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 الاستخدام المقبول للأصول

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؛ لتقليل المخاطر السيبرانية، المتعلقة باستخدام أنظمة <اسم الجهة> وأصولها، وحمايتها من التهديدات الداخلية والخارجية، والعناية بالأهداف الأساسية للحماية؛ وهي المحافظة على سرية المعلومة، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١-٣ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة> وتنطبق على جميع العاملين في <اسم الجهة>.

بنود السياسة

1- البنود العامة

1-1 يجب التعامل مع المعلومات حسب التصنيف المحدد، وبما يتوافق مع سياسة تصنيف البيانات وسياسة حماية البيانات والمعلومات الخاصة بـ<اسم الجهة> بشكل يضمن حماية سرية المعلومات وسلامتها وتوافرها.

2-1 يحظر انتهاك حقوق أي شخص، أو شركة محمية بحقوق النشر، أو براءة الاختراع، أو أي ملكية فكرية أخرى، أو قوانين أو لوائح مماثلة؛ بما في ذلك، على سبيل المثال لا الحصر، تثبيت برامج غير مصرح بها أو غير قانونية.

3-1 يجب عدم ترك المطبوعات على الطابعة المشتركة دون رقابة.

4-1 يجب حفظ وسائط التخزين الخارجية بشكل آمن وملائم، مثل التأكد من ضبط درجة الحرارة بدرجة معينة، وحفظها في مكان معزول وآمن.

5-1 يمنع استخدام كلمة المرور الخاصة بمستخدمين آخرين، بما في ذلك كلمة المرور الخاصة بمدير المستخدم أو مرؤوسيه.

6-1 يجب الالتزام بسياسة المكتب الآمن والنظيف، والتأكد من خلو سطح المكتب، وكذلك شاشة العرض من المعلومات المصنفة.

7-1 يمنع الإفصاح عن أي معلومات تخص <اسم الجهة>، بما في ذلك المعلومات المتعلقة بالأنظمة والشبكات لأي جهة أو طرف غير مصرح له سواءً كان ذلك داخلياً أو خارجياً.

8-1 يُمنع نشر معلومات تخص <اسم الجهة> عبر وسائل الإعلام، وشبكات التواصل الاجتماعي دون تصريح مسبق.

9-1 يُمنع استخدام أنظمة <اسم الجهة> وأصولها بغرض تحقيق منفعة وأعمال شخصية، أو تحقيق أي غرض لا يتعلق بنشاط وأعمال <اسم الجهة>.

10-1 يُمنع ربط الأجهزة الشخصية بالشبكات، والأنظمة الخاصة بـ<اسم الجهة> دون الحصول على تصريح مسبق، وبما يتوافق مع سياسة أمن الأجهزة المحمولة (BYOD).

11-1 يُمنع القيام بأي أنشطة تهدف إلى تجاوز أنظمة الحماية الخاصة بـ<اسم الجهة>، بما في ذلك برامج مكافحة الفيروسات، وجدار الحماية، والبرمجيات الضارة دون الحصول على تصريح مسبق، وبما يتوافق مع الإجراءات المعتمدة لدى <اسم الجهة>.

12-1 تحتفظ <الإدارة المعنية بالأمن السيبراني> بحقها في مراقبة الأنظمة والشبكات والحسابات الشخصية المتعلقة بالعمل، ومراجعتها دورياً لمراقبة الالتزام بسياسات الأمن السيبراني ومعاييره.

13-1 يُمنع استضافة أشخاص غير مصرح لهم بالدخول للأماكن الحساسة دون الحصول على تصريح مسبق.

14-1 يجب ارتداء البطاقة التعريفية في جميع مرافق <اسم الجهة>.

15-1 يجب تبليغ <الإدارة المعنية بالأمن السيبراني> في حال فقدان المعلومات أو سرقتها أو تسريبها.

2- حماية أجهزة الحاسب الآلي

1-2 يمنع استخدام وسائط التخزين الخارجية دون الحصول على تصريح مسبق من <الإدارة المعنية بالأمن السيبراني>.

2-2 يُمنع القيام بأي نشاط من شأنه التأثير على كفاءة الأنظمة والأصول وسلامتها دون الحصول على إذن مسبق من <الإدارة المعنية بالأمن السيبراني>، بما في ذلك الأنشطة التي تُمكّن المستخدم من الحصول على صلاحيات وامتيازات أعلى.

3-2 يجب تأمين الجهاز قبل مغادرة المكتب وذلك بقفل الشاشة، أو تسجيل الخروج (Sign out or Lock)، سواء كانت المغادرة لفترة قصيرة أو عند انتهاء ساعات العمل.

4-2 يُمنع ترك أي معلومات مصنفة في أماكن يسهل الوصول إليها، أو الاطلاع عليها من قبل أشخاص غير مصرح لهم.

5-2 يُمنع تثبيت أدوات خارجية على جهاز الحاسب الآلي دون الحصول على إذن مسبق من <الإدارة المعنية بتقنية المعلومات>.

6-2 يجب تبليغ <الإدارة المعنية بالأمن السيبراني> عند الاشتباه بأي نشاط قد يتسبب بضرر على أجهزة الحاسب الآلي الخاصة بـ <اسم الجهة> أو أصولها.

