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 نص

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

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

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

اعتماد الوثيقة

الدور	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل الاسم الكامل للشخص>	اضغط هنا لإضافة نص	<أدخل التوقيع>

نسخ الوثيقة

النسخة	التاريخ	عُدلَ بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة نص	<أدخل الاسم الكامل للشخص>	<أدخل وصف التعديل>

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بتوثيق متطلبات الأمن السيبراني والتزام <اسم الجهة> بها، لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية، ويتم ذلك من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأعمال التنظيمية الخاصة بـ<اسم الجهة>، والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية لـ<اسم الجهة> وتنطبق على جميع العاملين في <اسم الجهة>.

وتعتبر هذه السياسة هي المحرك الرئيسي لجميع سياسات الأمن السيبراني وإجراءاته ومعاييره ذات المواضيع المختلفة، وكذلك أحد المدخلات لعمليات <اسم الجهة> الداخلية، مثل عمليات الموارد البشرية وعمليات إدارة الموردين وعمليات إدارة المشاريع وإدارة التغيير وغيرها.

عناصر السياسة

1- يجب على <الإدارة المعنية بالأمن السيبراني> تحديد معايير الأمن السيبراني وتوثيق سياساته وبرامجه، بناءً على نتائج تقييم المخاطر، وبشكل يضمن نشر متطلبات الأمن السيبراني، والتزام <اسم الجهة> بها، وذلك وفقاً لمتطلبات الأعمال التنظيمية لـ<اسم الجهة>، والمتطلبات التشريعية والتنظيمية ذات العلاقة. واعتمادها من قبل <رئيس الجهة>. كما يجب إطلاع العاملين المعنيين في <اسم الجهة> والأطراف ذات العلاقة عليها.

2- يجب على <الإدارة المعنية بالأمن السيبراني> تطوير سياسات الأمن السيبراني وبرامجه ومعاييره وتطبيقها، والمتمثلة في:

2-1 **برنامج استراتيجية الأمن السيبراني (Cybersecurity Strategy)** لضمان خطط العمل للأمن السيبراني والأهـداف والمبادرات والمشاريع وفعاليتها داخل <اسم الجهة> في تحقيق المتطلبات التشريعية والتنظيمية ذات العلاقة.

2-2 **أدوار ومسؤوليات الأمن السيبراني (Cybersecurity Roles and Responsibilities)** لضمان تحديد مهمات ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني في <اسم الجهة>.

2-3 **برنامج إدارة مخاطر الأمن السيبراني (Cybersecurity Risk Management)** لضمان إدارة المخاطر السيبرانية على نحو ممنهج يهدف إلى حماية الأصول المعلوماتية والتقنية لـ<اسم الجهة>، وذلك وفقاً للسياسات والإجراءات التنظيمية لـ<اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة.

4-2 **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 لـ<اسم الجهة> وضمان دقتها وتوافرها، وكذلك التأكد من تطبيق معايير الأمن السيبراني في أنشطة تطوير التطبيقات والبرامج، وفقاً للسياسات والإجراءات التنظيمية لـ<اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة.

5-2 **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.

6-2 **سياسة المراجعة والتدقيق الدوري للأمن السيبراني (Cybersecurity Periodical Assessment and Audit)** للتأكد من أن ضوابط الأمن السيبراني لدى <اسم الجهة> مطبقة، وتعمل وفقاً للسياسات والإجراءات التنظيمية لـ<اسم الجهة>، والمتطلبات التشريعية التنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المُقرة تنظيمياً على <اسم الجهة>.

7-2 **سياسة الأمن السيبراني المتعلق بالموارد البشرية (Cybersecurity in Human Resources)** للتأكد من أن مخاطر الأمن السيبراني ومتطلباته المتعلقة بالعاملين (الموظفين والمتعاقدين) في <اسم الجهة> تعالج بفعالية قبل إنهاء عملهم، وأثنائه وعند انتهائه، وذلك وفقاً للسياسات والإجراءات التنظيمية لـ<اسم الجهة>، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

8-2 **برنامج التوعية والتدريب بالأمن السيبراني (Cybersecurity Awareness and Training Program)** للتأكد من أن العاملين بـ<اسم الجهة> لديهم الوعي الأمني اللازم، وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني، مع التأكد من تزويد العاملين بـ<اسم الجهة> بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني؛ لحماية الأصول المعلوماتية والتقنية لـ<اسم الجهة> والقيام بمسؤولياتهم تجاه الأمن السيبراني.

9-2 **سياسة إدارة الأصول (Asset Management)** للتأكد من أن <اسم الجهة> لديها قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العلاقة لجميع الأصول المعلوماتية والتقنية المتاحة لـ<اسم الجهة>، من أجل دعم العمليات التشغيلية لـ<اسم الجهة> ومتطلبات الأمن السيبراني، لتحقيق سرية الأصول المعلوماتية والتقنية وسلامتها لـ<اسم الجهة>ودقتها وتوافرها.

