سياسة أمن المعلومات

التصنيف: داخلي

رقم الإصدار: 1.0
تاريخ الإصدار: 2023/10/25

سجل الاعتماد والتعديلات

سياسة أمن المعلومات

الإصدار	التاريخ	وصف التعديل	الإعداد	المراجعة	الاعتماد
1	2023/10/15	استحداث	قسم تقنية المعلومات	مكتب الجودة	المدير العام

1 المقدمة

1.1 تدرك جمعية بيت الخير أهمية أمن المعلومات، وبالتالي فهي ملتزمة بتزويد المتعاملين وأصحاب المصالح والشركاء والموظفين ببيئة آمنة لمعالجة المعلومات، وتعتزم الجمعية تحقيق الأمن

لأصول المعلومات الخاصة بها استناداً إلى المبادئ التأسيسية الثلاثة لأمن المعلومات "السرية والسلامة والتوافر".

2 نطاق التطبيق

2.1 تنطبق هذه السياسة على كافة الأطراف المعنية في جمعية بيت الخير.

3 الأهداف

3.1 تهدف هذه السياسة إلى تحديد المبادئ الأساسية لحماية جميع أصول المعلومات جمعية بيت الخير، وتوعية كافة الأطراف المعنية لدى الجمعية بالتهديدات الأمنية المحتملة والمخاطر المرتبطة بها.

4 المصطلحات والتعاريف

م	المصطلح	التعريف
.1	**الجمعية:**	جمعية بيت الخير
.2	**سياسة أمن المعلومات**	تعهد والتزام من جمعية بيت الخير بتزويد المتعاملين وأصحاب المصالح والشركاء والموظفين ببيئة آمنة لمعالجة المعلومات.
.3	**أمان البنية الأساسية**	الأمان الذي يشمل البنية الأساسية التكنولوجية الكاملة للجمعية، بما في ذلك أنظمة الأجهزة والبرامج.
.4	**أمان التطبيقات**	النُهج والإجراءات والأدوات وأفضل الممارسات التي يتم وضعها لحماية التطبيقات وبياناتها.
.5	**إدارة الثغرات الأمنية**	هي العملية التي تجريها الجمعية لتحديد وتقييم ومعالجة الثغرات الأمنية في نقاط النهاية والبرامج والأنظمة الخاصة بها.
.6	**الاستجابة للحوادث**	خطة الجمعية للاستجابة لتداعيات أي هجوم عبر الإنترنت أو تسرب للبيانات أو حدث تخريبي آخر ومعالجته وإدارته.

5 المراجع

- مواصفة نظام إدارة الحوكمة المؤسسية ISO 37000
- مواصفة نظام إدارة أمن المعلومات ISO 27001

6 بيان سياسة أمن المعلومات

6.1 تلتزم جمعية بيت الخير بتأمين سرية المعلومات المتعلقة بالأعمال اليومية وسلامتها وتوافرها، لذلك يعد أمن المعلومات، والأصول الأخرى، من العوامل الأساسية لنجاح عمل جمعية بيت الخير.

6.2 تعد هذه السياسة العامة لأمن المعلومات عنصراً أساسياً من عناصر الإطار العام لإدارة أمن المعلومات في جمعية بيت الخير والتي يتوجب أخذها بعين الاعتبار على قدم المساواة مع سياسات جمعية بيت الخير المحددة والمفصلة الخاصة بأمن المعلومات وإجراءاته ومعاييره وإرشاداته.

6.3 إن من شأن التقيد بهذه السياسة أن يساعد على حماية البيانات والمعلومات الخاصة بجمعية بيت الخير وحماية المتعاملين معها من التهديدات المتعلقة بأمن المعلومات، سواء أكانت داخلية أم خارجية، متعمدة أم غير مقصودة .

6.4 من المسلم به أنه ستكون هناك حاجة إلى سياسات وإجراءات مفصلة، تلتزم جمعية بيت الخير بتنفيذها بالكامل.

7 المبادئ الأساسية:

تدرك جمعية بيت الخير أن أمن المعلومات يتوقف على أمن ثلاثة عناصر تنظيمية أساسية، وهي: الأشخاص، والعمليات، والتقنيات، ولذا يتعين في كافة عمليات جمعية بيت الخير التقيد بالمبادئ العامة الموضوعة.

