هذا المربع مخصّص لأغراض توجيهية. احذف جميع المربعات التوجيهية بعد تعبئة النموذج. يجب تحرير البنود الملوّنة باللون الأزرق بصورة مناسبة. والبنود الملونة باللون الأخضر هي أمثلة يجب حذفها. ويجب حذف التظليل الملون بعد إجراء التعديلات.

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج سياسة الأمن السيبراني للبيانات

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.
- 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.

اختر التصنيف

الإصدار <١,٠>

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	عُدّلَ 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

اختر التصنيف

الإصدار <١,٠>

الغرض

الغرض من هذه السياسة هو تحديد متطلبات الأمن السيبراني المتعلقة بالأمن السيبراني للبيانات الخاصة بـ<اسم الجهة> لتقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية وذلك لتحقيق الأهداف الرئيسية للحماية وهي: سرية المعلومات، وسلامة أنظمة المعلومات، وتوافرها.

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

نطاق السياسة

تنطبق هذه السياسة على جميع البيانات التي تحتفظ بها <اسم الجهة> وتخزنها وتعالجها وتنقلها من خلال الأصول المعلوماتية والتقنية، وعلى جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

بنود السياسة

١- البنود العامة

١-١ يجب أن تلتزم <اسم الجهة> بالمتطلبات التشريعية والتنظيمية المتعلقة بحماية البيانات في المملكة العربية السعودية، والسياسات والإجراءات المتبعة في <اسم الجهة>.

١-٢ يجب أن تحدد <اسم الجهة> وتحدث متطلبات الأمن السيبراني للبيانات بشكل دوريًا.

١-٣ يجب على <اسم الجهة> ضمان إدارة متطلبات الأمن السيبراني للبيانات بكفاءة وفقًا لسياسة الأمن السيبراني في الموارد البشرية وسياسة إدارة الأصول الخاصة ب<اسم الجهة>.

١-٤ يجب أن تضمن <اسم الجهة> حماية الأجهزة المحمولة وفقًا لسياسة أمن الأجهزة المحمولة في <اسم الجهة>.

١-٥ يجب أن تستخدم <اسم الجهة> تقنيات وحلول منع تسريب البيانات.

١-٦ يحظر استخدام بيانات <اسم الجهة> في أي بيئة غير بيئة الإنتاج، إلا بعد إجراء تقييم للمخاطر وتطبيق الضوابط لحماية تلك البيانات، مثل: تقنيات تعتيم البيانات (masking) أو تقنيات مزج البيانات (data scrambling).

١-٧ يجب أن تحدد <اسم الجهة> التقنيات والأدوات والإجراءات للتخلص من البيانات بطريقة آمنة حسب مستوى التصنيف.

١-٨ يجب أن تعمل <اسم الجهة> على إعداد وتنفيذ استراتيجية للخروج لضمان وسائل الإتلاف الآمن للبيانات عند إنهاء أو انتهاء سريان العقد مع مقدم الخدمة السحابية.

١-٩ يجب أن تضمن <اسم الجهة> الاستخدام المناسب والفعال لتقنيات التشفير لحماية بيانات <اسم الجهة> وفقًا لسياسة ومعايير التشفير في <اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة.

اختر التصنيف

الإصدار <١,٠>

١-١٠ يجب على <اسم الجهة> تحديد الأدوار والمسؤوليات للأمن السيبراني لضمان ان البيانات متوافقة مع المتطلبات القانونية والتنظيمية.

١-١١ يجب أن تستخدم <اسم الجهة> طريقة آمنة لاستخراج ونقل البيانات واستخراج ونقل البنية التحتية الافتراضية.

١-١٢ يجب أن تمنع <اسم الجهة> نقل أي بيانات للأنظمة الحساسة من بيئة الإنتاج إلى أي بيئة أخرى.

١-١٣ يجب أن تستخدم <اسم الجهة> خاصية العلامات المائية (watermark feature) لترميز الوثيقة بأكملها عند إعدادها، أو تخزينها، وطباعتها، او عرضها على الشاشة، والتأكد من احتواء كل نسخة من الوثيقة على رقم يمكن تتبعه.

١-١٤ يجب قياس مؤشرات الأداء الرئيسية (KPI) للتأكد من التحسين المستمر لمتطلبات الأمن السيبراني لحماية البيانات.

٢- التصنيف والتعامل الآمن مع المعلومات

٢-١ يجب تصنيف بيانات <اسم الجهة> وفقًا لسياسة تصنيف البيانات المعتمدة في <اسم الجهة>.

٢-٢ يجب تصنيف جميع بيانات <اسم الجهة> في كل الصيغ التالية:

٢-٢-١ الصيغ الرقمية (مثل وثائق برنامج معالج النصوص "Word"، وجداول البيانات "Spreadsheets"، وقواعد البيانات).