10-2 **سياسة إدارة هويات الدخول والصلاحيات (Identity and Access Management)** لضمان حماية الأمن السيبراني للوصول المنطقي (Access Logical) إلى الأصول المعلوماتية والتقنية لـ<اسم الجهة> من أجل منع الوصول غير المصرح به، وتقييد الوصول إلى ماهو مطلوب لإنجاز الأعمال المتعلقة بـ<اسم الجهة>.

11-2 **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 لـ<اسم الجهة> من المخاطر السيبرانية.

12-2 **سياسة حماية البريد الإلكتروني (Email Protection)** لضمان حماية البريد الإلكتروني لـ<اسم الجهة> من المخاطر السيبرانية.

2-13 **سياسة إدارة أمن الشبكات (Networks Security Management)** لضمان حماية شبكات <اسم الجهة> من المخاطر السيبرانية.

2-14 **سياسة أمن الأجهزة المحمولة (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 الحساسة، والمعلومات الخاصة بأعمال <اسم الجهة> وحمايتها، أثناء النقل والتخزين، وعند استخدام الأجهزة الشخصية للعاملين في <اسم الجهة> (مبدأ "BYOD").

2-15 **سياسة حماية البيانات والمعلومات (Data and Information Protection)** لضمان حماية السرية، وسلامة بيانات ومعلومات <اسم الجهة> ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية لـ<اسم الجهة>، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-16 **سياسة التشفير ومعياره (Cryptography)** لضمان الاستخدام السليم والفعال للتشفير؛ لحماية الأصول المعلوماتية الإلكترونية لـ<اسم الجهة>، وذلك وفقاً للسياسات، والإجراءات التنظيمية لـ<اسم الجهة>، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-17 **سياسة إدارة النسخ الاحتياطية (Backup and Recovery Management)** لضمان حماية بيانات <اسم الجهة> ومعلوماتها، وكذلك حماية الإعدادات التقنية للأنظمة والتطبيقات الخاصة بـ<اسم الجهة> من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقاً للسياسات والإجراءات التنظيمية لـ<اسم الجهة>، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-18 **سياسة إدارة الثغرات ومعياره (Vulnerabilities Management)** لضمان اكتشاف الثغرات التقنية في الوقت المناسب، ومعالجتها بشكل فعال، وذلك لمنع احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية وتقليل ذلك، وكذلك تقليل الآثار المترتبة على أعمال <اسم الجهة>.

2-19 **سياسة اختبار الاختراق ومعياره (Penetration Testing)** لتقييم مدى فعالية قدرات تعزيز الأمن السيبراني واختباره في <اسم الجهة>، وذلك من خلال محاكاة تقنيات الهجوم السيبراني الفعلية وأساليبه، ولاكتشاف نقاط الضعف الأمنية غير المعروفة، والتي قد تؤدي إلى الاختراق السيبراني لـ<اسم الجهة>؛ وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-20 **سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني (Cybersecurity Event Logs and Monitoring Management)** لضمان جمع سجلات أحداث الأمن السيبراني، وتحليلها، ومراقبتها في الوقت المناسب؛ من أجل الاكتشاف الاستباقي للهجمات السيبرانية، وإدارة مخاطرها بفعالية؛ لمنع الآثار السلبية المحتملة على أعمال <اسم الجهة> أو تقليلها.

2-21 **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 استباقياً، من أجل منع الآثار السلبية المحتملة أو تقليلها على أعمال <اسم الجهة>، مع مراعاة ما ورد في الأمر السامي الكريم ذو الرقم 37140 والتاريخ 14\8\1438هـ.

2-22 **سياسة الأمن المادي (Physical Security)** لضمان حماية الأصول المعلوماتية والتقنية لـ<اسم الجهة> من الوصول المادي غير المصرح به، والفقدان والسرقة والتخريب.

2-23 **سياسة حماية تطبيقات الويب ومعياره (Web Application Security)** لضمان حماية تطبيقات الويب الداخلية والخارجية لـ<اسم الجهة> من المخاطر السيبرانية.

2-24 **جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال (Cybersecurity Resilience)** لضمان توافر متطلبات صمود الأمن السيبراني في إدارة استمرارية أعمال <اسم الجهة>، ولضمان معالجة الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحرجة وتقليلها لـ<اسم الجهة> وأنظمة معالجة معلوماتها وأجهزتها جراء الكوارث الناتجة عن المخاطر السيبرانية.

