« سياسة تقنية المعلومات »

الإصدار	التاريخ	الإعداد	المراجعة	الاعتماد
الإصدار الرابع	٢٨ / ٠٧/ ٢٠٢٥م	فريق العمل	المسؤول التنفيذي	مجلس الإدارة

تم اعتماد السياسة في اجتماع مجلس الإدارة الرابع
بتاريخ : ٠٣/ ٠٢ / ١٤٤٧هـ الموافق : ٢٨ / ٠٧ / ٢٠٢٥م

أولًا: مقدمة

تهدف هذه السياسة إلى وضع إطار مؤسسي منظم لاستخدام وإدارة تقنية المعلومات في جمعية الدعوة والإرشاد وتوعية الجاليات بالطائف، بما يضمن الاستخدام الآمن والفعال للأنظمة والأجهزة والشبكات والبيانات والموارد التقنية، ورفع كفاءة العمل المؤسسي، والمحافظة على سرية المعلومات وسلامتها وتوافرها.

ثانيًا: أهداف السياسة

تهدف السياسة إلى:

١. **تنظيم استخدام موارد وتقنيات المعلومات في الجمعية.**
٢. **حماية بيانات الجمعية والعاملين والمستفيدين والداعمين والمتطوعين.**
٣. **المحافظة على سرية المعلومات وسلامتها وتوافرها.**
٤. **الحد من مخاطر الاختراق أو فقدان البيانات أو إساءة استخدامها.**
٥. **تنظيم صلاحيات الوصول إلى الأنظمة والملفات الإلكترونية.**
٦. **ضمان الاستخدام الأمثل للأنظمة والبرامج والأجهزة التقنية.**
٧. **تنظيم النسخ الاحتياطي واستعادة البيانات عند الحاجة.**
٨. **رفع مستوى الوعي بالأمن السيبراني بين منسوبي الجمعية.**
٩. **الالتزام بالأنظمة واللوائح والتعليمات ذات العلاقة في المملكة العربية السعودية.**

ثالثًا: نطاق التطبيق

تسري هذه السياسة على:

- **جميع موظفي الجمعية والمتعاونين والمتطوعين والمتدربين.**
- **جميع أجهزة الحاسب الآلي والأجهزة المحمولة والأجهزة الذكية المملوكة للجمعية أو المستخدمة لأغراض العمل.**
- **الشبكات والأنظمة والتطبيقات والمنصات الإلكترونية.**
- **البريد الإلكتروني والحسابات الرسمية للجمعية.**
- **قواعد البيانات والملفات والمستندات الإلكترونية.**
- **الخدمات السحابية وأنظمة التخزين الإلكتروني.**
- **أي وسيلة تقنية تستخدم في تنفيذ أعمال الجمعية.**

رابعًا: المسؤوليات

1. الإدارة العليا

تتولى الإدارة العليا:

- اعتماد سياسة تقنية المعلومات.
- توفير الموارد اللازمة لتطبيقها.
- دعم متطلبات أمن المعلومات واستمرارية الأعمال.
- متابعة مستوى الالتزام بالسياسة.

2. إدارة الدعم المؤسسي / الجهة المختصة بتقنية المعلومات

تتولى:

- إدارة الأنظمة والأجهزة والشبكات.
- منح وإلغاء صلاحيات المستخدمين وفق الصلاحيات المعتمدة.
- متابعة أمن الأنظمة والتحديثات التقنية.
- تنفيذ النسخ الاحتياطي وفق الخطة المعتمدة.
- معالجة الأعطال والحوادث التقنية.
- متابعة تراخيص البرامج والأنظمة.
- توعية الموظفين بالممارسات الآمنة لاستخدام التقنية.

3. الموظفون والمستخدمون

يلتزم كل مستخدم بما يلي:

- استخدام الأنظمة والأجهزة لأغراض العمل المشروعة.
- المحافظة على بيانات الدخول وعدم مشاركتها.
- حماية الأجهزة والملفات من الوصول غير المصرح به.
- الإبلاغ فوراً عن أي حادثة أو اشتباه أمني.
- الالتزام بالتعليمات التقنية الصادرة من الجمعية.

