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 سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية

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.

اختر التصنيف

التاريخ: اضغط هنا لإضافة نص

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

اعتماد الوثيقة

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

نسخ الوثيقة

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

قائمة المحتويات

الأهداف

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني لضمان حماية الأصول المعلوماتية والتقنية في <اسم الجهة> من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية بما في ذلك خدمات الإسناد لتقنية الملعومات والخدمات المدارة وفقا للسياسات والإجراءات التنظيمية الخاصة بـ<اسم الجهة>.

تتبع هذه السياسة المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهي متطلب تشريعي كما هو مذكور في الضابط رقم ١-١-٤ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تنطبق هذه السياسة على جميع الخدمات المقدمة من الأطراف الخارجية لـ<اسم الجهة>، وتنطبق على جميع العاملين في <اسم الجهة>.

بنود السياسة

1- البنود العامة

1-1 يجب توثيق واعتماد إجراءات موحدة لإدارة علاقة <اسم الجهة> مع الأطراف الخارجية قبل وأثناء وبعد انتهاء العلاقة التعاقدية.

2-1 يجب تحديد واختيار الأطراف الخارجية المقدمة للخدمات بعناية ووفقاً للسياسات والإجراءات التنظيمية لـ<اسم الجهة>، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

3-1 يجب إجراء تقييم للمخاطر على الأطراف الخارجية والخدمات المقدمة والتأكد من سلامتها، وذلك بمراجعة مشاريع الأطراف الخارجية داخل <اسم الجهة> ومراجعة سجلات الأحداث السيبرانية الخاص بخدمة الطرف الخارجي (إن أمكن) قبل وأثناء العلاقة وبشكل دوري.

4-1 يجب إعداد العقود والاتفاقيات مع الأطراف الخارجية بشكل يضمن التزام الطرف الخارجي بتطبيق متطلبات وسياسات الأمن السيبراني لـ<اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة.

5-1 يجب مراجعة العقود والاتفاقيات مع الأطراف الخارجية من قبل <الإدارة المعنية بالشؤون القانونية> للتأكد من أن تكون بنود الاتفاقية ملزمة أثناء فترة العقد وبعد انتهاءها وأن مخالفتها يعرض الطرف الخارجي للمساءلة قانونياً.

6-1 يجب أن تشمل العقود والاتفاقيات على بنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) والحذف الآمن من قِبَل الطرف الخارجي لبيانات <اسم الجهة> عند انتهاء الخدمة.

7-1 يجب مراجعة متطلبات الأمن السيبراني مع الأطراف الخارجية بشكل دوري.

8-1 يجب مراجعة سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية سنوياً، وتوثيق التغييرات واعتمادها.

2- متطلبات الأمن السيبراني الخاصة بخدمات الإسناد لتقنية المعلومات "Outsourcing" أو الخدمات المدارة "Managed Services" المقدمة من قبل الأطرف الخارجية

2-1 للحصول على خدمات إسناد لتقنية المعلومات أو خدمات مدارة، فإنه يجب اختيار الطرف الخارجي بعناية، ويجب أن يتم التحقق من الآتي:

2-1-1 إجراء تقييم لمخاطر الأمن السيبراني، والتأكد من وجود مايضمن السيطرة على تلك المخاطر، قبل توقيع العقود والاتفاقيات أو عند تغيير المتطلبات التشريعية والتنظيمية ذات العلاقة.

2-1-2 يجب أن تكون مراكز عمليات خدمات الأمن السيبراني المدارة للتشغيل والمراقبة والتي تستخدم طريقة الوصول عن بعد موجودة بالكامل داخل المملكة. (ECC-4-1-3-2)

2-1-3 خدمات الإسناد على الأنظمة الحساسة يجب أن تكون عن طريق شركات وجهات وطنية، وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة. (CSCC-4-1-1-2)

3- متطلبات الأمن السيبراني المتعلقة بموظفي الأطراف الخارجية

3-1 يجب أن يتم إجراء المسح الأمني (Screening or Vetting) لشركات خدمات الإسناد، ولموظفي خدمات الإسناد، والخدمات المدارة العاملين على الأنظمة الحساسة. (CSCC-4-1-1-1)

3-2 يجب تضمين مسؤوليات الأمن السيبراني وبنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) في عقود موظفي الأطراف الخارجية (لتشمل خلال وبعد انتهاء/ إنهاء العلاقة الوظيفية مع <اسم الجهة>).

4- التوثيق وضوابط الوصول

4-1 يجب أن تُطوّر الأطراف الخارجية وتتبع عملية رسمية وموثّقة بعناية لمنح وإلغاء حق الوصول إلى جميع الأنظمة المعلوماتية والتقنية التي تُعالِج أو تنقل أو تخزّن معلومات <اسم الجهة> بما يتماشى مع متطلّبات الأمن السيبراني وأهداف ضوابط الأمن السيبراني الخاصة بـ <اسم الجهة>.

4-2 يجب توفير إمكانية الوصول إلى معلومات <اسم الجهة> ومعالجتها بطريقة آمنة ومراقبة.

4-3 يجب تطبيق الضوابط المتعلّقة بكلمات المرور على جميع المستخدمين الذين يملكون حق الوصول إلى معلومات <اسم الجهة> بما يتماشى مع متطلّبات الأمن السيبراني وأهداف ضوابط الأمن السيبراني الخاصة بـ <اسم الجهة>.

4-4 يجب تطبيق نظام التحقّق من الهوية متعدّد العناصر على إمكانية الوصول إلى الأنظمة الحسّاسة التي تُعالج المعلومات الخاصة بـ <اسم الجهة> أو تنقلها أو تُخزّنها.

