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 أمن البريد الإلكتروني

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

اختر التصنيف

الإصدار <١,٠>

الغرض

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المتعلقة بحماية البريد الإلكتروني لـ<اسم الجهة> من المخاطر السيبرانية والتهديدات الداخلية والخارجية في <اسم الجهة> ، ويتم ذلك 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

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية (شاملة أنظمة البريد الإلكتروني) الخاصة بـ<اسم الجهة> وتنطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

بنود السياسة

١- البنود العامة

١-١ يجب استخدام التقنيات اللازمة؛ لحماية سرية رسائل البريد الإلكتروني وسلامتها، وتوافرها أثناء نقلها وحفظها؛ وتحديثها بشكل مستمر.

٢-١ يجب استخدام تقنيات لحماية البريد الإلكتروني وتحليل وتصفية (Filtering) رسائل البريد الإلكتروني وحظر الرسائل المشبوهة، مثل الرسائل الاقتحامية (Spam Emails) ورسائل التصيّد الإلكتروني (Phishing Emails).

٣-١ يجب استخدام التقنيات اللازمة لحماية البيانات من التسرب من خلال البريد الإلكتروني داخل وخارج <اسم الجهة> مثل (DLP).

٤-١ يجب استخدام تقنيات لحماية خوادم البريد الإلكتروني من ن التهديدات المتقدمة المستمرة (APT Protection) ومن الفيروسات والبرمجيات الضارة غير المعروفة مسبقًا (Zero-Day Malware).

٥-١ يجب استخدام تقنيات لفحص مرفقات رسائل البريد الإلكتروني والروابط في بيئة معزولة (sand box) قبل وصولها لصندوق بريد المستخدم إن كانت مرسلة من داخل <اسم الجهة> أو خارجها.

٦-١ يجب استخدام تقنيات حديثة للتأكد من موثوقية نطاقات رسائل البريد الواردة إلى <اسم الجهة> على سبيل المثال لا الحصر: استخدام خدمة توثيق البريد الإلكتروني، ضمن البوابة الوطنية لخدمات الأمن السيبراني "حصين"، تطبيق البرتوكولات (SPF, DKIM & DMARC verification) لمنع الرسائل الانتحالية (Email Spoofing).

٧-١ يجب استخدام التقنيات اللازمة لتشفير رسائل البريد الإلكتروني التي تحتوي على معلومات مصنفة وذلك وفقًا للسياسات والإجراءات التنظيمية الخاصة بـ<اسم الجهة>.

١-٨ يجب تطبيق خاصية التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) للدخول للبريد الإلكتروني عن بعد والدخول عن طريق صفحة موقع البريد الإلكتروني (Webmail).

١-٩ يجب أرشفة رسائل البريد الإلكتروني والقيام بالنسخ الاحتياطي دوريًا وذلك وفقًا للسياسات والإجراءات التنظيمية ذات العلاقة والمعتمدة لدى <اسم الجهة>.

١-١٠ يجب تحديد ملاك الحسابات العامة والمشتركة (Generic Account) للبريد الإلكتروني ومسؤولياتهم.

١-١١ يجب تطبيق الوصول الآمن إلى رسائل البريد الإلكتروني وتقييده ليكون متاح فقط للعاملين لدى <اسم الجهة>.

١-١٢ يجب اتخاذ الإجراءات اللازمة؛ لمنع استخدام البريد الإلكتروني ل<اسم الجهة> في غير أغراض العمل المسموح بها.

١-١٣ يجب منع وصول مسؤول النظام (System Administrator) إلى معلومات ورسائل البريد الإلكتروني الخاصة بأي موظف دون الحصول على تصريح مسبق ويكون ذلك وفقًا لإجراءات محددة ومعتمدة.

١-١٤ يجب تحديد حجم ونوع مرفقات البريد الإلكتروني الصادر والوارد، وسعة صندوق البريد لكل مستخدم. وكذلك العمل على الحد من إتاحة إرسال الرسائل الجماعية لعدد كبير من المستخدمين.

١-١٥ يجب تذييل رسائل البريد الإلكتروني المرسلة إلى خارج <اسم الجهة> بإشعار إخلاء المسؤولية.

١-١٦ يجب تصنيف رسائل البريد الإلكتروني بحسب حساسية المرفقات وحساسية المعلومات المضمنة فيها وفقًا لسياسة تصنيف البيانات والمعلومات المعتمدة لدى <اسم الجهة>.

١-١٧ يجب تعطيل خدمة تحويل البريد الإلكتروني من الخادم (Open Mail Relay).

١-١٨ يجب منع استخدام البريد الالكتروني للحسابات ذات الصلاحية العالية (Privileged Accounts).

١-١٩ يجب تشفير الاتصال بين خوادم البريد الإلكتروني (Email Gateways) لمنع هجمات (Man-in-the-Middle) غير النشطة.

١-٢٠ يجب على <الإدارة المعنية بالأمن السيبراني> التأكد من وعي جميع الموظفين بالأمن السيبراني والعمل على تثقيفهم لأداء مهام وخدمات البريد الإلكتروني بشكل آمن واكتشاف رسائل التصيد الاحتيالي.

١-٢١ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات حماية البريد الإلكتروني.

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> 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 بشكل دوري.

٢- يجب على كافة 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>.