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

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 "<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

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية في <اسم الجهة> من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية بما في ذلك خدمات الإسناد لتقنية المعلومات والخدمات المدارة وفقًا للسياسات والإجراءات التنظيمية الخاصة ب<اسم الجهة>.

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

نطاق العمل

تنطبق هذه السياسة على جميع الخدمات المقدمة من الأطراف الخارجية وموظفيهم بما في ذلك خدمات الإسناد لتقنية المعلومات والخدمات المدارة ل<اسم الجهة>، وتنطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

بنود السياسة

١- البنود العامة

١-١ يجب توثيق واعتماد وتطبيق الإجراءات لإدارة علاقة <اسم الجهة> مع الأطراف الخارجية قبل وأثناء وبعد انتهاء العلاقة التعاقدية.

١-٢ يجب إجراء تقييم لمخاطر الأمن السيبراني على الأطراف الخارجية والخدمات المقدمة، ويشمل ذلك على سبيل المثال لا الحصر مراجعة مشاريع الأطراف الخارجية داخل <اسم الجهة> ومراجعة سجلات الأحداث السيبرانية الخاص بخدمات الطرف الخارجي (إن أمكن) قبل وأثناء العلاقة وبشكل دوري وفقًا لسياسة إدارة مخاطر الأمن السيبراني المعتمدة لدى <اسم الجهة>، بحيث تشمل إجراءات تقييم مخاطر الأمن السيبراني تحديد ضوابط الحماية للازمة تطبيقها لإدارة الفعالة لمخاطر الأمن السيبراني المكتشفة.

١-٣ يجب أن يتم إجراء المسح الأمني (Screening or Vetting) لشركات خدمات الإسناد والخدمات المدارة التي تقدم خدمات لدعم أو تشغيل الأنظمة الحساسة.

١-٤ يجب أن تتضمن العقود والاتفاقيات مع الأطراف الخارجية متطلبات الأمن السيبراني ل<اسم الجهة> وبنود إلزام الأطراف الخارجية بسياسات الأمن السيبراني ل<اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٥ يجب تضمين مسؤوليات الأمن السيبراني وبنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) والحذف الآمن في عقود موظفي الأطراف الخارجية لبيانات <اسم الجهة> (لتشمل خلال وبعد انتهاء/ إنهاء العلاقة الوظيفية مع <اسم الجهة>).

١-٦ يجب التأكد من قيام الطرف الخارجي بإدارة مخاطر الأمن السيبراني الخاصة به.

١-٧ يجب على الأطراف الخارجية منح <اسم الجهة> الصلاحيات اللازمة لإجراء الاختبارات للتحقق من التزام الأطراف الخارجية لمتطلبات الأمن السيبراني لدى <اسم الجهة>، وتوفير التقارير المطلوبة عند الحاجة.

١-٨ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات الأمن السيبراني المتعلقة بالأطراف الخارجية.

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

٢-١ للحصول على خدمات إسناد لتقنية المعلومات أو خدمات مدارة، فإنه يجب اختيار الطرف الخارجي بعناية، ويجب أن يتم التحقق على الأقل من الآتي:

٢-١-١ 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.

٢-١-٢ يجب أن تكون مراكز عمليات خدمات الأمن السيبراني المدارة للتشغيل والمراقبة والتي تستخدم طريقة الوصول عن بعد موجودة بالكامل داخل المملكة.

٢-١-٣ يجب أن تكون خدمات الإسناد على الأنظمة الحساسة عن طريق شركات وجهات وطنية، وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-١-٤ يجب أن تكون خدمات الإسناد والخدمات المدارة التي تتعامل مع البيانات المصنفة عن طريق شركات وجهات وطنية، وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.

٣- متطلبات الأمن السيبراني المتعلقة بموظفي الأطراف الخارجية

٣-١ يجب أن يتم إجراء المسح الأمني (Screening or Vetting) لشركات خدمات الإسناد، ولموظفي خدمات الإسناد، والخدمات المدارة للعاملين على الأنظمة الحساسة والعاملين الذين لديهم صلاحيات الاطلاع على البيانات المصنفة.

٣-٢ يجب ضمان توقيع موظفي الأطراف الخارجية المتوقع وصولهم بشكل مباشر أو غير مباشر إلى أصول <اسم الجهة> على تعهد حماية سرية المعلومات قبل الدخول في علاقة العمل، وذلك وفقًا للصيغة المعتمدة لدى <اسم الجهة>.

٣-٣ يجب ضمان توعية موظفي الطرف الخارجي بمتطلبات الأمن السيبراني الخاصة ب<اسم الجهة> وضمان التزامهم بها.

٤- متطلبات الأمن السيبراني المتعلقة بالتوثيق وضوابط الوصول

٤-١ يجب أن تُطوّر الأطراف الخارجية إجراءات معتمدة لمنح وإلغاء حق الوصول لجميع الأنظمة المعلوماتية والتقنية التي تُعالِج أو تنقل أو تخزّن معلومات <اسم الجهة> بما يتماشى مع متطلّبات الأمن السيبراني وأهداف ضوابط الأمن السيبراني الخاصة ب<اسم الجهة>.

٤-٢ يجب تقييد الوصول لموظفي الأطراف الخارجية إلى معلومات <اسم الجهة> ومعالجتها بطرق آمنة والتأكد من مراقبة عمليات الوصول بشكل مستمر.

٤-٣ يجب تطبيق الضوابط المتعلّقة بكلمات المرور على جميع المستخدمين الذين يملكون صلاحية الوصول إلى معلومات <اسم الجهة> بما يتوافق مع متطلّبات الأمن السيبراني وأهداف ضوابط الأمن السيبراني الخاصة ب<اسم الجهة>.

