هذا المربع مخصّص لأغراض توجيهية. احذف جميع المربعات التوجيهية بعد تعبئة النموذج. يجب تحرير البنود الملوّنة باللون الأزرق بصورة مناسبة. ويجب إزالة التظليل الملون بعد إجراء التعديلات.

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج السياسة العامة للأمن السيبراني

اختر التصنيف

التاريخ: اضغط هنا لإضافة تاريخ

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

استبدل <اسم الجهة> باسم الجهة في مجمل صفحات الوثيقة. وللقيام بذلك، اتبع الخطوات التالية:

- اضغط على مفتاحي "Ctrl" و"H" في الوقت نفسه.
- أضف "<اسم الجهة>" في مربع البحث عن النص.
- أدخل الاسم الكامل لجهتك في مربع "استبدال" النص.
- اضغط على "المزيد" وتأكّد من اختيار "Match case".
- اضغط على "استبدل الكل".
- أغلق مربع الحوار.

إخلاء المسؤولية

طُور هذا النموذج عن طريق الهيئة الوطنية للأمن السيبراني كمثال توضيحي يمكن استخدامه كدليل ومرجع للجهات. يجب أن يتم تعديل هذا النموذج ومواءمته مع أعمال <اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة. كما يجب أن يُعتمد هذا النموذج من قبل رئيس الجهة أو من يقوم/تقوم بتفويضه. وتخلي الهيئة مسؤوليتها من استخدام هذا النموذج كما هو، وتؤكد على أن هذا النموذج ما هو إلا مثال توضيحي.

اعتماد الوثيقة

الدور	المسمى الوظيفي	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل المسمى الوظيفي>	<أدخل الاسم الكامل للموظف>	اضغط هنا لإضافة تاريخ	<أدخل التوقيع>

نسخ الوثيقة

النسخة	التاريخ	عُدِّلَ بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة تاريخ	<أدخل الاسم الكامل للموظف>	<أدخل وصف التعديل>

جدول المراجعة

معدل المراجعة	التاريخ لأخر مراجعة	تاريخ المراجعة القادمة
مره واحدة كل سنة	اضغط هنا لإضافة تاريخ	اضغط هنا لإضافة تاريخ

اختر التصنيف

الإصدار <١,٠>

قائمة المحتويات

الغرض

الغرض من هذه السياسة هو تحديد المتطلبات العامة المتعلقة بالأمن السيبراني في <اسم الجهة>، وذلك للوصول للهدف الأساسي من السياسة وهو أن تكون هي الأساس لجميع سياسات، ومعايير وإجراءات الأمن السيبراني في <اسم الجهة> ولتكون أحد المدخلات لعمليات الجهة الداخلية مثل عمليات الموارد البشرية، إدارة الموردين، إدارة المشاريع، وإدارة التغيير.

تمت موائمة هذه السياسة مع الضوابط والمعايير الصادرة من الهيئة الوطنية للأمن السيبراني والمتطلبات التنظيمية والتشريعية ذات العلاقة.

نطاق العمل

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية ل<اسم الجهة> وتنطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

بنود السياسة

١- يجب على <الإدارة المعنية بالأمن السيبراني> تحديد وتطوير سياسات الأمن السيبراني، المعايير التقنية، الأطر التنظيمية، الإجراءات والمنهجيات، بناءً على نتائج تقييم المخاطر، وبشكل يضمن نشر متطلبات الأمن السيبراني، والتزام <اسم الجهة> بها، وذلك وفقًا لمتطلبات الأعمال التنظيمية ل<اسم الجهة>، والمتطلبات التشريعية والتنظيمية ذات العلاقة. كما يجب اعتماد السياسة من قبل <رئيس الجهة> ونشرها للعاملين المعنيين في <اسم الجهة> والأطراف ذات العلاقة عليها، والمتمثلة في:

١-١ **استراتيجية الأمن السيبراني (Cybersecurity Strategy)** لضمان خطط العمل للأمن السيبراني والأهـداف والمبادرات والبرامج والمشاريع وفعاليتها داخل <اسم الجهة> لتحقيق الأهداف الاستراتيجية والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٢ **سياسات وإجراءات الأمن السيبراني (Cybersecurity Policies and Procedures)** لضمان توثيق ونشر متطلبات الأمن السيبراني والتزام <اسم الجهة> بها، وذلك وفقًا لمتطلبات الأعمال التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٣ **أدوار ومسؤوليات الأمن السيبراني (Cybersecurity Roles and Responsibilities)** لضمان تحديد أدوار ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني في <اسم الجهة>.

