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

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	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 لضمان التأكد من أن مخاطر ومتطلبات الأمن السيبراني المتعلقة بالعاملين (موظفين ومتعاقدين) في <اسم الجهة> تعالج بفعالية قبل وأثناء وعند انتهاء/إنهاء عملهم.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٩-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأنظمة الخاصة بـ<اسم الجهة> وتنطبق على جميع العاملين في <اسم الجهة>.

بنود السياسة

البنود العامة

1-1 يجب تحديد متطلبات الأمن السيبراني المتعلقة بالعاملين.

2-1 يجب أن يشغل الوظائف ذات العلاقة بالأنظمة الحساسة في <اسم الجهة> مواطنون ذو الكفاءة اللازمة.

3-1 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

4-1 يجب على العاملين في <اسم الجهة> فهم أدوارهم الوظيفية، والشروط والمسؤوليات ذات العلاقة بالأمن السيبراني، والموافقة عليها.

5-1 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>).

6-1 يجب إدراج المخالفات ذات العلاقة بالأمن السيبراني في لائحة مخالفات الموارد البشرية في <اسم الجهة>.

7-1 يُمنع الاطلاع على المعلومات الخاصة بالموظفين دون تصريح مسبق.

8-1 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لمتطلبات الأمن السيبراني المتعلق بالموارد البشرية.

قبل التوظيف

1-2 يجب على العاملين التعهد بالالتزام بسياسات الأمن السيبراني قبل منحهم صلاحية الوصول إلى أنظمة <اسم الجهة>.

2-2 يجب تحديد أدوار الموظفين ومسؤولياتهم مع الأخذ في الحسبان تطبيق مبدأ عدم تعارض المصالح.

3-2 يجب تحديد أدوار الموظفين ومسؤولياتهم المتعلقة بالأمن السيبراني في الوصف الوظيفي.

4-2 يجب أن تشمل الأدوار والمسؤوليات المتعلقة بالأمن السيبراني الآتي:

- حماية جميع أصول <اسم الجهة> من الوصول غير المصرح به، أو تخريب تلك الأصول.
- تنفيذ جميع الأنشطة المطلوبة المتعلقة بالأمن السيبراني.
- الالتزام بسياسات الأمن السيبراني ومعاييره الخاصة بـ<اسم الجهة>.
- الالتزام ببرنامج زيادة مستوى الوعي بالمخاطر السيبرانية.

5-2 يجب إجراء مسح أمني للعاملين في وظائف الأمن السيبراني، والوظائف التقنية ذات الصلاحيات الهامة والحساسة، والوظائف ذات العلاقة بالأنظمة الحساسة.

أثناء العمل

1-3 يجب تقديم برنامج توعوي، يختص بزيادة مستوى الوعي بالأمن السيبراني؛ بما في ذلك سياسات الأمن السيبراني ومعاييره، بشكل دوري.

2-3 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.

3-3 يجب التأكد من تطبيق متطلبات الأمن السيبراني الخاصة بالموارد البشرية.

4-3 يجب إدراج مدى الالتزام بالأمن السيبراني ضمن جوانب تقييم الموظفين.

5-3 يجب التأكد من تطبيق مبدأ الحاجة إلى المعرفة (Need-to-know) في تكليف المهمات.

انتهاء الخدمة أو إنهاؤها

1-4 يجب تحديد إجراءات انتهاء الخدمة المهنية أو إنهائها بشكل يغطي متطلبات الأمن السيبراني.

2-4 يجب على <الإدارة المعنية بالموارد البشرية> إبلاغ الوحدات ذات العلاقة في حال اقتراب موعد انتهاء العلاقة الوظيفية أو إنهائها لاتخاذ الإجراءات اللازمة.

3-4 يجب التأكد من إعادة جميع الأصول الخاصة بـ<اسم الجهة> وإلغاء صلاحيات الدخول للعاملين في آخر يوم عمل لهم وقبل حصولهم على المخالصات اللازمة.

4-4 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

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

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

3- **تنفيذ السياسة وتطبيقها:** <الإدارة المعنية بالموارد البشرية>.

الالتزام بالسياسة

1- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> ضمان التزام <اسم الجهة> بهذه السياسة دورياً.

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

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

اختر التصنيف