سياسة أمن البريد الإلكتروني

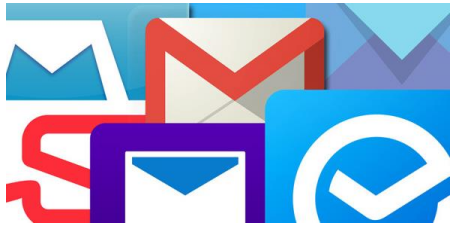
السياسات العامة لأمن المعلومات

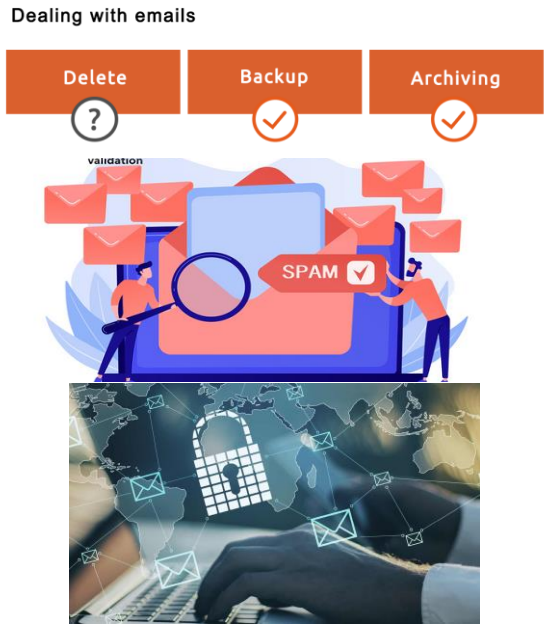
في الجهات الحكومية

المحاور

- بنود سياسة امن البريد الإلكتروني
- المقدمة
- الاهداف
- نطاق تطبيق السياسة
- مكونات أمن البريد الإلكتروني
- بعض أنواع هجمات البريد الإلكتروني
- بعض أفضل الممارسات لتطبيق إجراءات تأمين البريد الإلكتروني
- الأدوار والمسئوليات

بنود سياسة أمن البريد الإلكتروني





يجب لأي جهة حكومية تتبنى العمل بالبريد الإلكتروني امتلاك بريد إلكتروني خاص بها وضمن النطاق الوطني ye. كما يجب أن يكون نظام وقاعدة بيانات البريد الإلكتروني داخل البلد وليس مستضاف في الخارج

يجب على الجهة الحكومية توضيح سياستها للموظفين بشكل واضح فيما يتعلق بالاستخدام المقبول للبريد الإلكتروني

يجب أن تحدد الجهة سياستها (المناسبة لطبيعة عملها) تجاه استخدام خدمات البريد الإلكتروني العامة (المجانية أو التجارية) مثل (Gmail, mail,...etc.) ووسائل التواصل الاجتماعي مثل (واتساب ,تيلجرام...,الخ) فيما يخص أعمال الجهة وإرسال واستقبال الوثائق ونحوها

يجب على نظم المعلومات التابع للجهة الحكومية إنشاء عملية منهجية للتسجيل والاحتفاظ وحذف رسائل البريد الإلكترونية والسجلات المرفقة بها

يجب فحص الرسائل الصادرة والواردة للبريد الإلكتروني من الفيروسات وأي ملفات مشبوهة

يجب حماية عناوين البريد الالكتروني الداخلية أو التي تحتوي على المواقع الحكومية من التعديل أو الوصول غير المصرح به

وزارة الاتصالات وتقنية المعلومات

بنود سياسة أمن البريد الإلكتروني

لا يجوز التطفل على سجلات البريد الإلكتروني أو الدخول إليها إلا عن طريق صاحب البريد ومختص أمن المعلومات، باستثناء التدقيق في مثل الحالات (وجود أدلة على استخدام غير صحيح للسجل، احتواء السجل على محتويات تتعارض مع سياسات هذه الوثيقة، وجود حكم قضائي او دواعي أمنية من الجهات المختصة)

يجب أن تكون كافة المعلومات التي يتم تبادلها عبر الإنترنت من خلال الأجهزة والتسهيلات الخاصة بالجهة الحكومية هي ملك للجهة وليست للمستخدمين، لذا فإن للإدارة الحق في التدقيق ومر اقبة الجهة المستقبلة ومحتوى المراسلات كلما دعت الحاجة، وذلك من أجل حماية مصالح الجهة الحكومية