٤-٤ يجب إلغاء حقوق الوصول والصلاحيات فور انتهاء/إنهاء خدمات أي موظف يعمل لدى الأطراف الخارجية ويملك حق الوصول إلى المعلومات أو الأصول المعلوماتية والتقنية الخاصة ب<اسم الجهة> أو في حال تغيير دوره الوظيفي الذي لا يتطلّب استمرارية وصوله إليها.

٤-٥ يجب أن تقوم الأطراف الخارجية بمراجعة حقوق الوصول دوريًا وفقًا لسياسة إدارة هويات الدخول والصلاحيات المعتمدة لدى <اسم الجهة>.

٤-٦ يجب تخزين جميع سجلات التدقيق بطرق آمنة والحفاظ عليها وتوفيرها بناءً على طلب <اسم الجهة> ووفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.

٥- متطلبات الأمن السيبراني المتعلقة بإدارة التغيير

٥-١ يجب أن تتبع الأطراف الخارجية عملية إدارة التغيير الرسمية والمناسبة وفقًا لسياسات وإجراءات <اسم الجهة>.

٥-٢ يجب مراجعة واختبار التغييرات التي تم إجراءها على الأصول المعلوماتية والتقنية الخاصة ب<اسم الجهة> قبل تطبيقها على بيئة الإنتاج (Production Environment).

٥-٣ يجب إبلاغ الأطراف المعنية في <اسم الجهة> بالتغييرات الرئيسية المخطط إجراؤها وكذلك التي أجريت على الأصول المعلوماتية والتقنية الخاصة ب<اسم الجهة>.

٦- متطلبات إدارة حوادث الأمن السيبراني واستمرارية الأعمال

٦-١ 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.

٦-٢ يجب تحديد وتوثيق إجراءات التواصل بين الطرف الخارجي و <اسم الجهة> في حال تعرض الطرف الخارجي إلى حادثة أمن سيبراني أو الإبلاغ عن الثغرات، ومراجعة وتحديث هذه الإجراءات بشكل دوري.

٦-٣ يجب وضع خطة مناسبة لاستمرارية الأعمال لتفادي عدم توافر الخدمات المقدمة ل<اسم الجهة> وفقًا لمتطلّبات خطّة استمرارية الأعمال والتعافي من الكوارث الخاصة ب<اسم الجهة>.

٧- متطلبات حماية البيانات والمعلومات

٧-١ يجب تصنيف بيانات ومعلومات <اسم الجهة> الموجودة في جميع الأنظمة، والتي تُعالجها أو تخزنها الأطراف الخارجية، وفقًا لسياسة تصنيف البيانات والمعلومات المعتمدة في <اسم الجهة>.

٧-٢ يجب أن تقوم الأطراف الخارجية بمعالجة بيانات ومعلومات <اسم الجهة> وتخزينها وإتلافها وفقًا لسياسة ومعيار حماية البيانات والمعلومات المعتمدين في <اسم الجهة>.

٧-٣ يجب أن تتضمن العقود والاتفاقيات مع الأطراف الخارجية القدرة على حذف بيانات الجهة بطرق آمنة لدى الطرف الخارجي عند الانتهاء/إنهاء العلاقة التعاقدية مع تقديم الأدلة على ذلك.

٧-٤ يجب على الأطراف الخارجية تطبيق ضوابط تشفير مناسبة لحماية البيانات والمعلومات حسب تصنيفها لدى <اسم الجهة> وضمان الحفاظ على سريّتها وسلامتها وتوافرها وفقًا لمعيار التشفير المعتمد لدى <اسم الجهة>.

٧-٥ يجب على الأطراف الخارجية عمل نُسخ احتياطية من بيانات ومعلومات <اسم الجهة> بشكل دوري ووفقًا لسياسة إدارة النسخ الاحتياطية الخاصة ب<اسم الجهة>.

٧-٦ يجب عدم معالجة أو تخزين أو استخدام بيانات ومعلومات <اسم الجهة> الموجودة في الأنظمة الحسّاسة والبيانات الشخصية، 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) وبعد أخذ الموافقات اللازمة من الإدارات المعنية في <اسم الجهة> وذلك لضمان حماية البيانات وضمان خصوصية البيانات (Data privacy) وفقاً لإرشادات ومتطلبات مكتب إدارة البيانات الوطنية.

٧-٧ يجب عدم نقل بيانات ومعلومات <اسم الجهة> الموجودة في الأنظمة الحسّاسة، والتي تُعالجها أو تخزنها الأطراف الخارجية، خارج بيئة الإنتاج.

٨- التدقيق

٨-١ يجب أن تُجري <اسم الجهة> تدقيقًا للعمليات والأنظمة ذات الصلة متى كان ذلك ضروريًا أو مناسبًا.

٨-٢ يجب أن يتعاون جميع موظفي الطرف الخارجي بصورة كاملة مع أنشطة مراجعة سجل الأحداث والتدقيق التي تقوم بها <اسم الجهة> بما يشمل المراجعات المُنفّذة.

الأدوار والمسؤوليات

١- **مالك السياسة:** < رئيس الإدارة المعنية بالأمن السيبراني>.

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

٣- **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>.

٤- **قياس الالتزام بالسياسة:** <الإدارة المعنية بالأمن السيبراني>.

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.

اختر التصنيف

الإصدار <١,٠>

الالتزام بالسياسة

١- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذه السياسة بشكل دوري.
٢- يجب على جميع العاملين في <اسم الجهة> الالتزام بهذه السياسة.
٣- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة لإجراء تأديبي حسب الإجراءات المتبعة في <اسم الجهة>.