

سياسة نظام أمن المعلومات

1. ميثاق سياسة أمن المعلومات

- تلتزم جمعية دبي الخيرية بحماية جميع المعلومات والبيانات التي تقوم بإنشائها، أو معالجتها، أو تخزينها، أو نقلها.
- تهدف الجمعية إلى ضمان سرية المعلومات وسلامتها وتوافرها وفق مبادئ أمن المعلومات المعتمدة.
- تدعم هذه الحماية تحقيق رؤية ورسالة وأهداف الجمعية في مجال العمل الإنساني والخيري.
- تلتزم الجمعية بالامتثال لكافة المتطلبات القانونية والتنظيمية المعمول بها في دولة الإمارات العربية المتحدة.
- تؤكد الإدارة العليا التزامها بتطبيق أمن المعلومات وتحسينه بشكل مستمر.
- تلتزم الإدارة العليا بتوفير الموارد اللازمة لضمان فعالية واستدامة أمن المعلومات.

2. أهداف سياسة أمن المعلومات

تهدف هذه السياسة إلى ما يلي:

- حماية المعلومات من الوصول أو الاستخدام أو الإفصاح غير المصرح به.
- تقليل مخاطر فقدان أو تلف أو تسريب البيانات.
- تحديد الأدوار والمسؤوليات المتعلقة بأمن المعلومات.
- رفع مستوى الوعي بأمن المعلومات لدى جميع الموظفين والمتعاقدين.
- دعم استمرارية الأعمال والخدمات الحيوية للجمعية.

3. نطاق التطبيق

تُطبق هذه السياسة على:

- جميع موظفي الجمعية والمتعاقدين والأطراف ذات العلاقة.
- جميع أنظمة، وتقنيات المعلومات، والأجهزة، والشبكات.

- جميع أنواع المعلومات، سواء كانت ورقية أو إلكترونية أو شفوية.
- جميع الأصول المعلوماتية ضمن نطاق نظام أمن المعلومات.

4. مسؤوليات الإدارة العليا

تلتزم الإدارة العليا في جمعية دبي الخيرية بما يلي:

- الامتثال لكافة القوانين واللوائح المتعلقة بأمن المعلومات وحماية البيانات.
- متابعة متطلبات الجهات التنظيمية وأصحاب المصلحة.
- تشجيع الموظفين ومدراء الإدارات على الالتزام بالسياسة.
- تحميل كل طرف مسؤولياته تجاه تطبيق نظام أمن المعلومات.
- اعتبار أي مخالفة للسياسة مخالفة تنظيمية تستوجب الإجراءات المناسبة.
- توفير الموارد اللازمة لضمان فعالية واستدامة نظام أمن المعلومات.
- متابعة وتحسين النظام بشكل مستمر.

5. مسؤوليات تقنية المعلومات

تلتزم إدارة تقنية المعلومات في جمعية دبي الخيرية بما يلي:

- تطبيق وضمان الالتزام بسياسة أمن المعلومات والمعايير المعتمدة.
- حماية الأنظمة والأجهزة والشبكات من التهديدات الأمنية والفيروسات والبرمجيات الخبيثة.
- إدارة الوصول إلى المعلومات وفق مبدأ الحد الأدنى من الصلاحيات والتأكد من تحديث كلمات المرور دوريًا.
- تنفيذ إجراءات النسخ الاحتياطي واستمرارية الأعمال واختبار خطط استعادة البيانات بشكل دوري.
- مراقبة الأنظمة والشبكات واكتشاف أي نشاط غير مصرح به والاستجابة للحوادث الأمنية.
- تحديث الأنظمة والتطبيقات وتثبيت التصحيحات الأمنية بشكل دوري.
- توثيق الحوادث وتحليلها واتخاذ الإجراءات التصحيحية لمنع تكرارها.
- تقديم التوعية والدعم الفني للموظفين فيما يخص تطبيق ضوابط أمن المعلومات.

6. مسؤوليات الموظفين

يتحمل جميع الموظفين في جمعية دبي الخيرية المسؤولية عن:

- الالتزام بسياسات وضوابط أمن المعلومات المعتمدة.
- الحفاظ على سرية المعلومات وعدم مشاركتها مع أي طرف غير مخوّل.
- استخدام كلمات المرور والبيانات الخاصة بالوصول بشكل آمن.
- الإبلاغ الفوري عن أي حوادث أو شكاوى تتعلق بأمن المعلومات.
- المشاركة في برامج التوعية والتدريب المتعلقة بأمن المعلومات.
- تطبيق الإجراءات المتبعة لحماية الأجهزة والبيانات أثناء العمل سواء داخل المؤسسة أو عن بعد.