يجب تشفير رسائل البريد الإلكتروني بما يتو افق مع سياسات التشفير وسياسات تصنيف وحساسية المعلومات

لا يسمح باستخدام إعادة الإرسال بشكل آلي في الحالات التي تحمل فيها الرسالة معلومات مشفرة

يمنع فتح أو إعادة توجيه رسائل البريد الإلكتروني المرسلة من مصادر مشبوهة

يجب وضع آلية واضحة للموظفين للإبلاغ عن أي حالة اشتباه في اختراق للبريد الالكتروني الى إدارة / قسم امن المعلومات للقيام بالإجراءات المناسبة وتأمين وحماية البريد الالكتروني في الوقت المناسب

وزارة الاتصالات وتقنية المعلومات

السياسات العامة لأمن المعلومات

في الجهات الحكومية

المقدمة

البريد الإلكتروني هو الاكثر انتشار في جميع القطاعات الحكومية والتجارية والخاصة وغالباً ما يكون هو الطريقة الأساسية والرسمية للتواصل وتسيير الاعمال والتوعية داخل هذه القطاعات، البريد الالكتروني الرسمي يمثل رمز الاتصال الموثق بين أي جهة وباقي الجهات والأفراد التي تتعامل معها وبين موظفين الجهة نفسها، ويعطى للعميل مصداقية وطمأنينة على التعامل مع هذه الجهة.

ولكن سوء استخدام البريد الإلكتروني الرسمي أو عدم حمايته وتأمينه يمكن أن يولد العديد من المخاطر و التهديدات مثل الاختراق، التجسس على المراسلات، انتحال الشخصية وغيرها، وبالتالي من المهم عمل الإجراءات اللازمة لحماية وتأمين البريد الإلكتروني ووضع الضو ابط والتعليمات لاستخدام البريد الإلكتروني الرسمي للجهة الحكومية

سياسة أمن البريد الإلكتروني تضمن أمن وسلامة وسرية و إتاحية وخصوصية رسائل البريد الإلكتروني عند الارسال والاستقبال والحفظ والأرشفة