١-٤ **منهجية إدارة مخاطر الأمن السيبراني (Cybersecurity Risk Management)** لضمان إدارة المخاطر السيبرانية على نحو ممنهج يهدف إلى حماية الأصول المعلوماتية والتقنية ل<اسم الجهة>، وذلك وفقًا للسياسات والإجراءات التنظيمية ل<اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٥ **برنامج التوعية والتدريب بالأمن السيبراني (Cybersecurity Awareness and Training Program)** للتأكد من أن العاملين ب<اسم الجهة> لديهم الوعي الأمني اللازم، وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني، مع التأكد من تزويد العاملين ب<اسم الجهة>

بالمهارات والمؤهلات والدورات التدريبية المتخصصة في مجال العاملين والمطلوبة في مجال الأمن السيبراني؛ لحماية الأصول المعلوماتية والتقنية ل<اسم الجهة> والقيام بمسؤولياتهم تجاه الأمن السيبراني.

١-٦ **سياسة الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية (Cybersecurity in Information Technology Projects)** للتأكد من أن متطلبات الأمن السيبراني مضمنة في منهجية إدارة مشاريع <اسم الجهة> وإجراءاتها لحماية السرية، وسلامة الأصول المعلوماتية والتقنية ل<اسم الجهة> وضمان دقتها وتوافرها، وكذلك التأكد من تطبيق معايير الأمن السيبراني في أنشطة تطوير التطبيقات والبرامج، وفقًا للسياسات والإجراءات التنظيمية ل<اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٧ **سياسة الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني (Cybersecurity Regulatory Compliance)** للتأكد من أن برنامج الأمن السيبراني لدى <اسم الجهة> متوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٨ **سياسة المراجعة والتدقيق الدوري للأمن السيبراني (Cybersecurity Periodical Assessment and Audit)** للتأكد من أن ضوابط الأمن السيبراني لدى <اسم الجهة> مطبقة، وتعمل وفقًا للسياسات والإجراءات التنظيمية ل<اسم الجهة>، والمتطلبات التشريعية التنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المُقرة تنظيميًا على <اسم الجهة>.

١-٩ **سياسة الأمن السيبراني المتعلق بالموارد البشرية (Cybersecurity in Human Resources)** للتأكد من أن مخاطر الأمن السيبراني ومتطلباته المتعلقة بالعاملين في <اسم الجهة> تعالج بفعالية قبل بدء عملهم، وأثنائه وعند انتهائه، وذلك وفقًا للسياسات والإجراءات التنظيمية ل<اسم الجهة>، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-١٠ **سياسة إدارة الأصول وسياسة الاستخدام المقبول للأصول (Asset Management and Asset Acceptable Use Policies)** للتأكد من أن <اسم الجهة> لديها قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العلاقة لجميع الأصول المعلوماتية والتقنية المتاحة ل<اسم الجهة>، من أجل دعم العمليات التشغيلية ل<اسم الجهة> ومتطلبات الأمن السيبراني، لتحقيق سرية الأصول المعلوماتية والتقنية وسلامتها ل<اسم الجهة>ودقتها وتوافرها.

١-١١ **سياسة إدارة هويات الدخول والصلاحيات ومعياره (Identity and Access Management)** لضمان حماية الأمن السيبراني للوصول المنطقي (Logical Access) إلى الأصول المعلوماتية والتقنية ل<اسم الجهة> من أجل منع الوصول غير المصرح به، وتقييد الوصول إلى ما هو مطلوب لإنجاز الأعمال المتعلقة ب<اسم الجهة>.

١-١٢ **سياسة حماية الأنظمة وأجهزة معالجة المعلومات (Information System and Processing Facilities Protection)** لضمان حماية الأنظمة، وأجهزة معالجة المعلومات؛ بما في ذلك أجهزة المستخدمين، والبنى التحتية ل<اسم الجهة> من المخاطر السيبرانية.