خامسًا: إدارة حسابات المستخدمين وصلاحيات الوصول

١. يمنح كل موظف حسابًا خاصًا به متى كان النظام يدعم ذلك.
٢. يمنع استخدام حسابات الآخرين أو مشاركة كلمات المرور.
٣. تمنح الصلاحيات بناءً على طبيعة الوظيفة والحاجة الفعلية للوصول.
٤. تطبق قاعدة أقل صلاحية ممكنة بحيث لا يمنح المستخدم إلا الصلاحيات اللازمة لأداء مهامه.
٥. تراجع صلاحيات المستخدمين بشكل دوري.
٦. يتم إلغاء أو تعديل صلاحيات الموظف عند انتهاء خدمته أو انتقاله إلى وظيفة أخرى.

٧. لا يجوز منح صلاحيات إدارية أو عالية الحساسية إلا بموافقة الجهة المخولة.

سادسًا: كلمات المرور والمصادقة

يلتزم المستخدمون بما يلي:

- استخدام كلمات مرور قوية وغير سهلة التخمين.
- عدم مشاركة كلمات المرور مع أي شخص.
- عدم كتابة كلمات المرور في أماكن مكشوفة.
- عدم استخدام كلمة المرور نفسها للحسابات الحساسة متى أمكن ذلك.
- تفعيل المصادقة متعددة العوامل في الأنظمة التي تدعمها، خصوصًا الأنظمة الحساسة.
- تغيير كلمات المرور عند الاشتباه في تعرضها للاختراق.

سابعًا: استخدام أجهزة الجمعية

١. تخصص أجهزة الجمعية لأغراض العمل.
٢. يحظر تثبيت البرامج غير المعتمدة.
٣. يمنع تعطيل برامج الحماية أو إعدادات الأمان.
٤. يجب تثبيت التحديثات الأمنية والبرمجية المعتمدة.
٥. لا يجوز نقل أجهزة الجمعية أو تسليمها للغير دون موافقة الجهة المختصة.
٦. يجب المحافظة على الأجهزة من التلف أو الفقدان أو الاستخدام غير المصرح به.
٧. عند فقدان جهاز يحتوي على بيانات الجمعية، يجب الإبلاغ فورًا للجهة المختصة.

ثامنًا: استخدام البريد الإلكتروني والاتصالات الإلكترونية

١. يستخدم البريد الإلكتروني الرسمي في المراسلات المتعلقة بأعمال الجمعية.
٢. يمنع إرسال معلومات سرية أو حساسة إلى جهات غير مصرح لها.
٣. يجب التأكد من عنوان المستلم قبل إرسال الملفات أو البيانات المهمة.
٤. يحظر فتح الروابط أو المرفقات المشبوهة.
٥. يمنع استخدام البريد الرسمي في الأنشطة المخالفة للأنظمة أو لسياسات الجمعية.
٦. يجب التعامل مع الرسائل التي تتضمن طلبات مالية أو بيانات حساسة بحذر والتحقق من مصدرها.

تاسعًا: حماية البيانات والمعلومات

تلتزم الجمعية باتخاذ الإجراءات المناسبة لحماية المعلومات من:

- الوصول غير المصرح به.
- التعديل أو العبث.
- التسريب أو الإفشاء.
- الفقدان أو التلف.

- الاستخدام غير المشروع.

وتصنف المعلومات وفق درجة حساسيتها ، ومن ذلك:

١. معلومات عامة.
٢. معلومات داخلية.
٣. معلومات سرية.
٤. معلومات شديدة الحساسية.

ويجب تحديد الصلاحيات المناسبة لكل مستوى من مستويات المعلومات.

عاشراً: النسخ الاحتياطي واستعادة البيانات

١. تضع الجمعية خطة للنسخ الاحتياطي للبيانات والأنظمة المهمة.
٢. تحدد دورية النسخ الاحتياطي وفق أهمية النظام والبيانات.
٣. تحفظ النسخ الاحتياطية بطريقة آمنة تمنع الوصول غير المصرح به.
٤. يراعى وجود نسخة احتياطية منفصلة عن النظام الأساسي متى كان ذلك ممكناً.
٥. يتم اختبار استعادة النسخ الاحتياطية بصورة دورية للتأكد من صلاحيتها.
٦. توثق عمليات النسخ والاستعادة والحوادث المرتبطة بها.