٢-٢-٢ الاتصالات الإلكترونية (مثل رسائل البريد الإلكتروني وخدمات الاتصالات الصوتية والمؤتمرات والاتصالات الهاتفية وغيرها)

٢-٢-٣ الصيغ المادية (مثل المطبوعات، والنسخ الورقية للعقود ودفاتر الملاحظات).

٢-٢-٤ المحادثات الشفهية (مثل الاجتماعات والمقابلات).

٢-٣ يجب أن يتجنب العاملون مناقشة بيانات <اسم الجهة> بصيغة شفهية في المناطق العامة، أو في مناطق قد تُسمع فيها مناقشاتهم. ويجب أن تتم المناقشات في مقرات <اسم الجهة> وفي مواقع آمنة ضمن المقرات.

٢-٤ يجب تصنيف جميع البيانات التي تحتفظ فيها <اسم الجهة> في كل الأنظمة (بما في ذلك الأنظمة الحساسة وأنظمة الحوسبة السحابية) وترميزها وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة، وسياسة تصنيف البيانات المعتمدة في <اسم الجهة>.

٢-٥ يجب أن يتولى المسؤولون عن البيانات، الذين عينتهم <اسم الجهة> للعمل مع الأطراف المعنية ذات العلاقة مع <اسم الجهة>، مسؤولية تصنيف البيانات على النحو الوارد في هذه السياسة.

٢-٦ يجب إبلاغ الأطراف المعنية ذات العلاقة في <اسم الجهة> على الفور عن أي مخالفة لهذه السياسة ولضوابط تصنيف البيانات.

٢-٧ يجب تطبيق ضوابط الوصول عن بُعد للبيانات وفقًا لنموذج سياسة إدارة هويات الدخول والصلاحيات المعتمدة في <اسم الجهة>.

٢-٨ يجب عدم حفظ البيانات المصنفة (سرية، سرية للغاية) في أجهزة تخزين محمولة مثل الأقراص الصلبة الخارجية أو وحدات التخزين "USB"، بغض النظر عن مستوى التشفير المستخدم في جهاز التخزين المحمول.

٢-٩ يجب عدم إدخال أو معالجة أو تغيير أو حفظ أو نقل البيانات المصنفة (سرية، وسرية للغاية) إلى الأجهزة التي يملكها الموظفون، والتي يُطلق عليها استخدام الأجهزة الشخصية للعاملين في الجهة (BYOD)، ما لم تكن تلك البيانات خاصة بالموظفين.

٢-١٠ يجب حماية البيانات المصنفة (سرية، وسرية للغاية) التي يمكن الوصول إليها أو معالجتها أو حفظها أو نقلها من خلال أنظمة الدخول عن بعد، ما لم تكن تلك البيانات خاصة بالموظفين.

٢-١١ يجب تحديد المجموعات الفرعية من البيانات المصنفة (مثل سرية، وسرية للغاية)، التي يمكن الوصول إليها أو معالجتها أو حفظها أو نقلها من خلال أنظمة العمل عن بُعد، وفقًا للمتطلبات التنظيمية ذات العلاقة.

٢-١٢ يجب ألّا تحتوي الأصول التقنية لإدارة حسابات مواقع التواصل الاجتماعي لـ<اسم الجهة> على بيانات مصنفة، وفقًا للمتطلبات التنظيمية ذات العلاقة.

٣- الاحتفاظ بالسجلات

٣-١ يجب أن تحتفظ <اسم الجهة> بسجلات المعتمدة المقدمة من ملاك البيانات، ويجب أن تحتفظ بسجلات سحب أو إلغاء الموافقات لفترة زمنية محددة وفقًا للمتطلبات التشريعية والتنظيمية.

٣-٢ يجب أن تحتفظ <اسم الجهة> بسجل لجميع عمليات الإتلاف الآمن للبيانات التي تم تنفيذها.

٣-٣ يجب أن تحتفظ <اسم الجهة> بالبيانات طوال المدة المحددة وفقًا للمتطلبات التشريعية والتنظيمية أو عندما تصبح البيانات الحساسة غير مطلوبة للغرض الذي جمعت من أجله.

٣-٤ يجب أن تُنشئ <اسم الجهة> سجل بأنشطة المعالجة وتحدثه عند الحاجة مع الاحتفاظ بنسخ طوال المدة المحددة وفقًا للمتطلبات التشريعية والتنظيمية.

٣-٥ يجب تحديد فترة الاحتفاظ بجميع البيانات المتعلقة بالأنظمة وفقًا للتشريعات ذات العلاقة، والاحتفاظ فقط بالبيانات المطلوبة في بيئة الإنتاج.

الأدوار والمسؤوليات

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

٢- **مراجعة السياسة وتحديثها:** <الإدارة المعنية بالأمن السيبراني>.

اختر التصنيف

الإصدار <١,٠>

٣- **تنفيذ السياسة وتطبيقها:** <الإدارة المعنية بتقنية المعلومات> و<الإدارة المعنية بالأمن السيبراني>.

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.

الالتزام بالسياسة

١- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذه السياسة دوريًا.

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

٣- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في <اسم الجهة>.