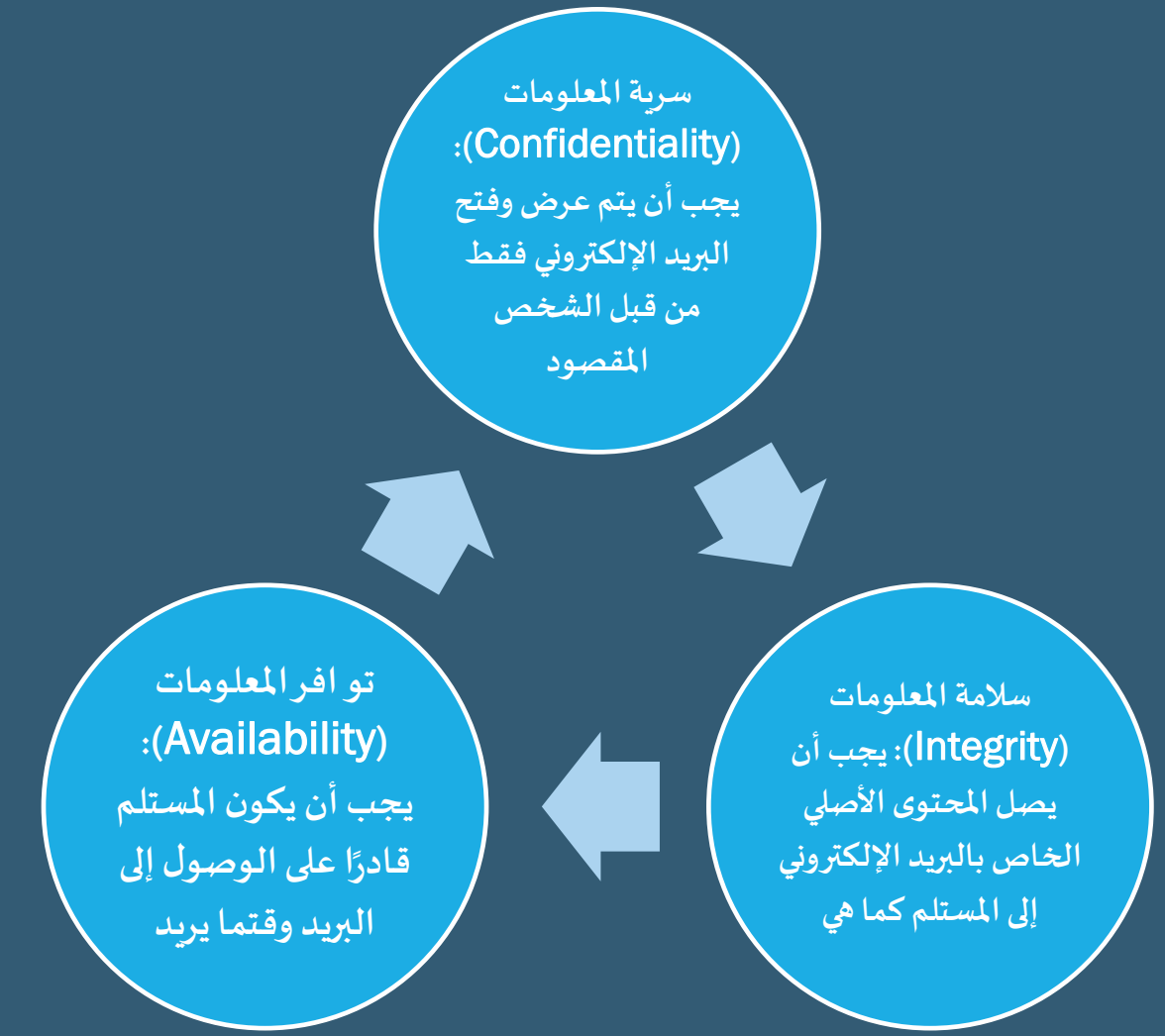
الأهداف

تهدف هذه السياسة الى ضمان أمن وسلامة وتوفر وخصوصية البريد الإلكتروني عند الإرسال والاستقبال وعند الحفظ والأرشفة، من خلال وضع تعليمات وضوابط توضح الاستخدام المقبول للبريد الإلكتروني، وتحديد الحد الأدنى من المتطلبات لاستخدام البريد الإلكتروني، ووضع الإجراءات اللازمة لتأمينه.

النطاق

تطبق هذه السياسة على جميع الموارد المعلوماتية المشمولة بأنظمة البريد الإلكتروني المعمول بها في الجهة الحكومية، والموظفين المتعاملين مع أنظمة البريد الإلكتروني الذين لهم حق استعمالها ولهم حساب بريد إلكتروني عليها.

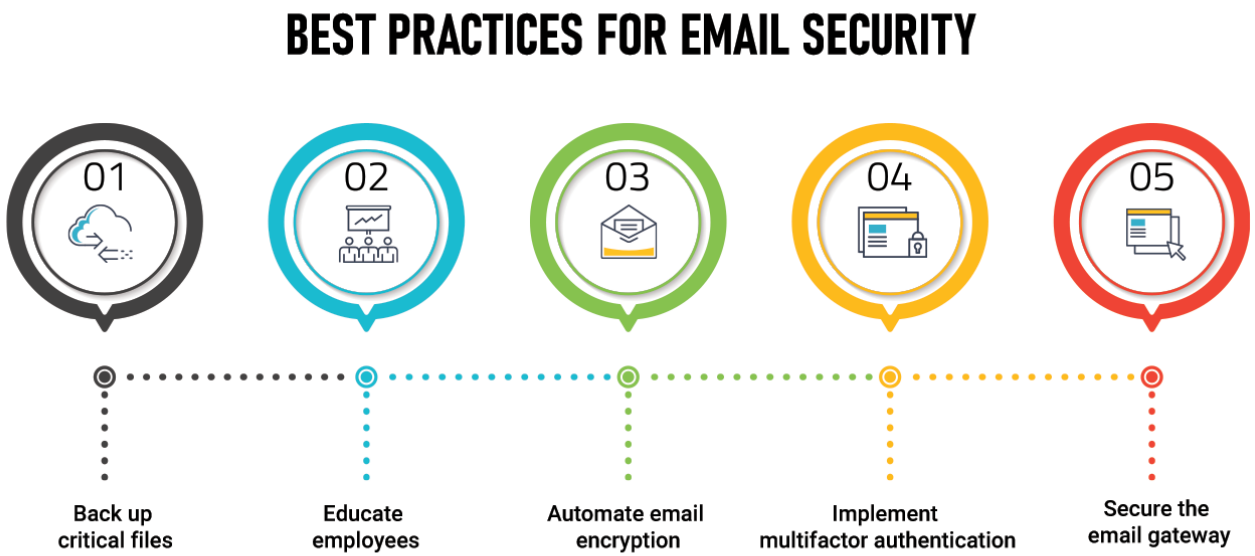
مبادئ أمن المعلومات (CIA) من منظور سياسة البريد الالكتروني



