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 للموارد البشرية

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	عُدِلَ 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 متطلبات الأمن السيبراني المتعلقة بالعاملين في <اسم الجهة> لتقليل المخاطر السيبرانية عليها وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

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

نطاق العمل

تطبق هذه السياسة على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

بنود السياسة

١- البنود العامة

١-١ يجب حصر واعتماد متطلبات الأمن السيبراني المتعلقة بالعاملين قبل توظيفهم وأثناء عملهم وعند انتهاء/إنهاء عملهم في الجهة.

١-٢ يجب على <اسم الجهة> تنظيم حملات توعية أمنية في الأمن السيبراني لجميع العاملين.

١-٣ يجب مراجعة متطلبات الأمن السيبراني الخاصة ب<الموارد البشرية> مرة واحدة سنويًا على الأقل بما يشمل الضوابط المتعلقة بالعاملين في الجهة دوريًا وتوثيق واعتماد التغييرات من قبل صاحب الصلاحية في الجهة وتحديث هذه السياسة وفقًا لذلك.

١-٤ يجب أن يشغل الوظائف ذات العلاقة بالأنظمة الحساسة في <اسم الجهة> مواطنون سعوديون ذو كفاءة عالية.

١-٥ يجب تحديد المؤهلات والمهارات والقدرات المطلوبة لوظائف الأمن السيبراني المختلفة بشكل دقيق.

١-٦ يجب أن يشغل وظائف الأمن السيبراني مواطنون سعوديون مؤهلون فيما يتعلق بمراكز البيانات التابعة لمقدم خدمة الحوسبة السحابية داخل المملكة العربية السعودية.

١-٧ يجب تنفيذ ضوابط الأمن السيبراني الخاصة بالموارد البشرية خلال دورة حياة عمل الموظف (Lifecycle) في <اسم الجهة> والتي تشمل المراحل التالية:

- قبل التوظيف.
- خلال فترة العمل.
- عند انتهاء فترة العمل أو إنهائها.

١-٨ يجب تطبيق متطلبات الأمن السيبراني المتعلقة بالعاملين المسؤولين عن إدارة حسابات التواصل الاجتماعي والالتزام بها وفقًا لسياسات وإجراءات وعمليات الأمن السيبراني لحسابات التواصل الاجتماعي.

١-٩ يجب على العاملين في <اسم الجهة> فهم أدوارهم الوظيفية، والشروط والمسؤوليات ذات العلاقة بالأمن السيبراني، والموافقة عليها.

١-١٠ يجب ضمان التأكد من أن مخاطر الأمن السيبراني المتعلقة بالعاملين (موظفين ومتعاقدين) لدى مقدمي خدمات الحوسبة السحابية والمشتركين في خدمات الحوسبة السحابية، تعالج بفعالية قبل وأثناء وعند انتهاء/إنهاء عملهم، وذلك وفقًا للسياسات والإجراءات التنظيمية لديهم، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-١١ يجب تضمين مسؤوليات الامن السيبراني وبنود المحافظة على سرية المعلومات (Non-Disclosure Agreement) في عقود العاملين في <اسم الجهة> (لتشمل خلال وبعد انتهاء/إنهاء العلاقة الوظيفية مع <اسم الجهة>).

١-١٢ يجب إدراج المخالفات ذات العلاقة بالأمن السيبراني في لائحة مخالفات الموارد البشرية في <اسم الجهة>.

١-١٣ يُمنع الاطلاع على المعلومات الخاصة بالموظفين دون تصريح مسبق.

١-١٤ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات الأمن السيبراني المتعلق بالموارد البشرية.

٢- قبل التوظيف

٢-١ يجب على العاملين التعهد بالالتزام بسياسات الأمن السيبراني قبل منحهم صلاحية الوصول إلى أنظمة <اسم الجهة>.

٢-٢ يجب تحديد أدوار الموظفين ومسؤولياتهم المتعلقة بالأمن السيبراني في الوصف الوظيفي مع الأخذ بالاعتبار تطبيق مبدأ عدم تعارض المصالح.

٢-٣ يجب أن تشمل الأدوار والمسؤوليات المتعلقة بالأمن السيبراني الآتي:

٢-٣-١ حماية جميع أصول <اسم الجهة> من الوصول غير المصرح به، أو تخريب تلك الأصول.

٢-٣-٢ تنفيذ جميع الأنشطة المطلوبة المتعلقة بالأمن السيبراني.

٢-٣-٣ الالتزام بسياسات وإجراءات ومعايير الأمن السيبراني الخاصة بـ<اسم الجهة>.

٢-٣-٤ الالتزام ببرنامج زيادة مستوى الوعي بالمخاطر السيبرانية.

٢-٤ يجب إقرار وتوقيع العاملين على جميع سياسات الأمن السيبراني كشرط مسبق للوصول إلى الأنظمة التقنية السحابية.

٢-٥ يجب إجراء مسح أمني للعاملين في وظائف الأمن السيبراني، والوظائف التقنية ذات الصلاحيات الهامة والحساسة، والوظائف ذات العلاقة بالأنظمة الحساسة.

٢-٦ يجب إجراء المسح الأمني للعاملين الذين لهم حق الوصول إلى المهام الحساسة لخدمات الحوسبة السحابية، مثل: إدارة المفاتيح، إدارة الخدمات، التحكم بالوصول (Access Control).

٣- اثناء العمل

١-٣ يجب تقديم برنامج توعوي لجميع العاملين في <اسم الجهة>، يختص بزيادة مستوى الوعي بالأمن السيبراني وذلك بشكل دوري.

٢-٣ يجب تقديم التوعية بالأمن السيبراني عن طريق جميع القنوات المتاحة والمستخدمة في <اسم الجهة> وبما يشمل حسابات التواصل الاجتماعي لـ<اسم الجهة>.

٣-٣ يجب على <الإدارة المعنية بالموارد البشرية> إبلاغ الإدارات ذات العلاقة عن أي تغيير في أدوار العاملين أو مسؤولياتهم بهدف اتخاذ الإجراءات اللازمة المتعلقة بإلغاء صلاحيات الوصول أو تعديلها.

٤-٣ يجب التأكد من تطبيق جميع متطلبات الأمن السيبراني الخاصة بالموارد البشرية.

٥-٣ يجب إدراج مدى الالتزام بالأمن السيبراني ضمن جوانب تقييم الموظفين.

٦-٣ يجب التأكد من تطبيق مبدأ الحاجة إلى المعرفة (Need-to-know) في تكليف المهمات.

٤- انتهاء الخدمة أو إنهاؤها

١-٤ يجب تحديد إجراءات انتهاء الخدمة المهنية أو إنهائها بشكل يغطي متطلبات الأمن السيبراني.

٢-٤ يجب على <الإدارة المعنية بالموارد البشرية> إبلاغ الوحدات ذات العلاقة في حال اقتراب موعد انتهاء العلاقة الوظيفية أو إنهائها لاتخاذ الإجراءات اللازمة.

٣-٤ يجب التأكد من إعادة جميع الأصول الخاصة ب<اسم الجهة> وإلغاء صلاحيات الدخول للعاملين في آخر يوم عمل لهم وقبل حصولهم على المخالصات اللازمة.

٤-٤ يجب تحديد المسؤوليات والواجبات التي ستبقى سارية المفعول بعد انتهاء خدمة العاملين في <اسم الجهة>، بما في ذلك اتفاقية المحافظة على سرية المعلومات، على أن يتم إدراج تلك المسؤوليات والواجبات في جميع عقود العاملين.

الأدوار والمسؤوليات

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

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

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

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 بشكل دوري.

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

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