وحيث اقتضى الأمر فقد جرى تفصيل هذه المبادئ أدناه لتوفير الأساس الذي يصيغ جمعية بيت الخير بناءً عليه اتجاه الأمن وسيره :

1. تأمين سرية وتكامل وتوافر المعلومات، وأصولها.
2. تصميم وتطبيق نظام لإدارة أمن المعلومات وفق أفضل الممارسات العالمية، والقوانين المحلية النافذة والتزامات الجمعية نحو المتعاملين معها من موردين ومتعاملين .
3. وضع أهداف نظام إدارة أمن المعلومات بما يتناسب مع رؤية الجمعية وتطلعاتها ومراجعة هذه الأهداف وتحديثها باستمرار
4. تلبية المتطلبات التنظيمية والقانونية والتشريعية لدولة الإمارات العربية المتحدة.
5. الإبلاغ عن كافة ما يشتبه به من انتهاكات لأمن المعلومات والتحقيق فيها.
6. توفير التدريب المناسب على أمن المعلومات لكافة الموظفين، ونشر الوعي بينهم بهذا الخصوص.
7. تصميم الضوابط والإجراءات الملائمة لدعم تنفيذ هذه السياسة الخاصة بأمن المعلومات.
8. ضمان أن يكون كافة أصحاب المصلحة مسؤولين عن تنفيذ السياسات والإجراءات الأمنية الخاصة كل منهم ضمن مجال عمله، والإشراف على التزام أعضاء الفرق الخاصة بهم .
9. الاستمرار بتطوير أمن المعلومات من خلال تنفيذ الإجراءات التصحيحية والوقائية .
10. إعداد خطط استمرار العمل واختبارها وتطويرها بأسلوب عملي بناءً على احتياجات العمل.
11. مراجعة هذه السياسة سنوياً للتحقق من أنها تفي بالأغراض المرجوة منها.

8 تعليمات عمل أمن المعلومات

حفاظاً على سلامة وأمن المعلومات في جمعية بيت الخير، فيجب على كافة مدراء الإدارات ورؤساء الأقسام وكافة موظفي الجمعية اتباع كافة تعليمات أمن المعلومات، والتي هي على النحو التالي:

1. لا تقم بفتح روابط مجهولة وغير متوقعة من رسائل بريد الكتروني حتى لو كنت تعرف مرسلها، يمكن الاستعانة بأحد موظفي قسم تقنية المعلومات للتأكد من الرابط قبل الضغط عليه.

2. لا تقم بتنزيل ملفات دون التأكد أنها موثوقة، يمكن التأكد من ذلك في أغلب الأحيان إذا كنت تعرف المرسل، وكنت تتوقع منه أن يرسل هذه الملفات، مع ضرورة فحص المرفقات ببرنامج مكافح الفيروسات أولا.

3. في كل الحالات يمكن الاستعانة بموظفي قسم تقنية المعلومات عند الشك في أي مرفق أو رابط الكتروني مشتبه يصلك.

4. تذكر أن الضرر عند الضغط على رابط مشبوه، أو تنزيل ملف مشبوه لا يقتصر على جهازك وانما قد يمتد ليشمل أجهزة أخرى أو حتى كامل شبكة الجمعية ويعرض لخطر المساءلة القانونية عن الضرر الناشئ عنه.

5. لا يسمح بتصفح الانترنت في غير الأغراض المخصصة لنطاق المهام المكلف بها أي من الموظف أو المتطوع، ويشمل ذلك أجهزة الكمبيوتر واللاب توب والأجهزة الذكية المتصلة بواي فاي الجمعية.

6. لضمان التصفح الآمن في شبكة الانترنت لا تقم بالضغط على روابط إعلانية أو روابط مشبوهة أو لا علاقة لها بالعمل.

7. لا يسمح لمستخدم الشبكة المحلية الالكترونية الخاصة بالجمعية بالدخول إلى أي جزء منها لا يتعلق بمهام عمل الموظف/المتطوع، وفي حال عمل ذلك سيعرض نفسه للإجراءات الإدارية.

8. تأكد من تطبيقك لسياسة كلمات المرور المطبقة في الجمعية، وعدم وضع كلمات مرور سهل توقعها، مثل اسمك، تاريخ ميلادك،... ABC1234 الخ.

9. لا تقم بمشاركة كلمات المرور الخاصة بك مع أي كان، ولا حتى لموظفي قسم تقنية المعلومات، ما لم يتم طلب ذلك رسمياً من إدارة قسم تقنية المعلومات ولغرض محدد.