بعض أنواع هجمات البريد الإلكتروني

بعض أفضل الممارسات لتطبيق إجراءات تأمين البريد الإلكتروني

- الاتصال بشبكة موثوقة وأمنة عند استخدام البريد الالكتروني
- استخدام كلمات مرور صعبة ومعقدة
- تفعيل التحقق والمصادقة الثنائية (2FA)
- فكر قبل الضغط على أي شي (Think Before You Click)
- عدم الكشف أبدًا عن كلمة المرور الخاصة بك
- تثبيت برنامج مكافحة الفيروسات
- استخدام Spam Filters
- مراجعة إعدادات أمان وخصوصية بريدك الإلكتروني
- توعية وتثقيف الموظفين حول أحدث ممارسات أمان البريد الإلكتروني الرسمي
- استخدم البريد الإلكتروني الرسمي للأعمال الرسمية فقط.
- تشفير الاتصال مع سيرفر البريد الإلكتروني (SSL)



الأدوار والمسئوليات

من أهم مسئوليات الجهة الحكومية

وضع آلية واضحة للموظفين للإبلاغ عن أي حالة اشتباه في اختراق للبريد الالكتروني الى إدارة / قسم امن المعلومات للقيام بالإجراءات المناسبة وتأمين وحماية البريد الالكتروني في الوقت المناسب

تتبنى العمل بالبريد الإلكتروني امتلاك بريد إلكتروني خاص بها وضمن النطاق الوطني (ye.كما يجب أن يكون نظام وقاعدة بيانات البريد الإلكتروني داخل البلد وليس مستضاف في الخارج

عدم التطفل على سجلات البريد الإلكتروني أو الدخول إليها إلا عن طريق صاحب البريد ومختص أمن المعلومات، باستثناء التدقيق في مثل الحالات (وجود أدلة على استخدام غير صحيح للسجل، احتواء السجل على محتويات تتعارض مع سياسات هذه الوثيقة، وجود حكم قضائي او دواعي أمنية من الجهات المختصة)

توضيح سياستها للموظفين بشكل واضح فيما يتعلق بالاستخدام المقبول للبريد الإلكتروني

تشفير رسائل البريد الإلكتروني بما يتو افق مع سياسات التشفير وسياسات تصنيف وحساسية المعلومات

الأدوار والمسئوليات

من أهم مسئوليات مدير النظام

إنشاء عملية منهجية وفق أفضل الممارسات للتسجيل والاحتفاظ وحذف رسائل البريد الإلكترونية والسجلات المرفقة بها.

حماية عناوين البريد الالكتروني الداخلية أو التي تحتوي على المواقع الحكومية من التعديل أو الوصول غير المصرح به

فحص الرسائل الصادرة والواردة للبريد الإلكتروني من الفيروسات وأي ملفات مشبوهة

عدم السماح باستخدام إعادة الإرسال بشكل آلي في الحالات التي تحمل فيها الرسالة معلومات مشفرة

تشفير رسائل البريد الإلكتروني بما يتوافق مع سياسة التشفير وسياسة تصنيف وحساسية المعلومات

الأدوار والمسئوليات

من أهم مسئوليات المستخدمين

عدم استخدام أنظمة البريد الإلكتروني لغير الأغراض الرسمية أو بطريقة تؤثر سلبًا على سير العمل

عدم إرسال أي معلومات مصنفة على أنها سرية أو سرية للغاية بدون تشفير

عدم السماح للأخرين بالدخول إلى سجل البريد الإلكتروني الخاص بك أو استخدامه بدون موافقة قسم / أدارة النظام

في حالة اشتباه في اختراق للبريد الالكتروني يتم تغيير كلمة المرور و ابلاغ قسم / أدارة أمن المعلومات للقيام بالإجراءات المناسبة وتأمين وحماية البريد الالكتروني في الوقت المناسب

تعتبر رسائل البريد الإلكتروني بيانات سرية، فعلى كافة المستخدمين للإيميل الرسمي للجهة الالتزام بتغيير كلمات المرور بشكل دوري وعند الحاجة واختيار كلمات مرور معقدة

عدم الرد على أي رسالة غريبة أو مشبوهة أو مجهولة المصدر

انتهى،،،