سياسة أمن وخصوصية المعلومات
لمؤسسة
عبد الله بن عبد المحسن الثميري الأهلية

الاعتماد

اعتمد مجلس الأمناء هذه السياسة في جلسته رقم (٢٤/٢)

بتاريخ ١٤٤٦/٤/٣٠هـ الموافق ٢٠٢٤/١١/٠٢

سياسات أمن وخصوصية المعلومات

أولاً : سياسة التحكم في الوصول للبيانات والمعلومات

الهدف : -

ضمان تطبيق المؤسسة لعملية التحكم في الوصول إلى المعلومات الإلكترونية المتعلقة بالمؤسسة، وضمان توافقها مع المتطلبات القانونية والأمنية حيثما تقتضي الحاجة.

مجال التطبيق : -

تنطبق هذه السياسة على جميع موظفي وأعضاء ومتطوعي المؤسسة وأي جهة ترتبط بأي شكل بمرافق نظم المعلومات بالمؤسسة.

السياسة : -

١. الالتزام بسياسة التحكم في الوصول للمعلومات في المؤسسة يقلل فرص التعرض للخروقات الأمنية في الوقت الذي يسمح لإدارة تقنية المعلومات بأن يقوموا بأنشطتهم في إطار السياسات.
٢. يقتصر التحكم في الوصول لمعلومات وبيانات المؤسسة على المستخدمين المسموح لهم فقط وذلك لمنع تعرض التطبيقات أو البيانات والمعلومات لأي خرق أو تعديل عرضي أو غير مقصود.
٣. تتحكم إجراءات تسجيل هوية المستخدم في منح صلاحية الدخول للحسابات أو وقفها أو حذفها.
٤. يتم إنشاء وتفعيل حسابات مستخدمي المؤسسة أو المتطوعين بواسطة وحدة تقنية المعلومات في المؤسسة.
٥. يمنح المستخدمون امتيازات مع حساباتهم حسب ما يتناسب ودورهم ووظيفتهم على وجه الخصوص.
٦. يتم التحكم باستخدام أو منح كلمة المرور وفق سياسة كلمة المرور.
٧. يجب حماية كافة أجهزة الحاسب التي تنتمي للشبكة بكلمة مرور وشاشة توقف معيارية.
٨. يجب على المستخدمين إيقاف أجهزتهم النشطة التي لا يعملون عليها.
٩. مسؤولية ترك أجهزة الحاسب غير مستخدمة تقع على عاتق المستخدمين.
١٠. أفضل طريقة للقفل التلقائي لشاشة التوقف هي أن يضبط المؤقت على 15دقيقة بحيث يتم توفير الأمن الضروري في الوقت الذي لا يتسبب ذلك في إزعاج المستخدم.
١١. يجب الالتزام بمعايير اختيار كلمات المرور كما هو مدرج في سياسة كلمة المرور.
١٢. يجب أن يسمح النظام للمستخدمين بتغيير كلمات المرور.
١٣. يجب على النظام أن يكون قادراً على حفظ عمر وتاريخ كلمة المرور كما هو مبين في سياسة كلمة المرور وأن يمنع استخدام كلمة المرور نفسها.
١٤. يجب أن يجبر النظام المستخدمين على تغيير كلمات المرور المؤقتة عند الدخول الأول لهم.

ثانياً : سياسة النسخ الاحتياطي واستعادة وحفظ البيانات

الهدف : -

الهدف من هذه السياسة هو توضيح قواعد عمل نسخة احتياطية من بيانات المؤسسة لضمان إمكانية استردادها.