١-١٣ **سياسة حماية البريد الإلكتروني ومعياره (Email Protection)** لضمان حماية البريد الإلكتروني ل<اسم الجهة> من المخاطر السيبرانية.

١-١٤ **سياسة إدارة أمن الشبكات ومعياره (Networks Security Management)** لضمان حماية شبكات <اسم الجهة> من المخاطر السيبرانية.

اختر التصنيف

الإصدار <١,٠>

١-١٥ **سياسة أمن الخوادم (Servers Security)** لضمان حماية خوادم <اسم الجهة> من المخاطر السيبرانية.

١-١٦ **سياسة إدارة حزم التحديثات والإصلاحات (Patch Management)** لضمان ادارة حزم التحديثات والإصلاحات للأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة وأجهزة معالجة المعلومات الخاصة ب<اسم الجهة> وتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية.

١-١٧ **سياسة أمن الأجهزة المحمولة ومعياره (Mobile Devices Security)** لضمان حماية أجهزة <اسم الجهة> المحمولة (بما في ذلك أجهزة الحاسب المحمول، والهواتف الذكية، والأجهزة الذكية اللوحية) من المخاطر السيبرانية. ولضمان التعامل بشكل آمن مع المعلومات المصنفة، والمعلومات الخاصة بأعمال <اسم الجهة> وحمايتها، أثناء النقل، التخزين، إزالة، وعند استخدام الأجهزة الشخصية للعاملين في <اسم الجهة> (مبدأ "BYOD").

١-١٨ **سياسة حماية البيانات والمعلومات ومعياره (Data and Information Protection)** لضمان حماية سرية وسلامة بيانات ومعلومات <اسم الجهة> ودقتها وتوافرها، وذلك وفقًا للسياسات والإجراءات التنظيمية ل<اسم الجهة>، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-١٩ **سياسة التشفير ومعياره (Cryptography)** لضمان الاستخدام السليم والفعال للتشفير؛ لحماية الأصول المعلوماتية الإلكترونية ل<اسم الجهة>، وذلك وفقًا للسياسات، والإجراءات التنظيمية ل<اسم الجهة>، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٢٠ **سياسة أمن قواعد البيانات (Database Security)** لضمان حماية قواعد البيانات ل<اسم الجهة> من المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية.

١-٢١ **سياسة إدارة النسخ الاحتياطية ومعياره (Backup and Recovery Management)** لضمان حماية بيانات <اسم الجهة> ومعلوماتها، وكذلك حماية الإعدادات التقنية للأنظمة والتطبيقات الخاصة ب<اسم الجهة> من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقًا للسياسات والإجراءات التنظيمية ل<اسم الجهة>، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٢٢ **سياسة إدارة الثغرات ومعياره (Vulnerabilities Management)** لضمان اكتشاف الثغرات التقنية في الوقت المناسب، ومعالجتها بشكل فعال، وذلك لمنع احتمالية استغلال هذه الثغرات في الهجمات السيبرانية في <اسم الجهة> وتقليل ذلك، وكذلك تقليل الآثار المترتبة على أعمال <اسم الجهة>.

١-٢٣ **سياسة اختبار الاختراق ومعياره (Penetration Testing)** لتقييم مدى فعالية أنظمة وفريق المراقبة في رصد التهديدات المحتملة واختباره في <اسم الجهة>، وذلك من خلال محاكاة تقنيات الهجوم السيبراني الفعلية وأساليبه، ولاكتشاف نقاط الضعف الأمنية غير المعروفة ومدى فاعلية أنظمة وفريق المراقبة في رصد التهديدات المحتملة، والتي قد تؤدي إلى الاختراق السيبراني ل<اسم الجهة>؛ وذلك وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٢٤ **سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني ومعياره (Cybersecurity Event Logs and Monitoring Management)** لضمان جمع سجلات أحداث الأمن السيبراني بشكل آلي، وتحليلها، وتخزينها ومراقبتها في الوقت المناسب؛ من أجل الاكتشاف الاستباقي للهجمات السيبرانية، وإدارة مخاطرها بفعالية؛ لمنع الآثار السلبية المحتملة على أعمال <اسم الجهة> أو تقليلها.