10. قم بتغيير كلمة المرور الخاصــة بك من فترة لأخرى، إن كلمة المرور بمثابة الدخول المعرف لشــخصـيتك عند اسـتخدام النظام، وأنت مسـؤول عن جميع المعاملات التي تسـجل باسـم معرفك وكلمة المرور الخاصـة بك طوال فترة العمل، وسـيتم الطلب منك تغيير كلمة المرور كل ثلاث أشهر بشكل دوري.

11. يفضل عدم تخزين كلمات المرور تلقائيا في متصفحات الموقع مثل خدمة" الإكمال التلقائي " أو" تذكرني"، كذلك تذكر أن كلمات المرور تحفظ ولا تكتب أو تخزن.

12. قبل مغادرتك للعمل احرص على إطفاء جهازك، وأثناء العمل وقبل مغادرتك المكتب لأي سبب احرص على تأمين جهازك بالضغط على علامة الويندوز مع حرف"L " .

13. عند استخدامك لبرامج العمل من خارج مقر العمل تأكد من التالي:

a. تأكد أنك تسـجل الدخول من جهازك الشـخصـي، وليس من جهاز عام مثل الأجهزة الموجودة في المكتبات العامة أو المقاهي أو غيرها.

b. كن حريصا عند تسجيل بيانات الدخول بحيث لا تتعرض بياناتك للسرقة والتلصص من أشخاص آخرين.

c. لا تســتخدم شــبكات الواي فاي العامة عند تســجيل الدخول للبرامج الذكية، وإنما يمكن اسـتخدام شـبكات الواي فاي الشـخصـية أو شـبكات الواي فاي المقدمة من مزودي الخدمة (اتصالات و دو) بشكل مباشر، أو من باقات البيانات الشخصية.

d. لا تقم بتخزين أي ملفات أو تقارير تتعلق بالعمل في غير أجهزة العمل، إلا في حدود جلسـة الاسـتخدام الخاصـة بك، وعند تسـجيل الخروج أو انتهاء الجلسـة تأكد من حذفك لكل تلك الملفات أو التقارير إن وجدت عن طريق حذف ذاكرة التخزين المؤقتة أو خيار" Clear Cashe " .

14. يمنع استخدام أو توصيل أي وحدات تخزين خارجية (فلاش ميموري، هارد ديسك خارجي) بأي جزء من مكونات الموارد الالكترونية بالجمعية، ويشمل ذلك توصيلها بأجهزة الكمبيوتر أوالكمبيوتر المحمول أو غيرها، وذلك منعاً لانتشــار الفيروســات أو برامج التجســس أو أي ملفات ضـارة أخرى.

15. عند انتهائك من جلسة العمل احرص على الخروج بطريقة نظامية من البرنامج العام والبرنامج الذكي والبريد الالكتروني وكذلك أي برامج أخرى محمية.

16. يجب عدم مشــاركة أي بيانات أو معلومات أو ملفات أو تقارير الكترونية أو أي مرفقات أو مســتندات متعلقة بالعمل الا للأشــخاص أو الجهات المخولين فقط بذلك من إدارة الجمعية،

بالنسبة لمشاركة المعلومات أو البيانات أو الملفات للجهات الخارجية يجب التأكد من وجود موافقة رسمية من إدارة الجمعية بمشاركة تلك المعلومات أو المستندات قبل ارسالها.

17. تشمل سياسة أمن المعلومات كذلك جميع أنواع المعاملات المتعلقة بالعمل، سواء كانت الكترونية أو ورقية أو شفوية أو غيرها، احرص على عدم كشف الأوراق أو المعاملات الرسمية أو المعلومات لدى الأشخاص أو الجهات غير المخولة بذلك.

18. قم بحفظ نسخ احتياطية من ملفاتك الخاصة بالعمل الموجودة في جهازك الخاص بالعمل، في مساحة التخزين السحابية المخصصة لك من قسم تقنية المعلومات بشكل دوري ومستمر، كإجراء احتياطي بحسب أهمية البيانات والملفات.

19. يجب على المسؤول مراجعة صلاحيات موظفيه الالكترونية من خلال "تقرير الصلاحيات"، والتأكد من كونها تلائم مهام العمل المطلوبة من الموظف دون زيادة أو نقصان، ومخاطبة قسم تقنية المعلومات عند الحاجة لإضافة أو تغيير أو حذف أي من الصلاحيات حسب مهام العمل المنوط بها.