مجال التطبيق : -

تنطبق هذه السياسة على جميع موظفي وأعضاء ومتطوعي المؤسسة

السياسة : -

١. وحدة تقنية المعلومات هي المسؤولة عن عملية استرداد المعلومات / البيانات الإلكترونية في حال تلف البيانات.
٢. يجب أن تضمن وحدة تقنية المعلومات الترتيبات اللازمة لاستئناف العمل في المؤسسة بصورة عادية في فترة معقولة من الوقت، مع فقدان الحد الأدنى من البيانات. ونظراً لاحتمالات أن تتعطل الأنظمة لأسباب عديدة مع مرور الزمن، فينبغي الحفاظ على أجيال متعددة من النسخ الاحتياطية لضمان استمرارية الخدمات الهامة.
٣. جميع النسخ الاحتياطية لمعلومات وبيانات المؤسسة يجب أن يتم حفظها وأن تكون قابلة للاسترداد بشكل كامل.
٤. يجب الحفاظ على ثلاث نسخ احتياطية من معلومات وبيانات المؤسسة كحد أدنى.
٥. يجب الاحتفاظ بنسخة احتياطية كاملة لمعلومات وبيانات المؤسسة في بيئة آمنة.
٦. يتم فقط حفظ معلومات وبيانات المؤسسة الموجودة على خادم الشبكة ويتم دعمها وفقاً لإجراءات حفظ النسخ الاحتياطية بالمؤسسة.
٧. إجراءات استعادة البيانات يجب تحديثها والتحقق منها بشكل دوري.

ثالثاً : سياسة أمن المعلومات

الهدف : -

١. تأمين الحماية لبيانات المؤسسة من التداعيات المحتملة الناتجة عن الخروقات السرية أو الأضرار الفيروسية.
٢. ضمان حماية كافة أصول المعلومات ومرافق الشبكات والحواسيب من التلف أو الفقدان أو سوء الاستخدام.
٣. ضمان معرفة موظفي وأعضاء المؤسسة والمتطوعين بمبادئ استخدام المعلومات الإلكترونية والالتزام بها.
٤. زيادة مستوى الوعي والفهم تجاه متطلبات أمن المعلومات في المؤسسة وسرية وسلامة البيانات التي يمتلكونها أو يتعاملون بها.

مجال التطبيق : -

تطبق هذه السياسة على أنواع الأمن التالية بالمؤسسة:

أ- تنطبق هذه السياسة على جميع موظفي وأعضاء ومتطوعي المؤسسة.
ب- تنطبق هذه السياسة على بيانات المؤسسة وبرامجها وأنظمتها وأجهزة الحاسب والشبكات السلكية واللاسلكية.

السياسة : -

١. يجب حماية المعلومات من أي اختراق غير مسموح به.
٢. يلتزم جميع العاملين في المؤسسة والمتطوعين بسرية المعلومات والحفاظ على خصوصيتها.
٣. يلتزم جميع العاملين في المؤسسة والمتطوعين بالحفاظ على سلامة ومصداقية المعلومات.
٤. يلتزم جميع العاملين في المؤسسة والمتطوعين بالحفاظ على إتاحة المعلومات.
٥. إبلاغ "وحدة تقنية المعلومات" عن كافة أشكال الخروقات الفعلية أو المحتملة لأمن المعلومات من أجل القيام بالإجراء اللازم.
٦. تحديث جميع برمجيات مكافحة الفيروسات من قبل خدمات تقنية المعلومات بانتظام، مع التحقق من الأنظمة.
٧. التحقق من أن جميع الملفات التي تم تحميلها عن طريق البريد الإلكتروني خالية من الفيروسات.
٨. التأكد من أن جميع السيرفرات قد تم تزويدها ببرامج مكافحة الفيروسات وأن كفاءتها ضد الفيروسات مضمونة.
٩. التحقق من فحص جميع الوسائط من الفيروسات قبل الاستخدام من قبل المستخدم.

١٠. يُسمح لأي مستخدم باستخدام الوسائط في أجهزة الحواسيب المكتبية الخاصة به، بعد التحقق من خلوها من الفيروسات.

١١. يجب أن يتم فحص جميع مراسلات البريد الإلكتروني الصادر والوارد للتأكد من خلوها من الفيروسات والمحتوى الضار قبل فتحها وخاصة مرفقات البريد الإلكتروني.

١٢. لن يحصل المستخدم على أي تفويض إداري في تفعيل أو تعطيل ميزات برنامج مكافحة الفيروسات.

١٣. يتم قفل حساب المستخدم المتضرر وفصل النظام المتضرر في الشبكة وعزله وتطويقه الى أن يتم تطهيره من قبل وحدة تقنية المعلومات.

١٤. يلتزم جميع العاملين في المؤسسة والمتطوعين بعدم الوصول للبريد الإلكتروني ذي المحتوى الضار أو المشكوك فيه من قبل المستخدمين دون تعليمات من قبل وحدة تقنية المعلومات.

١٥. تعتبر "وحدة تقنية المعلومات" مسؤولة عن الحفاظ على هذه السياسة وعن تقديم الدعم والنصيحة أثناء تنفيذها.