اختر التصنيف

١-٢٥ **سياسة إدارة حوادث وتهديدات الأمن السيبراني (Cybersecurity Incident and Threat Management)** لضمان اكتشاف حوادث الأمن السيبراني وتحديدها في الوقت المناسب، وإدارتها بشكل فعّال، والتعامل مع تهديدات الأمن السيبراني استباقيًا، من أجل منع الآثار السلبية المحتملة أو تقليلها على أعمال <اسم الجهة>.

١-٢٦ **سياسة الحماية من البرمجيات الضارة (Anti-Malware security)** لضمان حماية أجهزة المستخدمين والأجهزة المحمولة والخوادم الخاصة ب<اسم الجهة> من تهديدات البرمجيات الضارة.

١-٢٧ **سياسة الأمن المادي ومعياره (Physical Security)** لضمان حماية الأصول المعلوماتية والتقنية ل<اسم الجهة> من الوصول المادي غير المصرح به، والفقدان والسرقة والتخريب.

١-٢٨ **سياسة حماية تطبيقات الويب ومعياره (Web Application Security)** لضمان حماية تطبيقات الويب الداخلية والخارجية ل<اسم الجهة> من المخاطر السيبرانية.

١-٢٩ **سياسة صمود الأمن السيبراني في إدارة استمرارية الأعمال (Cybersecurity Resilience Aspects of Business Continuity Management)** لضمان توافر متطلبات صمود لأمن السيبراني في إدارة استمرارية أعمال <اسم الجهة>، ولضمان معالجة الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحرجة وتقليلها ل<اسم الجهة> وأنظمة معالجة معلوماتها وأجهزتها جراء الكوارث الناتجة عن المخاطر السيبرانية.

١-٣٠ **سياسة الأمن السيبراني المتعلقة بالأطراف الخارجية (Third-Party Cybersecurity)** لضمان حماية أصول <اسم الجهة> من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية (بما في ذلك خدمات الإسناد لتقنية المعلومات "Outsourcing" والخدمات المدارة " Managed Services") وفقًا للسياسات والإجراءات التنظيمية ل<اسم الجهة>، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٣١ **سياسة الأمن السيبراني المتعلقة بالحوسبة السحابية والاستضافة (Cloud Computing and Hosting Cybersecurity)** لضمان معالجة المخاطر السيبرانية، وتنفيذ متطلبات الأمن السيبراني للحوسبة السحابية، والاستضافة بشكل ملائم وفعّال، وذلك وفقًا للسياسات والإجراءات التنظيمية ل<اسم الجهة>، والمتطلبات التشريعية والتنظيمية، والأوامر والقرارات ذات العلاقة. وضمان حماية الأصول المعلوماتية والتقنية ل<اسم الجهة> على خدمات الحوسبة السحابية، التي تتم استضافتها أو معالجتها، أو إدارتها بواسطة أطراف خارجية.

١-٣٢ **سياسة الأمن السيبراني للأنظمة التشغيلية (Cybersecurity Industrial Controls Systems)** لضمان إدارة الأمن السيبراني بشكل سليم وفعال، لحماية توافر الأنظمة التشغيلية وأنظمة التحكم الصناعي (OT\ICS) في <اسم الجهة> وسلامتها وسريتها؛ وحمايتها ضد الهجوم السيبراني (مثل الوصول غير المصرح به، والتخريب والتجسس والتلاعب) بما يتسق مع استراتيجية الأمن السيبراني ل<اسم الجهة>، وإدارة مخاطر الأمن السيبراني، والمتطلبات التشريعية والتنظيمية ذات العلاقة، وكذلك المتطلبات الدولية المقرّة تنظيميًا على <اسم الجهة> المتعلقة بالأمن السيبراني.

٢- يحق ل<الإدارة المعنية بالأمن السيبراني> الاطلاع على المعلومات، وجمع الأدلة اللازمة؛ للتأكد من الالتزام بالمتطلبات التشريعية والتنظيمية ذات العلاقة.

