جمعية
ينبع
للإسكان
التنموي

سياسة تقنية المعلومات لجمعية ينبع للإسكان التنموي

إعتماد مجلس الإدارة

تم إعتماد سياسة تقنية المعلومات في جمعية ينبع للإسكان التنموي في اجتماع مجلس الإدارة بجلسته الثانية لعام 2024م ، والمنعقدة يوم السبت بتاريخ 2024/11/16م.

اعتماد رئيس مجلس الإدارة

عبدالرحمن بن سليم الجهني

المركز الوطني لتنمية القطاع غير الربحي
ختم الجمعية
جمعية ينبع للإسكان التنموي
رقم الترخيص : 10005596100

جمعية ينبع للإسكان التنموي

رقم السياسة	006
إسم السياسة	سياسة تقنية المعلومات
المسؤولية عن التطبيق	مجلس الإدارة / اللجان الدائمة والمؤقتة / المدير التنفيذي / جميع العاملين بالجمعية

❖ المقدمة:

تهدف هذه اللائحة إلى تنظيم كافة الجوانب المتعلقة بتقنية المعلومات في جمعية ينبع للإسكان التنموي، بما في ذلك استخدام الإنترنت، حماية المعلومات الشخصية والبيانات، وتأمين البنية التحتية التقنية للجمعية ضد التهديدات السيبرانية. تلتزم الجمعية بتوفير بيئة رقمية آمنة وفعالة تدعم أعمالها وتحقق أعلى مستويات الأمان والخصوصية لموظفيها ومستفيديها.

❖ استخدام الإنترنت والشبكة الداخلية:

جميع الأنشطة التي يتم إجراؤها على الإنترنت والشبكة الداخلية للجمعية يجب أن تكون متوافقة مع أهداف الجمعية ومتطلباتها العملية. يحظر تمامًا استخدام الإنترنت للوصول إلى محتويات غير لائقة أو مخالفة للقوانين أو غير متعلقة بالعمل. يجب على جميع المستخدمين الالتزام بالضوابط التالية:

1. استخدام الإنترنت لأغراض العمل فقط، وعدم استخدامه لأنشطة شخصية أو ترفيهية.
2. يحظر تصفح مواقع ذات محتوى عنيف، إباحي، غير قانوني أو يروج لخطاب الكراهية.
3. يتعين على الموظفين الالتزام بالسياسات الداخلية المتعلقة بالتحميل أو تنزيل الملفات، حيث يجب أن تتم هذه العمليات بموافقة إدارة تقنية المعلومات.
4. يجوز لإدارة تقنية المعلومات مراقبة الأنشطة على الشبكة لضمان الامتثال للقواعد والسياسات المعمول بها.

❖ حماية المعلومات والبيانات الشخصية:

تعتبر حماية البيانات الشخصية والحساسة من أهم أولويات الجمعية. جميع المعلومات التي يتم جمعها من الموظفين أو المستفيدين أو الشركاء التنفيذيين يتم التعامل معها بسرية تامة وفقًا لأعلى معايير الأمان. تشمل الإجراءات المتبعة ما يلي:

1. لا يتم جمع أي بيانات إلا لأغراض محددة وواضحة، وتتخذ الجمعية كل التدابير اللازمة لحماية هذه البيانات من الوصول غير المصرح به أو سوء الاستخدام.
2. استخدام تقنيات التشفير لحماية المعلومات الحساسة سواء أثناء تخزينها أو نقلها عبر الشبكة.
3. لا تتم مشاركة البيانات مع أطراف خارجية إلا بعد الحصول على موافقة صاحب البيانات أو بموجب التزام قانوني.
4. يجب على جميع المستخدمين التعامل مع البيانات وفقًا للقوانين واللوائح المعمول بها لحماية خصوصية الأفراد.

