ضوابط وتعليمات استخدام البريد الإلكتروني في المؤسسات الحكومية

جمهورية العراق

المركز الوطني للأمن السيبراني

2026

TLP:White

ضوابط وتعليمات إستخدام البريد الإلكتروني في المؤسسات الحكومية

تمهيد

إستناداً إلى وثيقة السياسات والمعايير لأمن المعلومات ومشاركة البيانات المقرة بموجب قرار مجلس الوزراء وبناءاً على مقتضيات تنظيم وحماية أمن البيانات الحكومية تنسب على المؤسسات الحكومية كافة مراعاة الآتي:

أولاً: إنشاء حساب البريد الإلكتروني:

1.1 متطلبات إنشاء الحساب

1.1.1 يمنح الموظف حساب بريد إلكتروني لإتمام المهام الموكلة اليه وحسب متطلبات العمل وفق رؤية المؤسسة، ويجب أن يكون محدد بشكل فريد لكل مستخدم ويقع ضمن امتداد (gov.iq).

1.1.2 عند إنشاء بريد إلكتروني جديد للمستخدم، يجب على المستخدم تغيير كلمة المرور الأولية الخاصة به في تسجيل الدخول التالي، بحيث أن النظام يفرض على المستخدمين تغيير كلمات المرور الأولية الخاصة بهم.

1.1.3 يجب أن تكون كلمة مرور البريد الإلكتروني الخاصة بالمستخدم تتوافق مع سياسة كلمة المرور الصادرة عن (جهة العمل).

1.1.4 يمنح كل مستخدم حساب بريد إلكتروني رسمي واحد مرتبط بهويته الوظيفية ويحظر إنشاء حسابات متعددة لنفس المستخدم إلا لأغراض تشغيلية محددة تقتضيها طبيعة العمل وبعد الحصول على موافقة مسبقة من الجهة المختصة مع توثيق المبررات وتحديد الصلاحيات.

1.2 إدارة صندوق البريد

1.2.1 يجب التحكم في حجم صندوق البريد من خلال تحديد سعة الحصة المخصصة، وكل مستخدم مسؤول إذا تجاوز السعة المحدودة، لذا يجب على المستخدم أرشفة الرسائل المهمة بشكل دوري وحذفها من البريد الوارد.

1.3 تسليم الحساب والتوعية

1.3.1 تسلم المؤسسة البريد الالكتروني للموظف ويكون في ذمته واعتماد اليات المؤسسة في الاستلام والتسليم ولا يجوز سحب البريد الالكتروني من الموظف دون علمه.

1.3.2 إقامة دورات توعية حول استخدام البريد الالكتروني والمخاطر التي قد يتعرض لها الموظف قبل تسليمه حساب البريد الالكتروني.

ثانيا: استخدام البريد الإلكتروني:

على جميع المستخدمين التقيد عند استخدام البريد الإلكتروني الخاص بـ (جهة العمل بما يلي:

2.1 الاستخدام العام والالتزام

2.1.1 يجب أن يكون استخدام البريد الإلكتروني متوافقاً مع سياسات (جهة العمل) وإجراءاتها ومع القوانين المعمول بها والممارسات السليمة والامتثال للقوانين المعمول بها.

2.1.2 يجب استخدام حسابات البريد الإلكتروني لـ (جهة العمل) لأعمال تتعلق بـ (جهة العمل)، حيث يستخدم لمساعدة الموظفين في تأدية وظائفهم.

2.1.3 لا ينبغي استخدام البريد الإلكتروني المخصص للموظف لأغراض شخصية.

2.2 حماية البيانات والمحتوى

2.2.1 يجب تأمين جميع بيانات (جهة العمل) الواردة في رسالة البريد الإلكتروني أو المرفق طبقاً لسياسة حماية البيانات.

2.2.2 يجب توخي الحذر عند إرفاق المستندات أو الملفات بالبريد الإلكتروني، فقد تكون هذه المرفقات تابعة للآخرين، وإعادة توجيه هذه البيانات إلى مستلم آخر دون الحصول على إذن مسبق من المرسل قد يعتبر انتهاكاً لحقوق الطبع والنشر.

2.3 أمن البريد الإلكتروني

2.3.1 يجب على جميع المستخدمين توخي الحذر عند فتح رسائل البريد الإلكتروني والمرفقات من مصادر غير معروفة.

2.3.2 يجب على من يتعرف على أو يلاحظ وجود مشكلة أمنية فعلية أو مشتبه بها، الاتصال على الفور بقسم أمن المعلومات في (جهة العمل) والإبلاغ بشكل فوري.

2.4 جودة المحتوى والمسؤولية

2.4.1 يجب على جميع المستخدمين ضمان أن يكون محتوى البريد الإلكتروني دقيقاً وواقعياً وموضوعياً، حيث يجب تجنب الآراء الشخصية حول الأفراد أو المؤسسات الأخرى.

2.4.2 يجب انتقاء الألفاظ اللائقة وعدم كتابة أي لفظ مسيء أو مهين للآخر.

2.4.3 على المستخدم أخذ العلم والدراية أنه المسؤول الوحيد عما تحتويه الرسائل المرسلة من خلال حساب بريده الإلكتروني.

2.5 الملكية والمراجعة

2.5.1 يستخدم البريد الإلكتروني الرسمي لأغراض مهنية فقط ويعد أحد أصول المؤسسة ويحق للمؤسسة حق الاطلاع عليه وهي المسؤولة عن أمن البيانات فيه.

2.5.2 يمكن مراجعة الرسائل الإلكترونية للموظف إذا رأت (جهة العمل) ذلك ضرورياً وبحضور الموظف إذا وجد دليل على أن المستخدم لا يلتزم بالتوجيهات المنصوص عليها في هذه الضوابط، كما وتحتفظ (جهة العمل) بالحق في اتخاذ إجراءات قانونية وفق اللوائح المعمول بها ويجب أن يدرك المستخدم ان الرسائل قد تخضع للتدقيق والرقابة.

