.

٢-٢	إدارة هويات الدخول والصلاحيات (Identity and Access Management)
الهدف	ضمان حماية الأمن السيبراني للوصول المنطقي (Logical Access) إلى أنظمة الفعالية؛ من أجل منع الوصول غير المصرح به، وتقييد الوصول إلى ما هو مطلوب؛ لإنجاز الأعمال المتعلقة، بالحدث أو المناسبة.
الضوابط	
١-٢-٢	يجب التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) لأنظمة الفعالية، وتحديد عناصر التحقق المناسبة، وعددها، وكذلك تقنيات التحقق المناسبة، بناء على نتائج تقييم الأثر المحتمل، لفشل عملية التحقق وتخطيها، وهذا يشمل عمليات الدخول عن بعد، والحسابات ذات الصلاحيات المهمة والحساسة.
٢-٢-٢	يجب إدارة تصاريح المستخدمين (Authorization) وصلاحياتهم؛ بناءً على مبادئ التحكم بالدخول والصلاحيات مبدأ الحاجة إلى المعرفة والاستخدام"Need-to-know and Need-to-use" ، ومبدأ الحد الأدنى من الصلاحيات والامتيازات "Least Privilege"، ومبدأ فصل المهام ("Segregation of Duties").
٣-٢-٢	يجب مراجعة هويات الدخول، والصلاحيات بشكل دوري.
٣-٢	حماية البريد الإلكتروني (Email Protection)
الهدف	ضمان حماية البريد الإلكتروني للحدث، أو المناسبة، من مخاطر الأمن السيبراني.
١-٣-٢	يجب تحديد متطلبات الأمن السيبراني، لحماية البريد الإلكتروني للحدث أو المناسبة، وتوثيقها، واعتمادها. ويجب أن تغطي هذه المتطلبات، بحدّ أدنى ما يلي: ٢-٣-١-١ تحليل رسائل البريد الإلكتروني، وتصفيتها (Filtering) وبخاصة رسائل التصيّد الإلكتروني (Phishing Emails) والرسائل الاقتحامية (Spam Emails) باستخدام تقنيات، الحماية الحديثة وآلياتها للبريد الإلكتروني. ٢-٣-١-٢ توثيق مجال البريد الإلكتروني للحدث أو المناسبة، 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").
٤-٢	إدارة أمن الشبكات (Networks Security Management)
الهدف	ضمان حماية شبكات الحدث، أو المناسبة، من مخاطر الأمن السيبراني.
١-٤-٢	يجب تطبيق متطلبات الأمن السيبراني، لإدارة أمن شبكات الحدث أو المناسبة. ويجب أن تغطي بحدّ أدنى ما يلي: ٢-٤-١-١ أمن الشبكات اللاسلكية، وحمايتها، باستخدام وسائل آمنة؛ للتحقق من الهوية والتشفير. ٢-٤-١-٢ العزل، والتقسيم المادي، أو المنطقي، لأجزاء الشبكات بشكل آمن. ٢-٤-١-٣ تطبيق نظام أمن أسماء النطاقات (DNS). ٢-٤-١-٤ حماية أنظمة الفعالية من هجمات تعطيل الشبكات (Distributed Denial of Service Attack "DDoS") للحد من مخاطر الأمن السيبراني، الناتجة عن هجمات تعطيل الشبكات.
٥-٢	حماية البيانات والمعلومات (Data and Information Protection)
الهدف	ضمان حماية سرية بيانات الحدث أو المناسبة وسلامتها وكذلك دقة المعلومات وتوافرها، وذلك وفقًا للسياسات، والإجراءات التنظيمية للحدث أو المناسبة، والمتطلبات التشريعية، والتنظيمية ذات العلاقة.
١-٥-٢	يجب تحديد متطلبات الأمن السيبراني لحماية بيانات الحدث ومعلوماته؛ أو المناسبة، والتعامل معها وفقًا للمتطلبات التشريعية، والتنظيمية ذات العلاقة، وتوثيقها، واعتمادها. ويجب أن تغطي بحدّ أدنى ما يلي: ٢-٥-١-١ إجراء النسخ الاحتياطي، لأنظمة الفعالية، بشكل دوري. وإجراء فحص دوري؛ للتأكد من فعالية استعادة النسخ الاحتياطية. ٢-٥-١-٢ استخدام خدمة حماية العلامة التجارية؛ لحماية بيانات الحدث، أو المناسبة، من الانتحال (Brand Protection). ٢-٥-١-٣ استخدام الطابعات، والماسحات الضوئية، وآلات التصوير بشكل آمن.
٦-٢	إدارة الثغرات (Vulnerabilities Management)
الهدف	ضمان اكتشاف الثغرات التقنية في الوقت المناسب، ومعالجتها بشكل فعال؛ وذلك لمنع احتمالية استغلال هذه الثغرات من الهجمات السيبرانية أو تقليلها، وتقليل الأثار المترتبة، على أنظمة الفعالية، أو المناسبة.
الضوابط	
١-٦-٢	يجب فحص الثغرات الأمنية لأنظمة الفعالية واكتشافها، بشكل دوري، وبوتيرة متزايدة، مع قرب الحدث أو المناسبة.