٣- يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات حماية الأصول المعلوماتية والتقنية.

اختر التصنيف

الإصدار <١,٠>

الأدوار والمسؤوليات

١- لضمان التزام ودعم صاحب الصلاحية لـ<اسم الجهة> فيما يتعلق بإدارة وتطبيق برامج الأمن السيبراني في <اسم الجهة> والمتطلبات ذات العلاقة، تُمثل القائمة الآتية مجموعة الأدوار والمسؤوليات اللازمة لإقرار سياسات الأمن السيبراني وإجراءاته، ومعاييره وبرامجه، وتنفيذها واتباعها:

١-١ مسؤوليات صاحب الصلاحية <رئيس الجهة أو من ينيبه>، على سبيل المثال:

١-١-١ إنشاء لجنة إشرافية للأمن السيبراني ويكون <رئيس الإدارة المعنية بالأمن السيبراني> أحد أعضائها.

١-٢ مسؤوليات <اللجنة الإشرافية للأمن السيبراني>، على سبيل المثال:

١-٢-١ اعتماد سياسات ومتطلبات الأمن السيبراني في <اسم الجهة>.

١-٣ مسؤوليات <الإدارة المعنية بالشؤون القانونية>، على سبيل المثال:

١-٣-١ التأكد من أن شروط ومتطلبات الامن السيبراني والمحافظة على سرية المعلومات (Non-Disclosure Clauses) مُلزمة قانونيًا في عقود العاملين في <اسم الجهة>، والأطراف الخارجية.

١-٤ مسؤوليات <الإدارة المعنية بالتدقيق والمراجعة الداخلية>، على سبيل المثال:

١-٤-١ مراجعة ضوابط الأمن السيبراني وتدقيق تطبيقها وفقًا للمعايير العامة المقبولة للمراجعة والتدقيق، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٥ مسؤوليات <الإدارة المعنية بتقنية المعلومات>، على سبيل المثال:

١-٥-١ تطبيق متطلبات الأمن السيبراني المتعلقة بالأصول التقنية في <اسم الجهة>.

١-٦ مسؤوليات <الإدارة المعنية بالموارد البشرية>، على سبيل المثال:

١-٦-١ تطبيق متطلبات الأمن السيبراني المتعلقة بالعاملين في <اسم الجهة>.

١-٧ مسؤوليات <الإدارة المعنية بالأمن السيبراني>، على سبيل المثال:

١-٧-١ تطوير سياسات الأمن السيبراني، واعتمادها من <رئيس الجهة أو من ينيبه>، والتأكد من إطلاع الأطراف المعنية عليها وتطبيقها، ومراجعتها وتحديثها بشكل دوري.

١-٨ مسؤوليات رؤساء الإدارات الأخرى، على سبيل المثال:

١-٨-١ دعم سياسات الأمن السيبراني وإجراءاته ومعاييره وبرامجه، وتوفير جميع الموارد المطلوبة، لتحقيق الأهداف المنشودة، بما يخدم المصلحة العامة لـ<اسم الجهة>.

١-٩ مسؤوليات العاملين، على سبيل المثال:

١-٩-١ المعرفة بمتطلبات الأمن السيبراني المتعلقة بالعاملين في <اسم الجهة>، والالتزام بها.

التحديث والمراجعة

يجب على <الإدارة المعنية بالأمن السيبراني> مراجعة السياسة سنويًا على الأقل أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في <اسم الجهة> أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بالسياسة

١- يجب على صاحب الصلاحية <رئيس الجهة أو من ينيبه> ضمان الالتزام بسياسة الأمن السيبراني والمتطلبات ذات العلاقة.

٢- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بسياسات الأمن السيبراني والمتطلبات ذات العلاقة بشكل دوري.

٣- يجب على جميع العاملين في <اسم الجهة> الالتزام بهذه السياسة والمتطلبات ذات العلاقة ما لم يكن هناك استثناء رسمي مسبق من <رئيس الإدارة المعنية بالأمن السيبراني> أو اللجنة الإشرافية للأمن السيبراني، بشرط ألا يتعارض هذا الاستثناء مع المتطلبات التشريعية والتنظيمية ذات العلاقة.