الحادي عشر: أمن الشبكات والأنظمة

تلتزم الجمعية بما يلي:

- تأمين شبكات الاتصال الداخلية واللاسلكية.
- استخدام وسائل الحماية المناسبة من البرمجيات الخبيثة.
- تحديث أنظمة التشغيل والبرامج بصورة دورية.
- تقييد الوصول إلى الشبكات والأنظمة الحساسة.
- مراقبة الأنظمة عند توفر الوسائل التقنية المناسبة.
- عدم توصيل أجهزة غير موثوقة بشبكة الجمعية دون تصريح.

الثاني عشر: استخدام الإنترنت

يجب استخدام خدمة الإنترنت بما يخدم أعمال الجمعية، ويحظر:

- الدخول المتعمد إلى المواقع المخالفة للأنظمة أو الآداب العامة.
- تحميل البرامج أو الملفات غير الموثوقة.
- استخدام الإنترنت بما يضر بسمعة الجمعية.
- استخدام موارد الجمعية لأعمال تجارية أو شخصية غير مصرح بها.
- تجاوز أنظمة الحماية أو محاولة الوصول إلى موارد غير مصرح بها.

الثالث عشر: استخدام الأجهزة والوسائط الخارجية

لا يسمح باستخدام وحدات التخزين الخارجية، مثل وحداتUSB ، لنقل البيانات الحساسة إلا عند الحاجة وبما يتوافق مع الضوابط المعتمدة.

ويجب فحص الوسائط الخارجية قبل استخدامها والتأكد من خلوها من البرمجيات الضارة.

الرابع عشر: الحوسبة السحابية والتطبيقات الإلكترونية

١. لا يجوز استخدام خدمات التخزين السحابي أو التطبيقات الإلكترونية لحفظ بيانات الجمعية إلا بعد اعتمادها.
٢. يجب التأكد من ملاءمة الخدمة لمتطلبات حماية البيانات وأمن المعلومات.
٣. يمنع رفع الملفات السرية إلى خدمات أو حسابات شخصية.
٤. يجب تحديد صلاحيات مشاركة الملفات وعدم جعل الملفات الحساسة متاحة للعامة.
٥. تراجع الحسابات والخدمات السحابية المستخدمة من الجمعية بصورة دورية.

الخامس عشر: إدارة البرمجيات والتراخيص

١. تستخدم الجمعية البرامج المرخصة أو المسموح باستخدامها نظاماً.
٢. يحظر استخدام البرامج المقرصنة.
٣. يجب الاحتفاظ بسجل للبرامج والتراخيص المهمة.
٤. تتم مراجعة التراخيص قبل انتهائها.
٥. يمنع تثبيت أي برنامج غير معتمد على أجهزة الجمعية.

السادس عشر: التعامل مع الحوادث التقنية والأمنية

يجب على الموظف الإبلاغ فوراً عن أي حادثة أو اشتباه، مثل:

- فقدان جهاز أو هاتف تابع للجمعية.
- الاشتباه في اختراق حساب.
- وصول رسالة احتيالية أو مشبوهة.
- تسرب أو إرسال بيانات إلى جهة غير مصرح لها.
- إصابة الجهاز ببرمجيات ضارة.
- اكتشاف دخول غير مصرح به إلى أحد الأنظمة.

ولا يجوز للمستخدم محاولة إخفاء الحادثة أو حذف الأدلة التقنية المتعلقة بها.

السابع عشر: التوعية والتدريب

تعمل الجمعية على رفع الوعي التقني والأمني لمنسوبيها من خلال:

- برامج توعوية دورية.
- التدريب على حماية الحسابات وكلمات المرور.
- التوعية بالتصيد والاحتيال الإلكتروني.

- التوعية بحماية البيانات والخصوصية.
- توعية الموظفين بالإبلاغ عن الحوادث الأمنية.

الثامن عشر: إدارة الأصول التقنية

تحتفظ الجمعية بسجل للأصول التقنية، ويشمل -بحسب الحاجة:-

- أجهزة الحاسب.
- الطابعات.
- أجهزة الشبكات.
- أجهزة الاتصالات.
- الأجهزة المحمولة.
- البرامج والتراخيص.
- الأنظمة والتطبيقات.