3- الاستخدام المقبول للإنترنت والبرمجيات

1-3 يجب إبلاغ <الإدارة المعنية بالأمن السيبراني> في حال وجود مواقع مشبوهة ينبغي حجبها؛ أو العكس.

2-3 يجب ضمان عدم انتهاك حقوق الملكية الفكرية أثناء تنزيل معلومات أو مستندات لأغراض العمل.

3-3 يُمنع استخدام البرمجيات غير المرخصة أو غيرها من الممتلكات الفكرية.

4-3 يجب استخدام متصفح آمن ومصرح به للوصول إلى الشبكة الداخلية أو شبكة الإنترنت.

5-3 يُمنع استخدام التقنيات التي تسمح بتجاوز الوسيط (Proxy) أو جدار الحماية (Firewall) للوصول إلى شبكة الإنترنت.

6-3 يُمنع تنزيل البرمجيات والأدوات أو تثبيتها على أصول <اسم الجهة> دون الحصول على تصريح مسبق من <الإدارة المعنية بتقنية المعلومات>.

7-3 يُمنع استخدام شبكة الإنترنت في غير أغراض العمل، بما في ذلك تنزيل الوسائط والملفات واستخدام برمجيات مشاركة الملفات.

8-3 يجب تبليغ <الإدارة المعنية بالأمن السيبراني> عند الاشتباه بوجود مخاطر سيبرانية، كما يجب التعامل بحذر مع الرسائل الأمنية التي قد تظهر خلال تصفح شبكة الإنترنت أو الشبكات الداخلية.

9-3 يُمنع إجراء فحص أمني لغرض اكتشاف الثغرات الأمنية، ويشمل ذلك إجراء اختبار الاختراقات، أو مراقبة شبكات <اسم الجهة> وأنظمتها، أو الشبكات والأنظمة الخاصة بالجهات الخارجية دون الحصول على تصريح مسبق من <الإدارة المعنية بالأمن السيبراني>.

10-3 يُمنع استخدام مواقع مشاركة الملفات دون الحصول على تصريح مسبق من <الإدارة المعنية بالأمن السيبراني>.

11-3 يُمنع زيارة المواقع المشبوهة بما في ذلك مواقع تعليم الاختراق.

4- الاستخدام المقبول للبريد الإلكتروني ونظام الاتصالات

1-4 يُمنع استخدام البريد الإلكتروني أو الهاتف أو الفاكس أو الفاكس الإلكتروني في غير أغراض العمل، وبما يتوافق مع سياسات الأمن السيبراني ومعاييره.

2-4 يُمنع تداول رسائل تتضمن محتوى غير لائق أو غير مقبول، بما في ذلك الرسائل المتداولة مع الأطراف الداخلية والخارجية.

3-4 يجب استخدام تقنيات التشفير عند إرسال معلومات حساسة عن طريق البريد الإلكتروني أو أنظمة الاتصالات.

4-4 يجب عدم تسجيل عنوان البريد الإلكتروني الخاص بـ<اسم الجهة> في أي موقع ليس له علاقة بالعمل.

5-4 يجب تبليغ <الإدارة المعنية بالأمن السيبراني> عند الاشتباه بوجود رسائل بريد إلكتروني تتضمن محتوى قد يتسبب بأضرار لأنظمة <اسم الجهة> أو أصولها.

6-4 تحتفظ <اسم الجهة> بحقها في كشف محتويات رسائل البريد الإلكتروني بعد الحصول على التصاريح اللازمة من صاحب الصلاحية و<الإدارة المعنية بالأمن السيبراني> وفقاً للإجراءات والتنظيمات ذات العلاقة.

7-4 يُمنع فتح رسائل البريد الإلكتروني والمرفقات المشبوهة أو غير المتوقعة حتى وإن كانت تبدو من مصادر موثوقة.

5- الاجتماعات المرئية والاتصالات القائمة على شبكة الإنترنت

1-5 يُمنع استخدام أدوات أو برمجيات غير مصرح بها لإجراء اتصالات أو عقد اجتماعات مرئية.

2-5 يُمنع إجراء اتصالات أو عقد اجتماعات مرئية لا تتعلق بالعمل دون الحصول على تصريح مسبق.

6- استخدام كلمات المرور

1-6 يجب اختيار كلمات مرور آمنة، والمحافظة على كلمات المرور الخاصة بأنظمة <اسم الجهة> وأصولها. كما يجب اختيار كلمات مرور مختلفة عن كلمات مرور الحسابات الشخصية، مثل حسابات البريد الشخصي ومواقع التواصل الاجتماعي.

1-6 يُمنع مشاركة كلمة المرور عبر أي وسيلة كانت، بما في ذلك المراسلات الإلكترونية، والاتصالات الصوتية، والكتابة الورقية. كما يجب على جميع المستخدمين عدم الكشف عن كلمة المرور لأي طرف آخر بما في ذلك زملاء العمل وموظفو <الإدارة المعنية بتقنية المعلومات>.

2-6 يجب تغيير كلمة المرور، عند تزويدك بكلمة مرور جديدة من قبل مسؤول النظام.

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> وجميع العاملين.

الالتزام بالسياسة

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

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

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