7. مبادئ أمن المعلومات

تعتمد الجمعية على المبادئ الأساسية التالية:

- السرية: (Confidentiality) منع الوصول غير المصرح به إلى المعلومات.
- السلامة: (Integrity) ضمان دقة واكتمال المعلومات وعدم تعديلها دون تصريح.
- التوافر: (Availability) ضمان توفر المعلومات والأنظمة عند الحاجة.

8. تصنيف المعلومات

تصنّف المعلومات في الجمعية إلى:

- معلومات عامة
- معلومات داخلية
- معلومات سرية
- معلومات شديدة السرية

ويجب التعامل مع كل فئة وفق الضوابط والإجراءات المعتمدة، بما يضمن مستوى الحماية المناسب لكل تصنيف.

9. التحكم في الوصول

تلتزم الجمعية بما يلي:

- منح الصلاحيات وفق مبدأ الحد الأدنى من الصلاحيات.
- استخدام كلمات مرور قوية وتحديثها بشكل دوري.
- منع مشاركة بيانات الدخول بين المستخدمين.
- مراجعة صلاحيات الوصول بشكل دوري أو عند تغيير المهام الوظيفية.

10. أمن الأجهزة والأنظمة

تشمل ضوابط أمن الأجهزة والأنظمة ما يلي:

- حماية الأجهزة من الفيروسات والبرمجيات الخبيثة.
- تحديث الأنظمة والتطبيقات بشكل دوري.
- منع تثبيت أو استخدام برامج غير مصرح بها.
- حماية الأجهزة المحمولة ووسائل التخزين.

11. أمن الشبكات

تلتزم الجمعية بتأمين شبكاتها من خلال:

- استخدام جدران الحماية وأنظمة كشف ومنع الاختراق.
- تأمين الشبكات اللاسلكية.
- مراقبة استخدام الشبكة واكتشاف أي أنشطة غير مصرح بها.
- فصل الشبكات الحساسة عند الحاجة.

12. النسخ الاحتياطي واستمرارية العمل

تشمل متطلبات النسخ الاحتياطي واستمرارية العمل:

- إجراء نسخ احتياطية دورية للبيانات والمعلومات الهامة.
- حفظ النسخ الاحتياطية في أماكن آمنة ومحمية.
- اختبار خطط استعادة البيانات واستمرارية الأعمال بشكل دوري.
- ضمان توفر المعلومات والخدمات في حالات الطوارئ.

13. إدارة حوادث أمن المعلومات

في حال وقوع أي حادث أمني، يتم:

- الإبلاغ الفوري عن الحادث للجهة المختصة.
- توثيق الحوادث وتحليل أسبابها وآثارها.
- اتخاذ الإجراءات التصحيحية والوقائية لمنع تكرارها.
- متابعة فعالية الإجراءات المتخذة.

14. التوعية والتدريب

تلتزم الجمعية بـ:

- توعية الموظفين بمخاطر أمن المعلومات ومسؤولياتهم.
- تنفيذ برامج تدريبية دورية في مجال أمن المعلومات.
- تعزيز ثقافة أمن المعلومات على مستوى الجمعية.

15. الالتزام والمساءلة

- الالتزام بهذه السياسة إلزامي لجميع العاملين والأطراف ذات العلاقة.
- أي مخالفة لأحكام هذه السياسة قد تعرض صاحبها للمساءلة وفق الأنظمة واللوائح المعمول بها في الجمعية.

16. المراجعة والتحديث

تتم مراجعة هذه السياسة بشكل دوري أو عند حدوث تغييرات تقنية أو تنظيمية أو تشريعية، ويتم تحديثها بما يضمن استمرار ملاءمتها وفعاليتها.

اعداد

وميض سامي عثمان

بتاريخ: 2025-12-24



تدقيق ومراجعة

دكتور محمد سعيد

بتاريخ: 2025-12-26



اعتماد المدير التنفيذي

أحمد إبراهيم السويدي

بتاريخ: 2025-12-29