2-25 **سياسة الأمن السيبراني المتعلقة بالأطراف الخارجية (Third-Party and Cloud Computing 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") وفقاً للسياسات والإجراءات التنظيمية لـ<اسم الجهة>، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-26 **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 وفقاً للسياسات والإجراءات التنظيمية لـ<اسم الجهة>، والمتطلبات التشريعية والتنظيمية، والأوامر والقرارات ذات العلاقة. وضمان حماية الأصول المعلوماتية والتقنية لـ<اسم الجهة> على خدمات الحوسبة السحابية، التي تتم استضافتها أو معالجتها، أو إدارتها بواسطة أطراف خارجية.

2-27 **سياسة حماية أجهزة وأنظمة التحكم الصناعي (Industrial Control Systems Cybersecurity)** لضمان إدارة الأمن السيبراني بشكل سليم وفعال، لحماية توافر أصول <اسم الجهة> وسلامتها وسريتها؛ وهي الأصول المتعلقة وأنظمة التحكم الصناعي وأنظمته (OT\ICS) ضد الهجوم السيبراني (مثل الوصول غير المصرح به، والتخريب والتجسس والتلاعب) بما يتسق مع إستراتيجية الأمن السيبراني لـ<اسم الجهة>، وإدارة مخاطر الأمن السيبراني، والمتطلبات التشريعية والتنظيمية ذات العلاقة، وكذلك المتطلبات الدولية المقرّة تنظيمياً على <اسم الجهة> المتعلقة بالأمن السيبراني.

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

الأدوار والمسؤوليات

1- تُمثل القائمة الآتية مجموعة الأدوار والمسؤوليات اللازمة لإقرار سياسات الأمن السيبراني وإجراءاته، ومعاييره وبرامجه، وتنفيذها واتباعها:

1-1 مسؤوليات صاحب الصلاحية <رئيس الجهة أو من ينيبه>، على سبيل المثال:

1-1-1 إنشاء لجنة إشرافية للأمن السيبراني ويكون <رئيس الإدارة المعنية بالأمن السيبراني> أحد أعضائها.

2-1 مسؤوليات <الإدارة المعنية بالشؤون القانونية>، على سبيل المثال:

1-2-1 التأكد من أن شروط ومتطلبات الامن السيبراني والمحافظة على سرية المعلومات (Non-disclosure Clauses) مُلزمة قانونياً في عقود العاملين في <اسم الجهة>، والأطراف الخارجية.

3-1 مسؤوليات <الإدارة المعنية بالتدقيق والمراجعة الداخلية>، على سبيل المثال:

1-3-1 مراجعة ضوابط الأمن السيبراني وتدقيق تطبيقها وفقاً للمعايير العامة المقبولة للمراجعة والتدقيق، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

4-1 مسؤوليات <الإدارة المعنية بالموارد البشرية>، على سبيل المثال:

1-4-1 تطبيق متطلبات الأمن السيبراني المتعلقة بالعاملين في <اسم الجهة>.

5-1 مسؤوليات <الإدارة المعنية بالأمن السيبراني>، على سبيل المثال:

1-5-1 الحصول على موافقة <رئيس الجهة أو من ينيبه> على سياسات الأمن السيبراني، والتأكد من إطلاع الأطراف المعنية عليها وتطبيقها، ومراجعتها وتحديثها بشكل دوري.

6-1 مسؤوليات رؤساء الإدارات الأخرى، على سبيل المثال:

1-6-1 دعم سياسات الأمن السيبراني وإجراءاته ومعاييره وبرامجه، وتوفير جميع الموارد المطلوبة، لتحقيق الأهداف المنشودة، بما يخدم المصلحة العامة لـ<اسم الجهة>.

7-1 مسؤوليات العاملين، على سبيل المثال:

1-7-1 المعرفة بمتطلبات الأمن السيبراني المتعلقة بالعاملين في <اسم الجهة>، والالتزام بها.

الالتزام بالسياسة

1- يجب على صاحب الصلاحية <رئيس الجهة> ضمان الالتزام بسياسة الأمن السيبراني ومعاييره.

2- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بسياسات الأمن السيبراني ومعاييره بشكل دوري.

3- يجب على جميع العاملين في <اسم الجهة> الالتزام بهذه السياسة.

4- قد يُعرّض أي انتهاك للسياسات المتعلقة بالأمن السيبراني صاحب المخالفة إلى إجراءٍ تأديبي حسب الإجراءات المتبعة في <اسم الجهة>.

الاستثناءات

يُمنع تجاوز سياسات الأمن السيبراني ومعاييره، دون الحصول على تصريح رسمي مسبق من <رئيس الإدارة المعنية بالأمن السيبراني> أو اللجنة الإشرافية للأمن السيبراني، ما لم يتعارض مع المتطلبات التشريعية والتنظيمية ذات العلاقة.