❖ الأمن السيبراني والحماية التقنية:

تلتزم الجمعية باتخاذ جميع الإجراءات اللازمة لحماية أنظمة تقنية المعلومات الخاصة بها من التهديدات السيبرانية. تشمل هذه الإجراءات استخدام أحدث وسائل الحماية مثل الجدران النارية وبرامج مكافحة الفيروسات وتحديثها بانتظام لضمان أعلى مستويات الأمان. كذلك:

1. يجب على جميع المستخدمين استخدام كلمات مرور قوية، وتغييرها بانتظام، وتجنب مشاركتها مع الآخرين.
2. يتم تفعيل أنظمة الحماية مثل التحقق الثنائي (Two-Factor Authentication) عند الحاجة لضمان حماية الحسابات.
3. يتم مراقبة الشبكة بانتظام للكشف عن أي محاولات اختراق أو نشاط غير معتاد، وتتم معالجة أي تهديدات فور اكتشافها.
4. يتعين على الموظفين الإبلاغ فورًا عن أي محاولة اختراق أو استخدام غير مشروع للنظام.

❖ النسخ الاحتياطي واستعادة البيانات:

تتبع الجمعية سياسات صارمة لضمان سلامة بياناتها من خلال إجراء نسخ احتياطي دوري لكافة البيانات الهامة. هذا النسخ الاحتياطي يتم تخزينه في أماكن آمنة لضمان إمكانية استعادة البيانات في حالة حدوث أي خلل في النظام. ويتم اتباع الإجراءات التالية:

1. النسخ الاحتياطي للبيانات يتم بانتظام وفقًا لجدول زمني محدد.
2. تخزين النسخ الاحتياطية في مواقع آمنة ومعزولة لضمان عدم التأثر بأي أعطال في النظام الأساسي.
3. يتم اختبار إجراءات استعادة البيانات بشكل دوري لضمان فعاليتها في حالات الطوارئ.

❖ إدارة الوصول والتحكم:

يتم تنظيم صلاحيات الوصول إلى أنظمة المعلومات في الجمعية بناءً على طبيعة المهام الموكلة لكل موظف، لضمان حماية الأنظمة والبيانات من أي محاولات للوصول غير المصرح به. وتشمل ضوابط إدارة الوصول ما يلي:

1. منح صلاحيات الوصول للموظفين بناءً على احتياجاتهم الوظيفية، وتقليصها عند الضرورة.
2. يتم إيقاف حسابات الموظفين فور انتهاء فترة عملهم في الجمعية لضمان عدم الوصول غير المصرح به إلى البيانات.
3. مراجعة وتحديث صلاحيات الوصول بانتظام لضمان ملاءمتها مع متطلبات العمل وتطور التهديدات.

❖ استخدام الأجهزة الشخصية:

في حالة السماح باستخدام الأجهزة الشخصية، يتعين على الموظفين الامتثال لمعايير الجمعية لضمان حماية أنظمتها. تشمل هذه المعايير:

1. يجب على الموظفين تثبيت برامج الحماية المناسبة على أجهزتهم الشخصية وتحديثها بانتظام.
2. لا يُسمح بربط الأجهزة الشخصية بشبكة الجمعية إلا بعد الحصول على موافقة مسبقة من إدارة تقنية المعلومات.
3. يجب على الموظفين اتخاذ كل الاحتياطات اللازمة لحماية البيانات والأنظمة عند استخدام أجهزتهم الشخصية.

❖ مكافحة التصيد الاحتيالي والهجمات السيبرانية:

تقوم الجمعية باتخاذ جميع التدابير اللازمة لتوعية الموظفين بمخاطر التصيد الاحتيالي والهجمات السيبرانية. وتشمل هذه التدابير:

1. تنظيم حملات توعية داخلية لتدريب الموظفين على كيفية التعرف على محاولات التصيد والاحتيال.
2. يتعين على الموظفين توخي الحذر عند التعامل مع رسائل البريد الإلكتروني غير الموثوقة أو غير المعروفة.
3. الإبلاغ الفوري عن أي رسائل بريد مشبوهة أو محاولات احتيالية.

❖ التنفيذ والمراجعة:

تخضع هذه اللائحة للمراجعة الدورية من قبل إدارة تقنية المعلومات لضمان مواكبتها للتطورات التقنية والتغيرات التنظيمية. يتم تحديث السياسة وفقًا للحاجة لضمان استمرارية الحماية وتحسين الأداء التشغيلي لأنظمة الجمعية.