رابعاً : سياسة كلمة المرور

الهدف:

تحمي سياسة إدارة كلمات المرور الفعالة بيانات المؤسسة وتخفض من مخاطر الدخول غير المسموح به، وتهدف هذه السياسة إلى إنشاء بيئة آمنة لتقنية معلومات من خلال تفعيل استخدام كلمات المرور القوية.

مجال التطبيق:

تطبق هذه السياسة على جميع العاملين الذين لديهم، أو هم مسؤولين عن، حسابات أو أي شكل من أشكال الدخول الذي يتطلب كلمة مرور. ويشمل ذلك أي نظام متواجد بالمؤسسة أو يتمتع بحق الدخول إلى الشبكة أو يخزن معلومات ليست متاحة للعامة عن المؤسسة.

السياسة

١. تعد كلمات المرور جانباً هاماً في أمن الحواسيب، كما تعد خط الدفاع الأول لحماية حسابات المستخدمين، إذ قد تتسبب كلمة المرور المنتقاة بشكل سيء في إلحاق الضرر بكامل الشبكة.

٢. يجب التعامل مع كلمات المرور كافة بوصفها معلومات حساسة وسرية في المؤسسة.

٣. تفعل سياسة كلمة المرور بشكل تلقائي.

٤. عند تقدم المستخدم بطلب لإعادة ضبط كلمة المرور فإن ذلك يتطلب التحقق من شخصية المستخدم.

٥. تقع على عاتق جميع أعضاء المؤسسة مسؤولية اختيار كلمات مرورهم وفق معايير آمنة .

خامساً : سياسة البريد الإلكتروني

الهدف:

تهدف هذه السياسة لضمان الاستخدام الأمثل والآمن لخدمة البريد الإلكتروني من قبل موظفي وأعضاء ومتطوعي المؤسسة.

مجال التطبيق:

تنطبق هذه السياسة على جميع موظفي وأعضاء ومتطوعي المؤسسة وأي جهة ترتبط بأي شكل بمرافق نظم المعلومات بالمؤسسة.

السياسة:

١. يجب على المستخدمين استخدام خدمات البريد الإلكتروني الرسمي للمؤسسة في المعاملات الرسمية، وعدم استخدام خدمات البريد الإلكتروني الشخصي.
٢. على المستخدم الحذر عند إعادة توجيه أي بريد إلكتروني، وعدم توجيه كل من البريد الإلكتروني غير المرغوب فيه والإعلانات التجارية والبريد العشوائي.
٣. يُسمح فقط للمستخدمين بإرسال رسائل البريد الإلكتروني والمرفقات التي تتفق مع القيم الدينية والثقافية والسياسية والأخلاقية للدولة، مع عدم السماح بإرسال رسائل قد تسبب ضرراً للمؤسسة أو تؤدي إلى تشويه صورتها وسمعتها.
٤. لا يُسمح للمستخدمين بإرسال أو الرد أو توجيه رسائل البريد الإلكتروني ذي المحتوى السري أو التي تنتهك حقوق الملكية الفكرية.
٥. يحظر على المستخدمين ارسال أو الرد أو توجيه رسائل البريد الإلكتروني التي تحتوي على مرفقات مصابة
بالفيروسات أو أي برمجيات ضارة.
٦. على المستخدمين عدم فتح رسائل البريد الإلكتروني غير المرغوب فيها ، مع حذفها من النظام.
٧. يحظر على المستخدمين استخدام البريد الإلكتروني للمؤسسة في المعاملات الخاصة.
٨. يحظر على المستخدمين استخدام نظام البريد الإلكتروني للمؤسسة لانتحال صفة شخص آخر.
٩. على المستخدمين التحقق والتأكد من أن مرفقات رسائل البريد الإلكتروني خالية من الفيروسات أو أي تعليمات برمجية ضارة.
١٠. على المستخدمين استخدام التواقيع وإخلاء المسؤولية المعتمدة في المؤسسة مع كافة رسائل البريد الإلكتروني.
١١. على المستخدمين عدم تسجيل عنوان البريد الإلكتروني الخاص بالمؤسسة في المواقع الالكترونية لغير أغراض العمل

سادساً : سياسة خصوصية البيانات

الهدف:

تهدف هذه السياسة إلى توضيح إجراءات التعامل مع بيانات جميع عملاء المؤسسة الداخليين والخارجيين والمحافظة على خصوصيتها داخل المؤسسة أو من خلال موقع المؤسسة الإلكتروني.