ويجب تحديث سجل الأصول عند الإضافة أو النقل أو الاستبدال أو الإتلاف.

التاسع عشر: التخلص من الأجهزة والبيانات

عند التخلص من الأجهزة أو نقل ملكيتها أو إخراجها من الخدمة، يجب اتخاذ الإجراءات المناسبة لحذف البيانات بطريقة آمنة، بما يمنع استعادتها أو الوصول إليها من غير المصرح لهم.

العشرون: العمل عن بُعد واستخدام الأجهزة الشخصية

عند السماح للموظف بالعمل عن بعد أو استخدام جهاز شخصي لأغراض العمل، يجب:

١. الالتزام بإجراءات حماية البيانات.
٢. عدم حفظ البيانات الحساسة على أجهزة شخصية إلا عند الحاجة وبموافقة الجهة المختصة.
٣. استخدام وسائل الاتصال والأنظمة المعتمدة.
٤. المحافظة على سرية بيانات الدخول.
٥. عدم تمكين الآخرين من استخدام الجهاز أثناء الوصول إلى بيانات الجمعية.

الحادي والعشرون: الخصوصية وحماية البيانات الشخصية

تلتزم الجمعية بالتعامل مع البيانات الشخصية وفق الأنظمة واللوائح والتعليمات المعمول بها في المملكة العربية السعودية، وبما يحقق الحد من جمع البيانات أو استخدامها أو الإفصاح عنها دون مسوغ نظامي.

كما يجب قصر الوصول إلى البيانات الشخصية على الأشخاص الذين تتطلب مهامهم الوظيفية ذلك.

الثاني والعشرون: التعاقد مع مزودي الخدمات التقنية

عند التعاقد مع مزود خدمة تقنية، يجب مراعاة:

- موثوقية مقدم الخدمة.
- مستوى حماية البيانات.
- صلاحيات الوصول.
- مسؤوليات الطرفين.
- سرية المعلومات.
- آلية التعامل مع الحوادث.
- استعادة البيانات عند انتهاء التعاقد.
- إلغاء صلاحيات الوصول بعد انتهاء العلاقة التعاقدية.

الثالث والعشرون: المراقبة والالتزام

للجمعية، وفق الأنظمة والضوابط المعمول بها، اتخاذ الإجراءات اللازمة للتحقق من الالتزام بهذه السياسة، بما في ذلك مراجعة استخدام الأنظمة والأجهزة والصلاحيات، مع مراعاة الخصوصية والضوابط النظامية ذات العلاقة.

الرابع والعشرون: المخالفات

يعد مخالفة لهذه السياسة كل استخدام غير مصرح به للأنظمة أو الأجهزة أو البيانات، أو مشاركة بيانات الدخول، أو إفشاء المعلومات، أو تجاوز الصلاحيات، أو تعطيل وسائل الحماية، أو استخدام موارد الجمعية بما يخالف الأنظمة والتعليمات.

وتتعامل الجمعية مع المخالفات وفق اللوائح والسياسات الداخلية والأنظمة المعمول بها.

الخامس والعشرون: المراجعة والتحديث

تراجع هذه السياسة دوريًا، أو عند حدوث تغييرات جوهرية في الأنظمة أو التقنية أو المخاطر، وتحدث عند الحاجة، ويكون اعتماد التعديلات من الجهة صاحبة الصلاحية في الجمعية.

السادس والعشرون: أحكام عامة

١. تعد هذه السياسة جزءًا من منظومة الحوكمة والضبط الداخلي في الجمعية.
٢. لا تعفي هذه السياسة أي موظف من الالتزام بالأنظمة واللوائح والتعليمات الحكومية ذات العلاقة.
٣. في حال تعارض أي حكم في هذه السياسة مع نظام أو لائحة حكومية واجبة التطبيق، فيطبق النص النظامي الأعلى.
٤. يجب تعريف الموظفين بهذه السياسة عند انضمامهم للجمعية، وتوعيتهم بالتحديثات الجوهرية عليها.
٥. يبدأ العمل بهذه السياسة من تاريخ اعتمادها.