20. لا تقم بمشاركة أي كلمات مرور عن طريق الأنظمة العامة مثل نظام المهام أو نظام مساحة العمل أو الملفات المشتركة، ولا عن طريق البريد الالكتروني المرسل لأكثر من شخص

21. يحق لقسم تقنية المعلومات تغيير سياسة كلمات المرور إذا اقتضت الضرورة، كما يحق له تغيير كلمة المرور لموظف / موظفين محددين مع إبلاغهم بذلك.

22. لا تقم بمحاولة تنزيل أو تثبيت أو تشغيل أي برنامج سواء عبر روابط من الإنترنت، أو من البريد الالكتروني، أو غيرها، تواصل مع قسم تقنية المعلومات للتأكد مسبقا من إمكانية ذلك.

23. في حال اشتبهت في أي خرق الكتروني محتمل لأمن المعلومات، فيرجى إبلاغ قسم تقنية المعلومات فوراً.

24. يجب على رؤساء وحدات العمل التأكد من قيامهم ومرؤوسيهم باتباع كافة بنود سياسة الموارد الالكترونية بالجمعية، لضمان الحفاظ على موارد الجمعية التقنية، يمكن الحصول على نسخة من سياسة الموارد من البرنامج العام، صلاحية الطلبات العامة.

25. يقوم قسم تقنية المعلومات ضمن خطة سنوية معدة مسبقاً بفحص الأجهزة الالكترونية لوحدات العمل المختلفة.

26. في حال نقل الموظفين والمتطوعين على قسم الموارد البشرية افادة قسم تقنية المعلومات عن التنقلات الدائمة والمؤقتة وذلك للإجراءات التقنية المصاحبة لذلك وكذلك الحال عند

استقالة الموظف على الموارد البشرية اخطار قسم تقنية المعلومات مباشرة لإيقاف الخدمات الالكترونية والحسابات الخاصة بالموظف المستقيل.

27. يقر كل الموظفين بأنه يجب الحفاظ على سرية البيانات والمعلومات الخاصة بالجمعية التي قد يطلع عليها الموظف او المتطوع خلال فترة عمله حتى بعد تركه للعمل.

28. يرجى متابعة إرشادات قسم تقنية المعلومات لضمان حسن استخدام الأنظمة بالطريقة المثلى لتحقيق الأهداف التي طورت من أجلها.

29. يتم تطبيق أي قانون أو مرسوم حكومي خاص بسياسة أمن المعلومات داخل الدولة مباشرة دون الحاجة للتحديث على سياسة أمن المعلومات.

إن قسم تقنية المعلومات يسعى جاهدا لتأمين بيئة العمل الكترونيا، ويسعى للحرص على ضمان استمرارية تقديم جميع الخدمات الالكترونية، ومع ذلك فإن مسؤولية أمن المعلومات هي مسؤولية مشتركة مع جميع مستخدمي الشبكة، وفي سبيل ذلك نتطلع لالتزام الجميع وتعاونهم، للوصول إلى الاستخدام الآمن والأمثل للأنظمة وتقديم الخدمة للجمهور بكفاءة ويسر.

9 الالتزام بالسياسة

9.1 أي مخالفة أو خرق لهذه السياسة قد يؤدي إلى إجراءات تأديبية بما يتوافق مع قوانين العمل المتبعة في دولة الإمارات العربية المتحدة وقواعد سلوك الموظفين وأية قوانين أخرى لدولة الإمارات العربية المتحدة مطبقة في هذا السياق.

9.2 في حال عدم وضوح أية مادة في هذه السياسة يتوجب على المستخدمين طلب توضيحات أو مشورة من قسم تقنية المعلومات.

9.3 يحتفظ قسم تقنية المعلومات بحق التحقق من تقيد المستخدمين بهذه السياسة.

9.4 أي استثناءات على هذه السياسة مصحوبة بتبريرات عملية سليمة ستتطلب موافقة من قسم تقنية المعلومات وذلك تبعاً للحالة.

10 المراجعة والتحديث

يتولى قسم تقنية المعلومات بالتنسيق مع مكتب الجودة وكافة الأطراف المعنية في الجمعية مراجعة هذه السياسة أثناء اجتماعات المراجعة الإدارية الدورية وضمان وملاءمتها، وتحديثها عند حدوث تغييرات هامة في الجمعية وكلما دعت الحاجة.

11 النشر

يتولى مكتب المدير العام تعميم السياسة داخلياً.
يتولى قسم تقنية المعلومات نشر نص السياسة على الموقع الإلكتروني للجمعية.