٢-٦-٢	يجب معالجة الثغرات الأمنية، المكتشفة على أنظمة الفعالية، فور اكتشافها.
٣-٦-٢	يجب معالجة جميع الثغرات والمخاطر، الواردة في نتائج تقارير تقييمات الأمن السيبراني، بشكل فوري، وإبلاغ الهيئة الوطنية للأمن السيبراني بالنتائج.
٤-٦-٢	يجب تحديث الأنظمة، والبرمجيات والأجهزة، وإصلاحها بانتظام (Patch Management).
٥-٦-٢	يجب على صاحب الصلاحية، التجاوب السريع مع التنبيهات الأمنية، الصادرة من الهيئة الوطنية للأمن السيبراني، ومعالجتها بشكل فعّال؛ للتصدي للهجمات والتهديدات السيبرانية، التي تستهدف الأنظمة، والخدمات، والمعرفات الرقمية، المرتبطة بالحدث، أو المناسبة، والحد من آثارها.
٧-٢	اختبار الاختراق (Penetration Testing)
الهدف	تقييم مدى فعالية قدرات تعزيز الأمن السيبراني لأنظمة الفعالية أو المناسبة واختيارها؛ وذلك من خلال عمل محاكاة لتقنيات الهجوم السيبراني الفعلية وأساليبها. ولاكتشاف نقاط الضعف الأمنية، غير المعروفة، التي قد تؤدي إلى الاختراق السيبراني. وذلك وفقًا للمتطلبات التشريعية، والتنظيمية ذات العلاقة.
الضوابط	
١-٧-٢	يجب تحديد متطلبات الأمن السيبراني، لعمليات اختبار الاختراق وتوثيقها، واعتمادها. ويجب أن تغطي في الحد الأدنى نطاق عمل اختبار الاختراق؛ ليشمل جميع الخدمات المقدمة خارجياً (عن طريق الإنترنت) ومكوناتها التقنية، ومنها: البنية التحتية، والمواقع الإلكترونية، وتطبيقات الويب، وتطبيقات الهواتف المحمولة، والبريد الإلكتروني، والدخول عن بعد.
٢-٧-٢	يجب تنفيذ عمليات اختبار الاختراق، على أنظمة الفعالية، والخدمات المعتمدة للنشر، ويكون ذلك قبلها بستين (٦٠) يومًا في الحد الأدنى.
٣-٧-٢	يجب تطبيق جميع التوصيات، ونتائج اختبار الاختراق، والتحقق من معالجتها، قبل الحدث، أو المناسبة فورًا؛ وإبلاغ الهيئة الوطنية للأمن السيبراني بالنتائج.
٨-٢	إدارة سجلات الأحداث ومراقبة الأمن السيبراني (Cybersecurity Event Logs and Monitoring Management)
الهدف	ضمان تجميع سجلات أحداث الأمن السيبراني وتحليلها ومراقبتها في الوقت المناسب؛ من أجل الاكتشاف الاستباقي للهجمات السيبرانية، وإدارة مخاطرها بفعالية، وتحليلها ومراقبتها لتقليل الآثار المترتبة على الحدث أو المناسبة.
الضوابط	
١-٨-٢	يجب مراقبة أنظمة الفعالية باستمرار قبل الحدث وأثنائه أو المناسبة، وحتى إيقاف الأنظمة، عن طريق مقدم خدمات مركز عمليات الأمن السيبراني المدار، مرخص للمستوى الأول، من قبل الهيئة الوطنية للأمن السيبراني.
٢-٨-٢	يجب الاحتفاظ بسجلات الأحداث، الخاصة بالأمن السيبراني، على ألا تقل المدة عن ٦ أشهر، قبل الحدث، أو المناسبة، وبعدها.
٩-٢	إدارة حوادث وتهديدات الأمن السيبراني (Cybersecurity Incident and Threat Management)
الهدف	ضمان تحديد حوادث الأمن السيبراني واكتشافها في الوقت المناسب، وإدارتها بشكل فعّال، والتعامل مع تهديدات الأمن السيبراني استباقيًا، من أجل منع أو تقليل الآثار المترتبة على أعمال الحدث أو المناسبة. مع مراعاة ماورد في الأمر السامي الكريم ذي الرقم ٣٧١٤٠ والتاريخ ١٤ / ٨ / ١٤٣٨ هـ.
الضوابط	
١-٩-٢	يجب وضع خطط الاستجابة لحوادث الأمن السيبراني وآليات التصعيد واختبارها.
٢-٩-٢	يجب تبليغ الهيئة بشكل فوري بأي خطر أو تهديد أو اختراق للأمن السيبراني للحدث، أو المناسبة، واقع أو محتمل.
١٠-٢	الأمن المادي (Physical Security)
الهدف	ضمان حماية الأصول المعلوماتية والتقنية للحدث، أو المناسبة؛ من الوصول المادي غير المصرح به، ومن الفقدان، والسرقة، والتخريب.
الضوابط	
١-١٠-٢	يجب تطبيق متطلبات الأمن السيبراني؛ لحماية أنظمة الفعالية، من الوصول المادي غير المصرح به، ومن الفقدان والسرقة، والتخريب. ويجب أن تغطي بحدّ أدنى ما يلي: ٢-١٠-١-١ اعتماد إجراءات الدخول المصرح به، للأماكن الحساسة في للحدث، أو المناسبة. ٢-١٠-١-٢ تفعيل سجلات الدخول والمراقبة (CCTV) على أن تحفظ سجلات الدخول والمراقبة لمدة ٦ أشهر بحد أدنى.

