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 معيار حماية البريد الإلكتروني

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 | عُدّل بواسطة | أسباب التعديل |
|---|---|---|---|
| <أدخل رقم النسخة> | اضغط هنا لإضافة نص | <أدخل الاسم الكامل للشخص> | <أدخل وصف التعديل> |
| | | | |

# قائمة المحتويات

## الأهداف

يهدف هذا المعيار إلى توفير متطلبات الأمن السيبراني التقنية المبنية على أفضل الممارسات والمعايير لتقليل المخاطر السيبرانية الناتجة عن استخدام <اسم الجهة> للبريد الإلكتروني وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي:

- سرية معلومات البريد الإلكتروني.
- سلامة معلومات البريد الإلكتروني.
- توافر خدمة البريد الإلكتروني.

يتبع هذا المعيار المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهو متطلب تشريعي في الضابط رقم ١-٣-٣ والضابط رقم ٢-٤-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

## نطاق العمل

يغطي هذا المعيار جميع أنظمة البريد الإلكتروني الخاصة بـ<اسم الجهة>، وينطبق على جميع مستخدمي البريد الإلكتروني في <اسم الجهة>.

## المعايير

| 1 | تصفية المحتوى وتحليله (Content Filtering and Analysis) |
|---|---|
| الهدف | ضمان حماية عناوين البريد الإلكتروني من الرسائل الاقتحامية (Spam Emails) والتصيّد الإلكتروني (Phishing Emails) وروابط الإنترنت الضارة والمشبوهة (Malicious URLs) وأي نوع آخر من المحتوى الضار. |
| المخاطر المحتملة | يُمكن أن ينخدع المستخدم برسائل البريد الإلكتروني التي تحتوي على محتوى ضار ومشبوه، وقد تتعرّض <اسم الجهة> لهجمات سيبرانية في حال عدم فحص رسائل البريد الإلكتروني والتأكد من سلامتها. |
| الإجراءات المطلوبة | |
| 1-1 | فحص جميع رسائل البريد الإلكتروني الواردة والصادرة الخاصة بـ<اسم الجهة> من المحتوى الضار والمشبوه (Malicious Content).<br>All <entity name>'s inbound and outbound emails shall be scanned for malicious and suspicious content. |
| 2-1 | ترميز أو وضع علامة (Tag/Label) على جميع رسائل البريد الإلكتروني الواردة والصادرة الخاصة بـ<اسم الجهة> بالترميزات الوقائية المناسبة بما يعكس مستوى الحساسية والسريّة بناءً على مستوى تصنيف البيانات ووفقاً لنتيجة تحليل المحتوى، أو استخدام إجراء الترميز المعياري (Tagging/Labeling Standard) المطبّق في <اسم الجهة> وفقاً لسياسة أمن البريد |

اختر التصنيف

| | |
|---|---|
| | الإلكتروني المتّبعة فيها. من الأمثلة على الترميزات أو العلامات: محتوى ضار، ومُرسِل غير مصرّح له، وغير لائق، ورسالة اقتحامية، ورسالة اقتحامية مشتبهة (Suspected SPAM)، وآمن، وحسّاس، وغيرها.<br><br>All <entity name>'s inbound and outbound emails shall be tagged/labeled with appropriate protective tagging/labeling reflecting the sensitivity and confidentiality levels based on the data classification level and as per <entity name>'s Data Classification Policy and the results of content analysis. Alternatively, <entity name>'s applicable Tagging/Labeling Standard shall be used as per <entity name>'s Email Protection Policy. Some examples of tags and labels are malicious, bad sender, inappropriate, spam, suspected spam, safe, sensitive, etc. |
| 3-1 | حجب جميع رسائل البريد الإلكتروني الواردة بترميزات أو علامات وقائية تُشير إلى المحتوى غير المسموح به وفقاً لسياسة أمن البريد الإلكتروني المتّبعة في <اسم الجهة>، على سبيل المثال:<br>• حجب الرسائل الخبيثة وغير المصرّح بها والاقتحامية.<br>• حجر الرسائل الاقتحامية المشتبهة.<br>• السماح بالرسائل الآمنة.<br><br>All inbound emails shall be blocked and tagged/labeled to reflect disallowed content as per <entity name>'s Email Protection Policy. For example:<br>• **Block** malicious, blacklisted and spam emails.<br>• **Quarantine** suspected spam emails.<br>• **Allow** safe emails. |
| 4-1 | حجب جميع رسائل البريد الإلكتروني الصادرة والمصنفة، بناءً على ترميزات أو علامات وقائية تُشير إلى مستوى سريّة رسالة البريد الإلكتروني وذلك وفقاً لسياسة أمن البريد الإلكتروني المتّبعة وسياسة تصنيف البيانات في <اسم الجهة>، على سبيل المثال:<br>• حجب الرسائل الحسّاسة والسريّة.<br>• السماح بالرسائل العامة والخاصة.<br><br>All outbound classified emails shall be blocked based on the protective tags/labels reflecting the email classification level as per <entity name>'s Email Protection Policy. For example:<br>• **Block** sensitive and confidential emails.<br>• **Allow** public and restricted emails. |
| 5-1 | حجب رسائل البريد الإلكتروني الاقتحامية التي تتضمّن درجات غير مسموح بها من المخاطر الاقتحامية وفقاً لسياسة أمن البريد الإلكتروني المتّبعة في <اسم الجهة>، على سبيل المثال:<br>• حجب الرسائل شديدة المخاطر.<br>• حجر الرسائل متوسطة المخاطر.<br>• السماح بالرسائل منخفضة ومعدومة المخاطر. |