مجال التطبيق :

تطبق هذه السياسة على جميع من يعمل لصالح المؤسسة سواء كانوا أعضاء مجلس الأمناء أو موظفين أو متطوعين أو مستشارين بصرف النظر عن مناصبهم في المؤسسة.

السياسة

- تلتزم المؤسسة بحماية خصوصية بيانات جميع عملائها الداخليين والخارجيين وكل من يعمل لصالح المؤسسة وجميع المستفيدين من خدمات المؤسسة.
- تلتزم المؤسسة بعدم مشاركة البيانات إلا في نطاق ضيق جدا حسب سياسة خصوصية البيانات .
- تلتزم المؤسسة بالسرية التامة مع جميع بيانات المتعاملين معها وعدم نشرها ما لم يوافقوا على النشر.
- تلتزم المؤسسة بعدم بيع أو مشاركة بيانات المتعاملين معها مع أي جهة أخرى دون إذنهم.
- لن ترسل المؤسسة أي إيميلات أو رسائل نصية للمتعاملين معها سواء بواسطتها أو بواسطة أي جهة أخرى دون إذنهم.
- صياغة سياسة منفصلة بخصوصية البيانات على المواقع الإلكترونية وكافة مواقع التواصل الاجتماعية التابعة للمؤسسة.

سابعاً : سياسة خصوصية البيانات للمواقع الإلكترونية للمؤسسة

الهدف:

تهدف هذه السياسة إلى توضيح إجراءات التعامل مع بيانات جميع زوار مواقع المؤسسة الإلكترونية والمحافظة على خصوصيتها.

مجال التطبيق :

تطبق هذه السياسة على جميع زوار موقع المؤسسة سواء كانوا أعضاء في المؤسسة أو مستفيدين أو زوار للموقع.

السياسة:

- تؤكد المؤسسة أن خصوصية الزوار تشكل لنا أولوية كبرى، وسوف لن نستخدم تلك البيانات إلا بالطريقة الملائمة للحفاظ على الخصوصية بشكل آمن.
- لن نقوم نهائياً بتبادل البيانات الشخصية مع أي جهة تجارية أو أطراف خارجية باستثناء ما يتم الإعلان عنه للمستخدم الكريم وبعد موافقته على ذلك.
- لن نقوم نهائياً باستخدام بيانات المستخدمين الكرام بإرسال رسائل ذات محتوى تجاري أو ترويجي.
- قد نستخدم البيانات المسجلة في الموقع لعمل الاستبانات وقياس آراء الزوار بهدف تطوير أداء المؤسسة أو تطوير مواقع المؤسسة الإلكترونية.
- في الحالات الطبيعية يتمُّ التعامل مع البيانات بصورة آلية (إلكترونية) من خلال التطبيقات والبرامج المحدَّدة لذلك، دون أن يستلزم ذلك مشاركة الموظفين أو اطلاعهم على تلك البيانات.
- وفي حالات استثنائية (كالتحقيقات والقضايا) قد يطلع عليها موظفو الجهات الرقابية أو من يلزم اطلاعه على ذلك؛ خضوعاً لأحكام القانون وأوامر الجهات القضائية.
- مواقعنا قد تحتوي على روابط إلكترونية لمواقع أو بوابات قد تستخدم طرقاً لحماية البيانات وخصوصياتها تختلف عن الطرق المستخدمة لدينا، ونحن غير مسؤولين عن محتويات وطرق خصوصيات المواقع الأخرى التي لا تقع تحت استضافة موقعنا وتتولى جهاتها مسؤولية حمايتها.
- ينشر في الموقع الإلكتروني العبارة التالية "نظرًا للتطوُّر الهائل في مجال التقنية، والتغيُّر في نطاق القوانين المتعلقة بالمجال الإلكتروني؛ فالموقع يحتفظ بالحقِّ في تعديل بنود سياسة الخصوصية هذه وشروطها في أي وقتٍ يراه ملائماً، ويتم تنفيذ التعديلات على هذه الصفحة، ويتم إخطاركم في حالة إجراء أية تعديلات ذات تأثير".
- يمكنك الاتصال بنا دائماً للإجابة عن استفساراتك بخصوص هذه السياسة من خلال وسائل التواصل (اتصل بنا) المذكورة في هذا الموقع