4-5 يجب إلغاء حقوق الوصول فور انتهاء/إنهاء خدمات أي موظف يعمل لدى الأطراف الخارجية ويملك حق الوصول إلى المعلومات أو الأصول المعلوماتية والتقنية الخاصة بـ <اسم الجهة> أو في حال تغيير دوره الوظيفي الذي لا يتطلّب استمرارية وصوله إليها.

4-6 يجب أن تقوم الأطراف الخارجية بمراجعة حقوق الوصول بوتيرة دورية وفقًا لسياسات الأمن السيبراني المعتمدة في <اسم الجهة>.

4-7 يجب تخزين كلّ سجلات التدقيق والحفاظ عليها وتوفيرها بناءً على طلب <اسم الجهة>.

5- متطلبات الأمن السيبراني المتعلقة بإدارة التغيير

1-5 يجب أن تتبع الأطراف الخارجية عملية إدارة التغيير الرسمية والمناسبة وفقاً لسياسات وإجراءات <اسم الجهة> وبما يتوافق مع متطلّبات الأمن السيبراني.

2-5 يجب مراجعة واختبار التغيير التي أجريت على الأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة> قبل تطبيقها على بيئة الإنتاج (Production Environment).

3-5 يجب إبلاغ الأطراف المعنية في <اسم الجهة> بالتغييرات الرئيسية التي مخطط إجراءها وكذلك التي أجريت على الأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة>.

6- متطلبات إدارة حوادث الأمن السيبراني واستمرارية الأعمال

1-6 يجب ان تتضمن بنود العقود والاتفاقيات مع الأطراف الخارجية على متطلبات متعلقة بالإبلاغ عن حوادث الأمن السيبراني وإبلاغ <اسم الجهة> في حال تعرض الطرف الخارجي إلى حادثة أمن سيبراني.

2-6 يجب تحديد وتوثيق إجراءات التواصل بين الطرف الخارجي و <اسم الجهة> في حال تعرض الطرف الخارجي إلى حادثة أمن سيبراني، ومراجعة وتحديث هذه الإجراءات بشكل دوري.

3-6 يجب وضع خطة مناسبة لاستمرارية الأعمال لتفادي عدم توافر الخدمات المقدمة لـ<اسم الجهة> وفقاً لمتطلّبات خطّة استمرارية الأعمال والتعافي من الكوارث الخاصة بـ<اسم الجهة>.

7- متطلبات حماية البيانات والمعلومات

1-7 يجب أن تقوم الأطراف الخارجية بمعالجة بيانات ومعلومات <اسم الجهة> وتخزينها وإتلافها وفقاً لسياسة ومعيار حماية البيانات والمعلومات المعتمدين في <اسم الجهة>.

2-7 يجب تطبيق ضوابط تشفير مناسبة لحماية بيانات ومعلومات <اسم الجهة> وضمان الحفاظ على سريّتها وسلامتها وتوافرها وفقاً لمعيار التشفير المعتمد في <اسم الجهة>.

3-7 يجب عمل نُسخ احتياطية من بيانات ومعلومات <اسم الجهة> بشكل دوري ووفقاً لسياسة إدارة النسخ الاحتياطية الخاصة بـ<اسم الجهة>.

4-7 يجب عدم معالجة أو تخزين أو استخدام بيانات ومعلومات <اسم الجهة> الموجودة في الأنظمة الحسّاسة والبيانات الشخصية (Data privacy)، والتي تُعالجها الأطراف الخارجية - في بيئة الاختبار إلا بعد استخدام ضوابط مشددة لحماية تلك البيانات مثل: تقنيات تعتيم البيانات (Data Masking) أو تقنيات مزج البيانات (Data Scrambling) أو تقنيات إخفاء البيانات (Data Anonymization). (CSCC-2-6-1-1)

5-7 يجب عدم نقل بيانات ومعلومات <اسم الجهة> الموجودة في الأنظمة الحسّاسة - والتي تُعالجها الأطراف الخارجية - خارج بيئة الإنتاج. (CSCC-2-6-1-5)

6-7 يجب تصنيف بيانات ومعلومات <اسم الجهة> الموجودة في الأنظمة الحسّاسة - والتي تُعالجها الأطراف الخارجية - وفقاً لسياسة تصنيف البيانات والمعلومات المعتمدة في <اسم الجهة>. (CSCC-2-6-1-2)

8- التدقيق

1-8 يجب أن تُجري <اسم الجهة> تدقيقًا للعمليات والأنظمة ذات الصلة متى كان ذلك ضرورياً أو مناسباً.

2-8 يجب أن تتعاون جميع مرافق الطرف الخارجي وموظفيه بصورة كاملة مع أنشطة مراجعة سجل الأحداث والتدقيق التي تقوم بها <اسم الجهة> بما يشمل المراجعات المُنفّذة.

الأدوار والمسؤوليات

1-**راعي ومالك وثيقة السياسة:** < رئيس الإدارة المعنية بالأمن السيبراني>.

2-**تحديث السياسة ومراجعتها:** < الإدارة المعنية بالأمن السيبراني>.

3-**تنفيذ السياسة وتطبيقها:** < الإدارة المعنية بالأمن السيبراني> و<الإدارة المعنية بتقنية المعلومات> و <الإدارة المعنية بالموارد البشرية> و <الإدارة المعنية بالشؤون القانونية> و <الإدارة المعنية بالمشتريات>.

الالتزام بالسياسة

1- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> ضمان التزام <اسم الجهة> بهذه السياسة بشكل دوري.
2- يجب على جميع الإدارات المعنية بتنفيذ وتطبيق السياسة في <اسم الجهة> الالتزام بهذه السياسة.
3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة لإجراء تأديبي حسب الإجراءات المتبعة في <اسم الجهة>.