| | |
|---|---|
| Spam emails reflecting unacceptable spam risk scores shall be blocked as per <entity name>'s Email Protection Policy. For example:<br>• **Block** high risk emails.<br>• **Quarantine** medium risk emails.<br>• **Allow** low risk and no-risk emails. | |
| حجب رسائل البريد الإلكتروني الواردة التي تحتوي على روابط إنترنت ونطاقات ضارة ومشبوهة (Malicious URLs and Domains) ومحاولات تصيّد وما إلى ذلك.<br>Inbound emails containing malicious URLs, phishing attempts, malicious domains, etc. shall be blocked. | 6-1 |
| استبدال عناوين الويب النشطة (Active Web Addresses) المُدرجة في نص رسالة البريد الإلكتروني بعناوين أخرى.<br>Active Web Addresses in emails shall be replaced with other addresses. | 7-1 |
| حجب رسائل البريد الإلكتروني الواردة التي تحتوي على محتوى تفاعلي (Active Content) في نص الرسالة الإلكترونية أو حذفه منها.<br>Inbound emails containing active content shall be blocked. Alternatively, the active content in the email's body shall be removed. | 8-1 |
| حجب رسائل البريد الإلكتروني الواردة والصادرة التي تحتوي على ملفات أو محتويات حجمها أكبر من الحجم المسموح حسب سياسات <اسم الجهة>، أو تأجيلها حتى يتم التحقق من الملف من قبل الموظف المسؤول أو وفقاً للسياسة المتبعة.<br>Inbound and outbound emails with extra-large files or content shall be blocked or delayed until the files are verified by the responsible employee or as per the enforced policy. | 9-1 |
| حجب رسائل البريد الإلكتروني المُرسلة إلى قائمة غير معرّفة من عناوين البريد الإلكتروني.<br>Outbound emails to unknown distribution lists shall be blocked. | 10-1 |
| حماية المصادقة (Secure Authentication) | 2 |
| ضمان حماية استخدام البريد الإلكتروني من خارج <اسم الجهة> من الوصول غير المصرّح به من خلال صفحة موقع البريد الإلكتروني (Webmail) أو برنامج قارئ البريد الإلكتروني الخارجي (Email Client). | الهدف |
| يُعرّض الوصول غير المصرّح به إلى البريد الإلكتروني <اسم الجهة> إلى مخاطر كبيرة قد تؤدي إلى سرقة المعلومات وانتحال الشخصيات مما يتيح استخدامها في تنفيذ المزيد من الهجمات السيبرانية ضد <اسم الجهة> وبنيتها التحتية. | المخاطر المحتملة |

| | الإجراءات المطلوبة |
|---|---|
| 1-2 | تطبيق آليات التحقّق من الهوية متعدّد العناصر (Multi-Factor Authentication "MFA") على إمكانية وصول المستخدمين للبريد من خارج الشبكة خلال برنامج قارئ البريد الإلكتروني الخارجي (Email Client) وصفحة موقع البريد الإلكتروني (Webmail)، (مثل: Outlook Web Access "OWA") وفقاً للضابط رقم ٢-٤-٣-٢ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018).<br><br>Multi-Factor Authentication (MFA) shall be implemented for remote email client access and webmail access by users (e.g., Outlook Web Access "OWA") as per ECC-2-4-3-2. |
| 2-2 | بالإضافة إلى ضرورة إدخال اسم المستخدم وكلمة المرور، يجب على المستخدم استعمال آليات أخرى للتحقّق من الهوية عند الدخول من خارج الشبكة، مثل: الخصائص الحيوية (Biometrics)، أو جهاز توليد الأرقام العشوائية (Hardware Keys)، أو الرسائل القصيرة المؤقتة لتسجيل الدخول (One-Time-Password)، أو البطاقات الذكية (Smartcards) أو شهادات التشفير (Certificates)، أو غيرها.<br><br>Besides a user/password combination, users shall implement other authentication mechanisms when accessing emails from outside the network (e.g., biometrics, hardware keys, one-time passwords, smart cards, encryption certificates, etc.). |
| 3-2 | ضبط متطلبّات إعدادات كلمات المرور المعقدة للبريد الإلكتروني وفقاً لسياسة إدارة هويات الدخول والصلاحيات المتّبعة في <اسم الجهة>.<br><br>Complex email password requirements shall be configured as per <entity name>'s Identity and Access Management Policy. |
| 4-2 | تطبيق تقنيات التشفير، مثل: «أمن مستوى النقل» (Transport Layer Security) و«الشبكات الخاصة الافتراضية» (Virtual Private Networks)، لحماية آليات التحقّق من الهوية خلال إرسالها. واستخدام أحدث بروتوكولات التشفير وخوارزميات التشفير المدعومة (Cipher Suites) المُوصى بها. يُرجى الرجوع إلى معيار التشفير المعتمد في <اسم الجهة>.<br><br>Encryption methods, such as Transport Layer Security (TLS) and Virtual Private Networks (VPN), shall be implemented to protect authentication mechanisms during transmission. Recommended next generation encryption protocols and cipher suites (such as cipher suite B) shall be used. Refer to <entity name>'s Cryptography Standard. |

| 3 | حماية محتوى البريد الإلكتروني (Content Protection) |
|---|---|
| الهدف | ضمان حماية رسائل البريد الإلكتروني التي تحتوي على مرفقات من الفيروسات والبرمجيات الضارة والتهديدات المتقدّمة المستمرة والهجمات غير المعروفة مسبقاً وأي نوع آخر من المرفقات الخبيثة. |
| المخاطر المحتملة | يُمكن أن ينخدع المستخدم برسائل البريد الإلكتروني التي تحتوي على مرفقات خبيثة حيث قد تتعرض <اسم الجهة> لاختراق بياناتها أو الوصول إليها بشكل غير مصرّح به أو كشفها في حال عدم فحص مرفقات البريد الإلكتروني. |
| الإجراءات المطلوبة | |
| 1-3 | تطبيق وتفعيل تصنيفين لمرفقات البريد الإلكتروني: التصنيف الأول وفقاً لنوع الملف، والتصنيف الثاني وفقاً لمحتوى الملف.<br>Two types of email attachment classification shall be configured; based on file type and based on file content. |
| 2-3 | ترميز المرفقات حسب أنواع المرفقات وصيغتها. على سبيل المثال:<br>• **اللائحة السوداء:** جميع أنواع نسخ البرمجيات القابلة للتنفيذ من ويندوز ( Windows PE) وأوامر ماكرو أوفيس (Office Macros) والبرمجيات أو الأوامر النصية (Scripts)، وغيره.<br>• **اللائحة الرمادية:** الأرشيفات متعدّدة المستويات (Multi-Layer Archives) وملفات حماية كلمة المرور وملفات التشفير والملفات التي يزيد حجمها عن الحد الأقصى، وغيرها من الملفات ضمن قائمة الحجر (Quarantine-list)<br>• **اللائحة البيضاء:** ملفات برامج أوفيس القياسية (مثل: docx وpptx وxlsx) وملفات pdf وtxt، والملفات الأرشيفية، وغيرها.<br>• **لائحة المرفقات غير المعروفة:** أنواع وصيغ الملفات غير المعروفة والتي يتعذّر التحقّق منها.<br>Attachments based on file types and formats shall be tagged. For example:<br>• **Blacklist:** All forms of Windows PE, Office macros, scripts, etc.<br>• **Graylist (quarantine-list):** Multi-layer archives, password protection files, encryption files, files exceeding the maximum size, etc.<br>• **Whitelist:** Standard Microsoft Office extensions (docx, pptx, xlsx, etc.), pdf, txt, archives, etc.<br>• **Unknown:** Unknown file type/format, or unable to detect. |
| 3-3 | ترميز جميع المرفقات بعد فحصها من البرمجيات الضارة بإدراج نتائج الفحص، على سبيل المثال:<br>• **ضارة:** تحتوي على فيروس أو برنامج ضار أو تهديد متقدّم مستمر أو غيره.<br>• **آمنة:** تحتوي على ملف مرفق آمن. |

اختر التصنيف

| | |
|---|---|
| | • **غير معروفة:** أي تعذّر فحصها.<br><br>All malware-scanned attachments shall be tagged with scan results. For example:<br>• **Malicious:** Contains virus, malware, APT, etc.<br>• **Safe:** Malware-free attachment.<br>• **Unknown:** Unable to scan. |
| 4-3 | تحديد أنواع الملفات باستخدام محتواها مثل ترويسة وتذييل الملف (Footer and Header) وليس من خلال صيغها.<br><br>File types shall be determined using file content (file header and footer), not extensions. |
| 5-3 | فحص جميع المرفقات المسموحة والتي تمت تصفيتها للتأكد من خلوها من الملفات الضارة، مثل: الفيروسات والبرمجيات الضارة وأي نوع آخر من الملفات المشبوهة.<br><br>All whitelisted and filtered attachments shall be scanned for malicious files including viruses, malware and any other form of suspicious files. |
| 6-3 | فحص جميع أنظمة وخوادم البريد للتحقّق من عدم وجود أي برمجيات ضارة أو مشبوهة في المكونات التقنية للبريد الإلكتروني وبوابة البريد (Mail Gateway) وخاصية ترحيل البريد (Mail Relay) أو خادم البريد (Mail Server) قبل أن تصل إلى برنامج قارئ البريد (Email Client).<br><br>Malware scanning shall be performed on Mail Gateway, Mail Relay or Mail Server before it reaches the Email Client. |
| 7-3 | إجراء فحص للتحقّق من عدم وجود أي برمجيات ضارة أو مشبوهة عبر برامج قراءة البريد (Email Clients) باستخدام حل يُقدّمه مورّد أو مزوّد مختلف عن الموجود في البند 6-3 مثل إضافة أدوات للحماية من الفيروسات إلى برنامج قارئ البريد.<br><br>Malware scanning shall be performed on email clients using a solution from a vendor or provider different from the one mentioned in clause 3-6 (e.g., AV plug-ins added to outlook client) |
| 8-3 | فحص جميع المرفقات المسموحة والتي تمت تصفيتها عبر إجراء تحليل ديناميكي للمرفقات باستخدام تقنية الحماية المعزولة (Sandbox) للتحقّق من التهديدات المتقدّمة المستمرة (APT) والبرمجيات الضارة غير المعروفة مسبقاً.<br><br>Allowed attachments, on which dynamic analysis was performed in sandbox, shall be scanned to detect Advanced Persistent Threats (APTs) and zero-day malware. |
| 9-3 | حجب (أي عدم السماح لها بالمرور إلى بريد المستخدم) أو تجريد جميع رسائل البريد الإلكتروني التي تحتوي على ملفات مرفقة ضارة أو مصنفة ضمن اللائحة السوداء وفقاً لسياسة أمن البريد الإلكتروني المتّبعة في <اسم الجهة> ثمّ إضافة عنوان المرسل والنطاق إلى اللائحة السوداء. |

اختر التصنيف

| | |
|---|---|
| | All emails with blacklisted or malicious attachments shall be blocked/stripped as per <entity name>'s Email Protection Policy. Sender's email address and domain shall be added to the blacklist. |
| 10-3 | حجر (أي إيقاف وصولها إلى بريد المستخدم إلى حين التأكد من سلامة محتواها) جميع رسائل البريد الإلكتروني التي تتضمّن ملفات ضمن اللائحة الرمادية إذا كانت آمنة.<br>All emails with graylisted attachments shall be quarantined if they are malware-free. |
| 11-3 | حجر جميع رسائل البريد الإلكتروني التي تتضمّن ملفات مرفقة غير معروفة.<br>All emails with **Unknown** attachments shall be quarantined. |
| 12-3 | قبول جميع رسائل البريد الإلكتروني التي تتضمّن ملفات مرفقة آمنة ومسموحة.<br>All emails with whitelisted attachments shall be allowed if they are malware-free. |
| 4 | التحقّق من مرسل البريد الإلكتروني (Email Sender Verification) |
| الهدف | ضمان الحفاظ على سريّة بيانات البريد الإلكتروني والتأكّد من سلامتها وموثوقيتها لحمايتها من الوصول غير المصرّح به والكشف عن المعلومات الحسّاسة. |
| المخاطر المحتملة | تحمي خاصية التأكّد من سلامة وموثوقية رسائل البريد الإلكتروني <اسم الجهة> من عمليات تزوير البريد الإلكتروني والرسائل الإلكترونية الضارة والكشف عن المعلومات المهمّة والحسّاسة والوصول غير المصرّح به إلى الرسائل الإلكترونية الخاصة بالمستخدم. |
| الإجراءات المطلوبة | |
| 1-4 | التحقّق من المُرسِل باختبار قاعدتين من بيانات سمعة المُرسِل (Sender Reputation) على الأقل.<br>Sender shall be verified against at least two sender reputation databases. |
| 2-4 | التحقّق من عنوان المُرسِل مقابل قوائم الرسائل الاقتحامية (Email SPAM lists) المتواجدة على الإنترنت والتي تحدث يومياً.<br>Sender email address shall be verified against sender spam lists that are available on the Internet and are updated daily. |
| 3-4 | التحقّق من بروتوكول الإنترنت (Internet Protocol "IP") الخاص بخادم بريد المُرسِل واسم النطاق بمقارنته مع القائمة اللحظية لعناوين الإنترنت العشوائية ( Real-time Blackhole Lists). |

| | |
|---|---|
| | Sender email server **IP** and **domain name** shall be verified against Real-time Blackhole Lists (RBL). |
| 5 | التحقّق من سلسلة الثقة المتعلقة بالبريد الإلكتروني<br>(Email Chain of Trust Verification) |
| الهدف | ضمان الحفاظ على سريّة بيانات البريد الإلكتروني والتأكّد من سلامتها وموثوقيتها لحمايتها من الوصول غير المصرّح به والكشف عن المعلومات الحسّاسة. |
| المخاطر المحتملة | قد يؤدي عدم التأكد من سلامة وموثوقية رسائل البريد الإلكتروني إلى عمليات تزوير البريد الإلكتروني والرسائل الإلكترونية الخبيثة والكشف عن المعلومات المهمة والحسّاسة والوصول غير المصرّح به إلى الرسائل الإلكترونية الخاصة بالمستخدمين. |
| الإجراءات المطلوبة | |
| 1-5 | إنشاء وتسجيل إطار سياسة المُرسِل (Sender Policy Framework "SPF") والبريد المُعرَّف بمفاتيح النطاق (Domain Key Identified Mail "DKIM") ومصادقة الرسائل والإبلاغ عنها ومطابقتها استناداً إلى النطاق (Domain-based Message Authentication, Reporting and Conformance "DMARC").<br>Sender Policy Framework (SPF), Domain Key Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC) shall be created and registered. |
| 2-5 | التحقّق من المُرسِل وفق نظام مصادقة هوية مُرسِل الرسائل (SenderID) وسجلات إطار سياسة المُرسِل (SPF) واتخاذ الإجراء المناسب وفقاً لسياسة أمن البريد الإلكتروني المتّبعة في <اسم الجهة>.<br>• رفض الفشل الكامل (SPF Strict -Fail) في إطار سياسة المُرسِل.<br>• حجر الفشل الجزئي (SPF Relaxed -Fail) في إطار سياسة المُرسِل.<br>Senders shall be verified according to their SenderID/SPF records and actions shall be taken as per <entity name>'s Email Protection Policy.<br>• **Reject** SPF hard-fail<br>• **Quarantine** SPF soft-fail |
| 3-5 | التحقّق من المُرسِلين وفق البريد المُعرَّف بمفاتيح النطاق (DKIM) التي يستخدمونها.<br>• رفض الفشل في البريد المُعرَّف بمفاتيح النطاق.<br>Senders shall be verified according to their DKIM.<br>• **Reject** DKIM fail. |
| 4-5 | ضبط إطار سياسة المُرسِل (SPF) على السجلات الخارجية المقابلة لنظام أسماء النطاقات (External DNS Records) لكل أسماء النطاقات التي تملكها <اسم الجهة> للسماح فقط بسجلات تبادل البريد (Mail Exchange Records) في الخوادم التي صرّحت لها <اسم الجهة> بإرسال الرسائل الإلكترونية نيابةً عنها. |

اختر التصنيف

| | |
|---|---|
| | SPF on external records facing DNS shall be configured for each and every domain name owned by <entity name> to allow only Mail Exchange Records (MX Records) of servers authorized by <entity name> to send emails on its behalf. |
| 5-5 | ضبط سجلات البريد المُعرَّف بمفاتيح النطاق (DKIM) لتوقيع محتوى رسائل البريد الإلكتروني (Email Digital Signing) الخاصة بـ<اسم الجهة> وذلك بتحديد مفاتيح عامة تشفيرية للتواقيع (Public Key Cryptography).<br><br>DKIM records shall be configured to sign the content of <entity name>'s emails by specifying cryptographic public keys for signing. |
| 6-5 | ضبط «مصادقة الرسائل والإبلاغ عنها ومطابقتها استناداً إلى النطاق» (DMARC) لأتمتة تطبيق الإجراءات المناسبة بشأن الأخطاء المرصودة في نظام مصادقة هوية مُرسِل الرسائل وسجلات إطار سياسة المُرسِل والبريد المُعرّف بمفاتيح النطاق وفقاً لسياسة حماية البريد الإلكتروني المتبعة في <اسم الجهة>. على سبيل المثال:<br>• **رفض/حجر** الفشل الجزئي (Relaxed Fail) في البريد المُعرَّف بمفاتيح النطاق (DKIM) وسجلات إطار سياسة المُرسِل (SPF).<br>ملاحظة: الفشل الجزئي (Relaxed Fail) يسمح بمرور الرسائل الواردة من النطاقات الفرعية، والفشل الكامل (Strict Fail) يمنع ذلك.<br><br>Domain-based Message Authentication, Reporting and Conformance (DMARC) shall be configured to automate the actions taken on SenderID/SPF fails and DKIM fails. For example:<br>• **Reject/Quarantine** Relaxed Fail in DKIM and SPF.<br>Note: Relaxed Fail allows emails received from sub-domains and Strict Fail blocks them. |
| 6 | حماية أنظمة البريد الإلكتروني (Email Systems Security) |
| الهدف | ضمان حماية وأمن البنية التحتية الأساسية لخدمة البريد الإلكتروني بما في ذلك خوادم البريد وبواباته وقواعد بياناته وحلوله الأمنية. |
| المخاطر المحتملة | من الممكن أن يؤدي عدم اتخاذ أي إجراء لحماية البنية التحتية لخدمة البريد الإلكتروني في <اسم الجهة> إلى استغلال المهاجمين لنقاط الضعف الكامنة في أنظمة البريد الإلكتروني واستغلال ثغراتها للوصول غير المصرّح به إلى شبكة <اسم الجهة> وبياناتها. |
| الإجراءات المطلوبة | |
| 1-6 | إجراء اختبارات أمنية دورية (مثل: فحص الثغرات الأمنية وتنفيذ عمليات اختبار الاختراق) وفقاً للسياسات والإجراءات ذات العلاقة في <اسم الجهة>.<br><br>Regular security testing (such as vulnerability assessments and penetration testing) shall be performed as per <entity name>'s relevant policies and procedures. |