	٢-١٠-١-٣ حماية معلومات سجلات الدخول والمراقبة. ٢-١٠-١-٤ أمن إتلاف وإعادة استخدام الأصول المادية التي تحوي معلومات مصنفة (وتشمل: الوثائق الورقية ووسائط الحفظ والتخزين). ٢-١٠-١-٥ أمن الأجهزة والمعدات داخل مباني الحدث أو المناسبة وخارجها.
٢-١١	إدارة حسابات التواصل الاجتماعي (Social Media Accounts Management)
الهدف	ضمان حماية حسابات التواصل الاجتماعي، الخاصة بالحدث، أو المناسبة، من مخاطر الأمن السيبراني.
الضوابط	
٢-١١-١	يجب تطبيق ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات (OSMACC- 1:2021).
٢-١٢	حماية التطبيقات (Application Security)
الهدف	ضمان حماية التطبيقات للحدث، أو المناسبة؛ من مخاطر الأمن السيبراني.
الضوابط	
٢-١٢-١	يجب تطبيق متطلبات الأمن السيبراني؛ لحماية تطبيقات الحدث، أو المناسبة، ويجب أن تغطي بحدّ أدنى ما يلي: ٢-١٢-١-١ استخدام معايير التطوير الآمن، للتطبيقات (Secure Coding Standards). ٢-١٢-١-٢ استخدام مصادر مرخصة، وموثوقة، لأدوات تطوير التطبيقات، والمكتبات الخاصة بها (Libraries). ٢-١٢-١-٣ إجراء اختبار؛ للتحقق من مدى استيفاء التطبيقات، للمتطلبات الأمنية السيبرانية، للحدث، أو المناسبة. ٢-١٢-١-٤ إجراء مراجعة للإعدادات والتحصين (Secure Configuration and Hardening) وحزم التحديثات، قبل إطلاق، وتدشين التطبيقات. ٢-١٢-١-٥ استخدام جدار الحماية، لتطبيقات الويب (Web Application Firewall). ٢-١٢-١-٦ استخدام بروتوكولات آمنة (مثل بروتوكول HTTPS). ٢-١٢-١-٧ ضمان التكامل الآمن، بين التطبيقات (Secure Integration). ٢-١٢-١-٨ التحقق من الهوية؛ على أن يجري تحديد عناصر التحقق المناسبة، وعددها، وكذلك تقنيات التحقق المناسبة؛ بناء على نتائج تقييم الأثر المحتمل، لفشل عملية التحقق، وتخطيها؛ أثناء عمليات دخول المستخدمين.