2.6 إدارة الحسابات والوصول

2.6.1 يجب على المستخدمين عدم الإفصاح عن كلمات المرور الخاصة بحساباتهم أو السماح لأي شخص آخر باستخدام حساباتهم، كما يجب عدم استخدام حساب مستخدم آخر.

2.6.2 يجب على المستخدمين ضمان إرسال رسائل البريد الإلكتروني إلى المستخدمين الذين يحتاجون إلى معرفة الأمر فقط.

2.7 إدارة الحساب عند تغيير الحالة الوظيفية

2.7.1 تتم إدارة حسابات البريد الإلكتروني للمستخدمين وفقاً لحالتهم الوظيفية وبما يضمن حماية أصول المعلومات واستمرارية العمل وذلك على النحو الآتي:

- في حال التحقيق الإداري أو القانوني: يتم تقييد أو تعليق الوصول إلى الحساب بشكل مؤقت وفقاً لتقييم المخاطر وطبيعة الحالة لحين صدور القرار النهائي.

- في حال الفصل أو العزل: يتم تعطيل الحساب فوراً وسحب صلاحيات الوصول مع حفظ وأرشفة محتوى البريد الإلكتروني باعتباره من أصول المؤسسة.
- في حال الاستقالة: يستمر الوصول بشكل منظم خلال فترة الإشعار بما يضمن نقل المعرفة وعدم الإضرار بسير العمل على أن يتم تعطيل الحساب بعد انتهاء الخدمة.
- في حال النقل أو تغيير جهة العمل أو المسمى الوظيفي: يتم تعديل الصلاحيات وإدارة الوصول بما يتناسب مع الدور الجديد دون تعطيل الحساب.
- في جميع الأحوال تلتزم الجهة بحماية البيانات وعدم فقدانها، وضمان استخدامها للأغراض المؤسسية فقط.

2.8 متطلبات إضافية

2.8.1 ارفاق كل رسالة بتوقيع نصي في النهاية يحمل الاسم والوظيفة ورقم الهاتف والقسم التابع له واسم (جهة العمل).

2.8.2 على الموظف والمؤسسة الحفاظ على محتوى البريد واعتباره وثيقة رسمية.

2.8.3 في حال إرسال معلومات إلى مستلم غير مقصود يلتزم المستخدم بالإبلاغ الفوري للجهة المختصة وفق الإجراءات المعتمدة وعدم اتخاذ أي إجراء فردي قد يؤثر على معالجة الواقعة أو إجراءاتها النظامية.

TLP:White

ثالثا: محظورات إستخدام البريد الإلكتروني:

تعد الممارسات التالية محظورة عند استخدام البريد الإلكتروني الخاص بـ (جهة العمل):

3.1 إساءة استخدام البريد

3.11 استخدام نظام البريد الإلكتروني لـ (جهة العمل) لإنشاء أو توزيع أي رسائل مدمرة أو هجومية كما يجب على الموظفين الذين يتلقون أي رسائل بريد إلكتروني بهذا المحتوى من أي موظف بـ (جهة العمل) ابلاغ الأمر إلى المسؤول على الفور.

3.12 استخدام البريد الإلكتروني الرسمي لتصفية خلافات شخصية أو إدارية أو لإثارة نزاعات داخلية.

3.13 استخدام البريد الإلكتروني الرسمي لتحقيق مصالح شخصية أو تجارية أو سياسية أو دعم أي جهة خارج نطاق العمل الرسمي.

3.2 إساءة استخدام النظام

3.2.1 استخدام حساب البريد الإلكتروني لـ (جهة العمل) لتسجيل الدخول في أي من مواقع شبكات التواصل الاجتماعي ما لم يكن ذلك لأغراض العمل، كما يجب الحصول على موافقة من الإدارة العليا أو من تخوله بذلك.

3.2.2 ارسال رسائل بريد إلكتروني غير مرغوب فيها بما في ذلك إرسال (بريد غير هامJunke mail)، أو مواد إعلانية إلى أفراد لم يطلبوها تحديدا كرسائل البريد الإلكتروني المزعج (SPAM).

3.2.3 إنشاء أو إجراء تحويل لـ (سلسلة رسائل chain letters) ، رسائل الاحتيال (Scam Email)، أو أي اشكال هرمية من أي نوع.

3.2.4 استخدام رسائل بريد غير مرغوب بها داخل شبكات (جهة العمل) لمزودي خدمات آخرين نيابة عن أو للدعاية لأي خدمة مستخدمة من قبل (جهة العمل) أو متصلة عبر شبكتها.

3.2.5 نشر الرسائل غير متعلقة بالعمل أو ما شابه ذلك لعدد كبير من مجموعات الأخبار((news groups أو ما يسمى بـ(newsgroup spam).

3.3 التلاعب والتزوير

3.3.1 استخدام هوية مزيفة في رسائل البريد الإلكتروني الخاصة بـ (جهة العمل).

3.3.2 يحظر تغيير أو العبث بمحتوى و/أو عناوين رسائل البريد الإلكتروني المعاد توجيهها أو مرفقاتها دون الحصول على موافقة مسبقة مع الالتزام بتوضيح أي تعديل يتم عليها بشكل صريح.

3.3.3 استخدام غير مصرح به لمعلومات البريد الإلكتروني أو تزويرها.

3.4 إدارة البيانات والرسائل

3.4.1 لا يمكن حذف الرسائل في البريد الالكتروني او التلاعب بخزنها الا وفق ضوابط المؤسسة.