| | |
|---|---|
| 2-6 | مراجعة وتطبيق حزم التحديثات والإصلاحات دورياً على أنظمة البريد الإلكتروني وفقاً لسياسة إدارة التحديثات والإصلاحات المتّبعة في <اسم الجهة>، وضمان تحديث جميع الأنظمة.<br>Email systems shall be regularly patched and updated as per <entity name>'s Patch Management Policy. Additionally, it shall be ensured that all systems are up-to-date. |
| 3-6 | حذف أو إلغاء تفعيل التطبيقات والخدمات غير الضرورية أو غير اللازمة من أنظمة البريد الإلكتروني، مثل: خدمات الطباعة وبروتوكول الاتصال عن بعد غير الآمن (Telnet) ، وغيرها.<br>Unnecessary/unrequired applications and services on email systems, such as printing services, telnet, etc. shall be removed/disabled. |
| 4-6 | ضبط إعدادات وتحصين (Secure Configuration and Hardening) أنظمة البريد الإلكتروني على مستوى التطبيقات وقاعدة البيانات والتشغيل كل ثلاثة أشهر. يُرجى الرجوع إلى معيار أمن الخادم ومعيار أمن قاعدة البيانات المعتمدين في <اسم الجهة>.<br>Secure Configuration and Hardening shall be applied every three months on applications, databases, and operating systems. Refer to <entity name>'s Server Security Standard and Database Security Standard. |
| 5-6 | تقييد الوصول (Restrict Access) إلى أنظمة البريد الإلكتروني ليكون مسموح به فقط لمديري أنظمة البريد الإلكتروني (Mail System Administrators).<br>Access to email systems shall be restricted to email system administrators only. |
| 6-6 | حذف أو إلغاء تفعيل الحسابات الافتراضية أو غير التفاعلية أو غير اللازمة.<br>Default/non-interactive/unneeded accounts shall be removed/disabled. |
| 7-6 | إلزام مديري الأنظمة ومُشغّلي أنظمة البريد الإلكتروني باستخدام آلية التحقّق من الهوية متعدّد العناصر للوصول إلى أنظمة البريد الإلكتروني.<br>Email systems administrators and operators shall be obliged to use multi-factor authentication to access email systems. |
| 8-6 | استخدام مبدأ الحماية الذي يمنح مديري ومُشغّلي أنظمة البريد الإلكتروني ( Email System Administrators and Operators) الحد الأدنى من صلاحيات الوصول (Least-Privilege Principle) إلى مختلف أنواع أنظمة البريد الإلكتروني.<br>The least-privilege principle shall be used to provide access for email system administrators and operators to email systems. |

| | |
|---|---|
| 9-6 | تقييد الوصول الشبكي إلى أنظمة إدارة البريد الإلكتروني على المنطقة الشبكية التي تتواجد فيها والمنطقة الشبكية الخاصة بالإدارة (Management Zone).<br>Network access to email management systems shall be restricted to Email System Zone and Management Zone. |
| 10-6 | حذف أو إلغاء تفعيل خصائص تطبيق البريد الإلكتروني وملفات الإعدادات غير الضرورية أو غير اللازمة.<br>Unnecessary/unrequired email application features and configuration files shall be removed/disabled. |
| 11-6 | حجب إمكانية الوصول (Restrict Access) إلى مجلدات الشبكة ( Network File Shares) والملفات غير الضرورية أو غير اللازمة.<br>Access to unnecessary/unrequired network and file directories shall be blocked. |
| 12-6 | استخدام ضوابط الأجهزة الطرفية (Peripheral Device Controls) وحجب الوصول إلى وسائل التخزين القابلة للإزالة مثل الأقراص المتحركة (CD) والأقراص المدمجة (DVD) وذاكرة التخزين (USB).<br>Peripheral device controls shall be used and access to removable media, such as CDs, DVDs, and USBs, shall be blocked. |
| 13-6 | تثبيت برامج أنظمة البريد الإلكتروني على خوادم استضافة مخصصة لها.<br>Email systems software shall be installed on dedicated hosts. |
| 14-6 | ضبط رسائل خدمة برتوكولات نقل البريد (مثل: بروتوكول إرسال البريد البسيط "SMTP"، وبروتوكول مكتب البريد "POP"، وبروتوكول الوصول إلى رسائل الإنترنت "IMAP"، وغيرها) لمنع الكشف عن معلومات إصدار البرنامج أو نظام التشغيل (Exchange Version).<br>The service banners of mail transport protocols (such as SMTP, POP, IMAP, etc.) shall be configured to prevent software/protocol version disclosure (Exchange version). |
| 15-6 | تفعيل أوامر البريد غير الخطرة فقط وذلك لتفادي الأوامر الخطرة مثل (VRFY وEXPN).<br>Safe email commands shall only be enabled to avoid risky email commands (such as VRFY and EXPN). |
| 16-6 | تفعيل سجلات الأحداث (Event Logging) في أنظمة البريد الإلكتروني وسجل التدقيق (Audit Log) الواجب إرسالهما إلى نظام مركزي لإدارة سجلات الأحداث وفقاً لسياسة ومعيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني في <اسم الجهة>. |

| | |
|---|---|
| Email systems event logging and audit log to be forwarded to a centralized event logging system shall be configured as per <entity name>'s Cybersecurity Event Logs and Monitoring Management Policy and Standard. | |
| إنشاء البنية التحتية لخدمة البريد الإلكتروني باستخدام مبدأ المعمارية متعددة المستويات (Multi-Tier Architecture) المحمية باستخدام طبقتين مختلفتين من جدار الحماية (Firewalls). وتحديداً، إدراج بوابة أمن البريد الإلكتروني (Mail Gateway) في منطقة الإنترنت المحايدة (DMZ)، وخوادم تطبيقات البريد الإلكتروني في منطقة الإنتاج (Production Zone)، وخوادم قواعد بيانات البريد الإلكتروني في المنطقة الموثوقة (Trusted Zone) أو منطقة قاعدة البيانات (Database Zone).<br><br>A Multi-Tier architecture protected by a dual layer of firewalls shall be applied when creating the email service infrastructure, specifically, **Mail Gateway** in the Internet DMZ, **Email Application Servers** in the Production Zone, and **Email Database Servers** in the Trusted or Database zone. | 17-6 |
| حماية صفحة موقع البريد الإلكتروني خلف جدار حماية تطبيق الويب (Web Application Firewall "WAF").<br><br>The webmail page shall be protected behind a web application firewall (WAF). | 18-6 |
| تعطيل خاصية الترحيل المفتوح (Open Mail Relay).<br><br>Open Mail Relay feature shall be disabled. | 19-6 |
| ضبط تشفير نقل البريد الإلكتروني باستخدام تقنيات التشفير، مثل: «أمن طبقة النقل» (Transport Layer Security) و«الشبكات الخاصة الافتراضية» (Virtual Private Networks) لحماية رسائل البريد الإلكتروني خلال إرسال الرسائل. واستخدام أحدث بروتوكولات التشفير وخوارزميات التشفير المدعومة (Cipher Suites) المُوصى بها (مثل التشفير بمجموعة Suite B). يُرجى الرجوع إلى معيار التشفير المعتمد في <اسم الجهة>.<br><br>Email transport encryption shall be configured using encryption technologies, such as Transport Layer Security (TLS) and Virtual Private Networks (VPN), to protect emails during transmission. Recommended next generation encryption protocols and cipher suites (such as cipher suite B) should be used. Refer to <entity name>'s Cryptography Standard. | 20-6 |
| ضبط مجموعات مواصفات الارتداد لبيانات البريد (Mail Bounce Profiles)، على سبيل المثال:<br>• الارتداد القوي لرسائل البريد الإلكتروني المرسلة إلى عناوين بريد غير موجودة أو منتهية الصلاحية أو غير مفعّلة. | 21-6 |

| | |
|---|---|
| | Mail bounce profiles shall be configured, for example:<br>• **Hard Bounce** for emails sent to non-existing users or expired/disabled email addresses. |
| 7 | برنامج قارئ البريد الإلكتروني (Email Client Security) |
| الهدف | ضمان حماية استخدام البريد الإلكتروني من خلال صفحة موقع البريد الإلكتروني (Webmail) أو برنامج قارئ البريد الإلكتروني (Email Client). |
| المخاطر المحتملة | من الممكن أن يؤدي عدم اتخاذ أي إجراء لحماية برنامج قارئ البريد الإلكتروني إلى مخاطر كبيرة قد تؤدي إلى سرقة المعلومات وانتحال الشخصيات مما يتيح استخدامها في تنفيذ المزيد من الهجمات الضارة ضد موظفي <اسم الجهة> وبنيتها التحتية. |
| الإجراءات المطلوبة | |
| 1-7 | استخدام برنامج قارئ بريد إلكتروني مرخص وموثوق.<br>Only fully supported and up-to-date email clients shall be used. |
| 2-7 | منع تشغيل صفحة موقع البريد الإلكتروني على المتصفحات غير المرخصة.<br>Running the webmail on unsupported browsers shall be prohibited. |
| 3-7 | تعطيل التطبيقات الإضافية أو المكونات غير الضرورية أو غير المسموح بها لبرنامج قارئ البريد الإلكتروني.<br>Unnecessary or not whitelisted email client plug-ins or add-ons applications shall be disabled. |
| 4-7 | منع تشغيل لغات البرمجة النصية في برنامج قارئ البريد الإلكتروني.<br>Running scripting languages in email clients shall be prohibited. |
| 5-7 | ضبط تكامل برنامج قارئ البريد الإلكتروني مع أنظمة حماية الأجهزة كمضاد الفيروسات والبرمجيات الضارة.<br>Email clients shall be integrated with endpoint security products (e.g., AV and Malware). |
| 8 | النسخ الاحتياطية والأرشفة (Backup and Archival) |
| الهدف | ضمان سلامة بيانات البريد الإلكتروني وتوافرها وقابلية استعادتها وحمايتها من فقدانها أو تخريبها. |
| المخاطر المحتملة | في حال حذف بيانات البريد الإلكتروني والرسائل الإلكترونية أو العبث بها أو فقدانها بالخطأ أو تخريبها أو تعرّضها لهجوم إلكتروني، لن تتمكّن <اسم الجهة> من استرداد بيانات بريدها الإلكتروني وسجل اتصالاتها مما يؤثّر على أنشطة أعمالها الاعتيادية. |
| الإجراءات المطلوبة | |

اختر التصنيف

| | |
|---|---|
| إجراء عمليات نسخ احتياطية دورية كاملة لخوادم وقواعد بيانات البريد الإلكتروني وفقاً لسياسة إدارة النسخ الاحتياطية، ويشمل ذلك النسخ الاحتياطية لأنظمة تشغيل الخوادم وإعدادات تطبيق البريد وقاعدة البيانات بالإضافة إلى مجمل قواعد البيانات وصناديق البريد، وإضافة ترتيب تسلسلي للنسخ الاحتياطية لنظام البريد الإلكتروني ومحتويات البريد الخاصة بـ<اسم الجهة> وتسجيل وقتها وتاريخها وجدولتها.<br><br>Full backups for the email systems and underlying infrastructure shall be performed as per <entity name>'s Backup and Recovery Management Policy. The backups must include at a minimum email servers and email databases, including servers' operating system backup, email application configuration backup, database configuration backup, databases and mailboxes. Additionally, <entity name>'s email system and mailbox backups shall be serialized, time-dated and indexed. | 1-8 |
| إجراء عملية نسخ احتياطي إضافية يومياً أو وفقاً لسياسة إدارة النسخ الاحتياطية لمحتويات بريد المستخدمين.<br><br>Incremental backup for user mailboxes shall be performed daily or as per <entity name>'s Backup and Recovery Management Policy. | 2-8 |
| تشفير النسخ الاحتياطية لنظام البريد الإلكتروني ومحتويات البريد وفقاً لسياسة التشفير المعتمدة في <اسم الجهة>.<br><br><Entity name>'s email system and mailbox backups shall be encrypted. | 3-8 |
| تخزين النسخ الاحتياطية لنظام البريد الإلكتروني ومحتويات البريد الخاصة بـ<اسم الجهة> في موقعين محميّين منفصلين على الأقل وفقاً لسياسة إدارة النسخ الاحتياطية المعتمدة في <اسم الجهة>.<br><br><Entity name>'s email system and mailbox backups shall be stored in, at least, two geographically distinct protected off-sites. | 4-8 |
| تطبيق إجراءات توثيق وسلامة (Integrity Verification) النسخ الاحتياطية لضمان نسخ بيانات البريد الإلكتروني أو أرشفتها بطريقة صحيحة.<br><br>Backup and integrity verification mechanisms shall be employed to ensure that email data is being correctly backed up or archived. | 5-8 |
| تجربة استعادة جميع أنواع النسخ الاحتياطية دورياً لضمان سلامة عملية النسخ الاحتياطي وفقاً لسياسة إدارة النسخ الاحتياطية.<br><br>Backup recovery shall be regularly tested to verify the safety of the backup process as per <entity name>'s Backup and Recovery Management Policy. | 6-8 |

## الأدوار والمسؤوليات

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

2- **مراجعة المعيار وتحديثه:** <الإدارة المعنية بالأمن السيبراني>.

3- **تنفيذ المعيار وتطبيقه:** <الإدارة المعنية بتقنية المعلومات>.