٣ صمود الأمن السيبراني (Cybersecurity Resilience)

٣-١	صمود الأمن السيبراني في إدارة استمرارية الأعمال (Cybersecurity Resilience In Business Continuity Management "BCM")
الهدف	ضمان توافر متطلبات صمود الأمن السيبراني، في إدارة استمرارية أعمال الحدث أو المناسبة. وضمان معالجة الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحرجة للحدث أو المناسبة والعمل على تقليلها، وكذلك أنظمة معالجة معلوماتها وأجهزتها وذلك جراء الكوارث الناتجة عن مخاطر الأمن السيبراني.
الضوابط	
٣-١-١	يجب تطبيق تمارين محاكاة ضمن إدارة استمرارية أعمال الحدث، أو المناسبة؛ لضمان صمود الأمن السيبراني للحدث أو المناسبة.

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

٤-١	الأمن السيبراني المتعلق بالأطراف الخارجية
الهدف	ضمان حماية أصول الحدث، أو المناسبة؛ من مخاطر الأمن السيبراني، المتعلقة بالأطراف الخارجية؛ (بما في ذلك خدمات الإسناد لتقنية المعلومات ("Outsourcing") والخدمات المدارة ("Managed Services"). وفقًا للسياسات والإجراءات التنظيمية للحدث، أو المناسبة، والمتطلبات التشريعية والتنظيمية، ذات العلاقة.
الضوابط	
٤-١-١	يجب إلزام جميع الأطراف الخارجية، التي أسندت إليها أعمال خاصة بالحدث أو المناسبة؛ بالالتزام بما ورد في هذه الضوابط.
٤-١-٢	يجب أن تغطي متطلبات الأمن السيبراني مع الأطراف الخارجية، التي تقدم خدمات الإسناد للأمن السيبراني أو لتقنية المعلومات، أو الخدمات المدارة، بحد أدنى؛ إجراء تقييم لمخاطر الأمن السيبراني، والتأكد من وجود ما يضمن السيطرة على تلك المخاطر؛ قبل توقيع العقود والاتفاقيات، أو عند تغيير المتطلبات التشريعية، والتنظيمية، ذات العلاقة.
٤-١-٣	يجب توقيع الطرف الخارجي وضمان التزامه ببنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) والحذف الآمن لبيانات الحدث أو المناسبة عند انتهاء الخدمة.
٤-٢	الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة
الهدف	ضمان معالجة مخاطر الأمن السيبراني، وتنفيذ متطلبات الأمن السيبراني للحوسبة السحابية، والاستضافة بشكل ملائم وفعّال. وضمان حماية الأصول المعلوماتية، والتقنية الموجودة، على خدمات الحوسبة السحابية، التي تجري استضافتها، أو معالجتها، أو إدارتها بواسطة أطراف خارجية.
الضوابط	
٤-٢-١	يجب أن يكون موقع استضافة أنظمة الفعالية وتخزينها، في داخل المملكة، وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.
٤-٢-٢	يجب تطبيق ضوابط الأمن السيبراني للحوسبة السحابية، وإلزام مقدم خدمات الحوسبة السحابية بها عند التعاقد.

ملاحق

ملحق (أ): قائمة الاختصارات

يوضح الجدول (٢) أدناه معنى الاختصارات التي ورد ذكرها في هذه الضوابط.

الاختصار	معناه
NECC	National Events Cybersecurity Controls ضوابط الأمن السيبراني للأحداث والمناسبات الوطنية.
HTTPS	Hyper Text Transfer Protocol Secure بروتوكول نقل النص التشعبي الآمن.
MFA	Multi-Factor Authentication التحقق من الهوية متعدد العناصر.
OSMACC	Organization's Social Media Accounts Cybersecurity Controls ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات.
CCTV	Closed-Circuit Television يستخدم التليفزيون ذو الدائرة المغلقة، والمعروف أيضًا باسم المراقبة بالفيديو، كاميرات الفيديو؛ لإرسال إشارة إلى مكان محدد، على مجموعة محدودة من الشاشات. وغالبًا ما يطلق هذا المصطلح، على تلك التقنية، المستخدمة للمراقبة في المناطق التي قد تحتاج إلى مراقبة؛ حينما يشكل الأمن المادي مطلبًا مهمًا فيها.
DNS	Domain Name System نظام أسماء النطاقات.

الجدول (٢): قائمة الاختصارات

الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority