معا للحياة
Together for life

سياسات تقنية المعلومات

بجمعية زمزم الصحية

الإصدار الأول
1445/04/20
2023/11/04

جمعية زمزم الصحية
ZMZM Health Society

إشراف المركز الوطني لتنمية القطاع غير الربحي
تصريح رقم (290)

info@zmzm.org | 9200 33377 | **zmzm.sa**

المحتويات

سياسة الاستخدام المقبول ٣
أولاً: الغرض من السياسة ٣
ثانياً: نطاق السياسة ٣
ثالثاً: عدم الامتثال للسياسة ٣
رابعاً: حقوق الملكية والاستخدام ٣
خامساً: توجيهات أمنية عامة ٤
سادساً: الاستخدام غير المقبول ٤
سابعاً: كلمات المرور ٤
ثامناً: مبادئ استخدام البريد الإلكتروني ٥
تاسعاً: أمن البريد الإلكتروني ٦

سياسة استخدام الأجهزة الشخصية في العمل ٧
أولاً: الغرض من السياسة ٧
ثانياً: نطاق السياسة ٧
ثالثاً: الأجهزة الشخصية المسموح باستخدامها في العمل ٧
رابعاً: عدم الامتثال للسياسة ٧
خامساً: الأعمال المصنفة كأعمال للجمعية ٧
سادساً: أمن الجهاز الشخصي ٧
سابعاً: صيانة وإدارة الجهاز الشخصي ٧
ثامناً: الاتصال بالشبكات اللاسلكية التابعة للجمعية ٨
تاسعاً: الاتصال بالشبكات اللاسلكية الأخرى ٨
عاشراً: تراخيص البرامج ٨

الاعتمادات ٨

سياسة الاستخدام المقبول

أولاً: الغرض من السياسة

١. الغرض من هذه السياسة هو وضع الأطر والقواعد العامة للاستخدام المقبول للأجهزة والبرامج في جمعية زمزم.
٢. هذه القواعد وضعت لحماية المستخدمين وجمعية زمزم في نفس الوقت.
٣. إن الإخلال بقواعد الاستخدام المقبول قد يعرض الجمعية لمخاطر تشمل هجوم الفيروسات، اختراق الشبكة أو الأنظمة، ومشاكل قانونية أخرى.

ثانياً: نطاق السياسة

١. تنطبق هذه السياسة على كل من:
- الموظفون بدوام كامل.
- الموظفون بدوام جزئي.
- المتطوعون.
- المتعاقدون الذين لهم صلاحية استخدام الأجهزة أو الأنظمة التابعة لجمعية زمزم.

٢. يستثنى من هذه السياسة:
- يستثنى فريق تقنية المعلومات من منع تنصيب البرامج على أجهزة الجمعية.
- يستثنى فريق تقنية المعلومات من منع إجراء الصيانة على أجهزة الجمعية أو نقلها لمراكز صيانة خارجية.
- يستثنى فريق تقنية المعلومات من تغيير إعدادات الشبكة وفصل وتوصيل كيابل الشبكة والتوصيلات الأخرى.

٣. تغطي هذه السياسة ما يلي:
- أجهزة الحاسب الآلي بجميع أنواعها.
- الأجهزة الإلكترونية الأخرى والملحقة.
- البرامج والأنظمة.
- أنظمة التشغيل المختلفة.
- وسائط تخزين البيانات.
- حسابات المستخدمين على الشبكة وعلى الأنظمة السحابية.
- تصفح الإنترنت.
- حسابات VPN

ثالثاً: عدم الامتثال للسياسة

عدم الامتثال للقواعد والتعليمات الواردة بالسياسة يعرض الموظف لتطبيق الجزاءات الواردة بلائحة تنظيم العمل ويحق للجمعية في تحريك الدعوى القضائية للمطالبة بالتعويض.

رابعاً: حقوق الملكية والاستخدام

بشكل عام فإن جميع الأجهزة والبيانات والمعلومات التي يتم إنتاجها في جمعية زمزم وكذلك الملفات الإلكترونية المخزنة في أجهزة الجمعية هي بمثابة أصول تملكها جمعية زمزم، ولا يجوز التصرف فيها بحذف أو نقل أو مشاركة إلا في حدود الصلاحية أو بإذن من جمعية زمزم.

١,٤ حفظ البيانات والملفات

١. جميع البيانات والمعلومات التي يتم إنتاجها وتداولها لصالح جمعية زمزم يجب أن تخزن كالتالي:
- بيانات خام تخزن في الأنظمة الإلكترونية التي تديرها جمعية زمزم (على سبيل المثال وليس الحصر: بيانات المستفيدين، بيانات الداعمين، بيانات طلبات العلاج الخيري، بيانات مالية وفواتير).
- بيانات ومعلومات يتم تخزينها على شكل ملفات وتخزن إما في OneDrive الخاص بالموظف على Office 365 أو على الفريق الخاص بالإدارة على Microsoft Teams.

٢. لا يجوز تخزين الملفات على وسائط تخزين شخصية أو على خدمات سحابية شخصية مثل Google Drive أو ما شابهها، أو على جهاز الحاسوب في غير ما تم تحديده (كسطح المكتب مثلا ما لم يتم مزامنة سطح المكتب).

٢,٤ صلاحيات الدخول على البيانات ومشاركتها

١. قائمة صلاحيات الدخول Access Control List (ACL) موجودة على ملف إكسل ACL.xlsx

٢. للاستفسارات حول صلاحيات الدخول، أو طلب صلاحية دخول لنظام أو الاطلاع على ملفات معينة فضلا التواصل مع مدير تقنية المعلومات.

٣,٤ الصيانة والصيانة الوقائية

١. يتم صيانة البيانات والأجهزة الحاسوبية وملحقاتها بشكل دوري في آخر ربع من كل سنة. ولطلب صيانة طارئة فضلا رفع طلب في نظام الدعم الفني.
٢. المسؤول عن صيانة أجهزة الجمعية هم أخصائي الدعم الفني واخصائي الشبكة، ولا يجوز للموظف الاستعانة بغيرهم لإجراء عمليات صيانة على أجهزة الجمعية، أو نقلها إلى محلات صيانة خارجية.
٣. يحق لموظفي تقنية المعلومات الاستعانة بفنيين من خارج الجمعية للعمل تحت إشرافهم في الحالات التي تتطلب الاستعانة بشركات دعم خارجي.

خامساً: توجيهات أمنية عامة

١. يسمح للموظف بالاطلاع على بيانات الجمعية التي يحتاجها لأداء عمله بالشكل المكلف به، ولا يسمح له بالاطلاع على أي بيانات أخرى خلاف ذلك إلا بموافقة مسبقة من صاحب الصلاحية.
٢. يجب أن تكون جميع أجهزة الحاسب الآلي محمية بكلمة مرور، حتى الأجهزة في الأماكن العامة مثل غرف الاجتماعات.
٣. جميع الأجهزة يفعل عليها شاشة توقف تعمل بعد ٥ دقائق من ترك الجهاز، وتتطلب استخدام كلمة مرور لتجاوزها.
٤. لا يحق للموظف التحدث باسم جمعية زمزم في أي من وسائل التواصل الاجتماعي إلا بتكليف من الجمعية، ويجب على الموظف أن يوضح عند إدلاء أي بيانات أو تصريح بأن ذلك شخصي وغير صادر عن الجمعية.
٥. يمنع تخزين البيانات على وسائط تخزين قابلة للإزالة (ذاكرة فلاش مثلا أو قرص صلب محمول) بسبب قابلية تلفها أو ضياعها أو سرقتها. ويستعاض عن ذلك باستخدام وسائط التخزين السحابية التي تسهل نقلها ومشاركتها (حسب صلاحيات الدخول على البيانات ومشاركتها).

سادساً: الاستخدام غير المقبول

جميع الأعمال التالية غير مقبولة بشدة:

١. انتهاك حقوق النشر أو الماركات المسجلة أو أية حقوق ملكية فكرية، بما في ذلك –وليس مقتصراً على– البرامج المقرصنة أو استخدام الصور بدون ترخيص.
٢. الدخول على بيانات الجمعية أو أنظمتها لهدف لا يتعلق بإنجاز أعمال الجمعية.
٣. إدخال برامج ضارة أو خبيثة لأجهزة الجمعية أو لأجهزة موظفي الجمعية.
٤. استخدام برامج لتجاوز أنظمة الحماية أو كسرها.
٥. استخدام أجهزة الجمعية أو أنظمتها لأغراض شخصية أو تجارية خاصة.
٦. استخدام أجهزة الجمعية في الألعاب أو الترفيه خلال أو خارج ساعات العمل.
٧. مشاهدة أو استعراض مواد مخلة من خلال أجهزة الجمعية أو شبكتها الحاسوبية.
٨. استخدام تقنية الجمعية أو شعارها أو نماذجها للقيام بأعمال احتيال.
٩. تقديم ضمانات أو خطابات ضمان باسم الجمعية ما لم تكن مكلفاً بذلك.
١٠. التسبب في حدوث خرق أو تعمد خرق إجراءات أمن الجمعية.
١١. تعطيل اتصال الشبكة.
١٢. المحاولات غير المصرح بها لاعتراض البيانات من خلال الشبكة.
١٣. التحايل على الإجراءات الأمنية أو محاولة تجاوز إجراءات المصادقة على المستخدم (اسم المستخدم وكلمة المرور).
١٤. أي محاولة لتعطيل أعمال الجمعية سواء داخليا أو افتراضيا.
١٥. تسريب البيانات الشخصية للموظفين داخل أو خارج الجمعية.
١٦. تعطيل أجهزة الجمعية عن طريق توصيلها بشكل خاطئ عمداً أو فصلها عن الشبكة.

سابعاً: كلمات المرور

١,٧ خصائص كلمات المرور

تماشيا مع متطلبات أمن المعلومات فإن كلمة المرور يجب أن تكون على النحو التالي:

١. تكون كلمة المرور من ٨ حقول فأكثر، وتحتوي على حرف إنجليزي واحد كبير على الأقل، وحرف إنجليزي صغير واحد على الأقل، ورمز واحد على الأقل.
٢. يجب تغيير كلمة المرور كل ٩٠ يوما، ولا يجوز استخدام آخر ٣ كلمات مرور.
٣. تجنب استخدام كلمات مرور ضعيفة مثل الأرقام، أو الأحرف المكررة أو المتسلسلة مثلا ١٢٣٤٥٦، أو المعلومات الشخصية كتاريخ الميلاد أو أسماء الأبناء، أو معلومات معروفة مثل اسم الجمعية أو عنوان أو رقم هاتفها، وغير ذلك.

٢,٧ تنبيهات بخصوص كلمات المرور

١. لا تكتب كلمة المرور على الورق، أو في ملاحظة عادية على الجوال.
٢. يمكن استخدام برامج حفظ كلمات المرور في الجوال فقط إذا كانت مشفرة ومقفلة بشكل افتراضي.
٣. تغيير كلمة المرور يجب أن يتم من خلال أجهزة الجمعية في داخل الجمعية (في الوقت الحالي) لدواعي أمنية.
٤. لا تشارك كلمة المرور باستخدام البريد الإلكتروني أو الرسائل النصية بأي وسيلة كانت، حتى لو كانت للحسابات المشتركة (مثل غرف الاجتماعات).

٣,٧ المسؤولية عن الحساب والحسابات المشتركة

١. الموظف مسؤول بشكل كامل عن حسابه في جمعية زمزم وكلمة المرور الخاصة به، ولا يجوز له أن يشاركها مع أي موظف آخر أو مع أي كان. وهو المسؤول بشكل مباشر عن كل ما يصدر عن حسابه.
٢. لا يحق للموظف استخدام حساب موظف آخر للقيام بأي عمل بدون إذن رسمي.
٣. بعض الحسابات مشتركة ويمكن للجميع استخدامها، مثل حسابات غرف الاجتماعات، أو حسابات غرف خدمات الشاي، ويمكن للجميع استخدامها حسب الحاجة فقط.
٤. في حال تم تسريب أو انكشاف كلمة المرور فيجب على الموظف أولا تغيير كلمة المرور فوراً، ثم التواصل مع رئيس قسم الشبكة والدعم الفني في إدارة تقنية المعلومات، على ألا يتجاوز الوقت بين التسريب وإخطار قسم الشبكة والدعم الفني عن ساعتين.

ثامناً: مبادئ استخدام البريد الإلكتروني

البريد الإلكتروني هو الوسيلة الرسمية للتواصل بين منسوبي الجمعية بعضهم ببعض. ويستخدم بشكل أساسي للمساعدة في إنجاز الأعمال والمهام المتعلقة بأعمال الجمعية.

١,٨ مراسلة جهات أو افراد خارجيين

١. حيث إن البريد الإلكتروني لجمعية زمزم يعطي صفة رسمية عند مراسلة جهات وأفراد خارجيين، فيمكن استخدام البريد الإلكتروني وعنوانك البريدي الرسمي التابع للجمعية لمراسلة جهات وأفراد آخرين ليسوا من منسوبي الجمعية، ولكن يجب أن يكون ذلك بهدف إنجاز مهام وأعمال الجمعية فقط، ولا يجوز استخدامه لإنجاز أعمال شخصية أو خاصة.

٢,٨ الرسائل الجماعية

١. لا يجوز استخدام بريد الجمعية لإرسال رسائل جماعية يمكن أن تصنف بأنها "رسائل غير مرغوب بها" أو "مزعجة" أو "SPAM"، ومن الممكن أن يسبب هذا الفعل إلى وضع بريد الجمعية في القائمة السوداء، مما يتسبب في توجيه جميع رسائل الجمعية إلى صندوق البريد غير الهام عند مراسلة جهات أخرى.
٢. لا يجوز أيضا إرسال رسائل بكميات كبيرة لأفراد أو جهات لم تطلب هذه الرسائل، ولا يجوز إرسال رسائل بريد إلكتروني لطلب تبرعات بشكل جماعي وبكميات كبيرة. جميع هذه التصرفات تضر بسمعة الجمعية وتسبب مشاكل في استخدام البريد الإلكتروني.

٣,٨ إعادة توجيه البريد الإلكتروني

١. في العادة يتم إعادة توجيه رسالة إلكترونية لزميل في العمل، أو رئيس بهدف الاطلاع، أو المشورة، أو غير ذلك. قبل إعادة توجيه أي رسالة إلكترونية عليك أولا أن تنتبه إلى حساسية المحتويات، فربما من غير المناسب مشاركة الرسالة مع آخرين.
٢. في حال أعددت رسالة وترغب في سريتها أو منع إعادة توجيهها فيجب أن تحدد هذا الخيار في برنامج البريد الإلكتروني قبل إرسال الرسالة لمنع طباعتها أو إعادة توجيهها.

٤,٨ القوائم البريدية

١. جميع البيانات للمستفيدين والداعمين وغيرهم ممن يتعامل مع جمعية زمزم هي حق حصري للجمعية ولا يجوز استخدامها إلا بإذن رسمي من الجمعية. كما لا يجوز بيعها أو نشرها أو نسخها لأي غرض وبأي وسيلة.
٢. القائمة البريدية التي تضم جميع موظفي الجمعية هي للاستخدام الحصري داخل الجمعية ولا يجوز إعطاء العنوان البريدي لطرف خارجي، كما لا يجوز استخدامها لإرسال أمور شخصية أو أمور لا تتعلق بالعمل الذي يتطلب نشر

معلومات بين افراد الجمعية. لطلب السماح باستخدام القائمة البريدية الخاصة بجميع موظفي زمزم الرجاء طلب توجيه بريد إلكتروني إلى مدير تقنية المعلومات توضح فيه مبررات استخدام القائمة البريدية.

٥,٨ الرقابة على البريد الإلكتروني

في الأحوال العادية فإنه لا يتم فرض الرقابة على رسائل البريد الإلكتروني للموظفين، ولكن قد يتم تفحص رسائل البريد الإلكتروني لأي موظف – بعد موافقة الإدارة – في حالات الاشتباه بإساءة الاستخدام، أو في حالات التحقيقات الأمنية.

تاسعاً: أمن البريد الإلكتروني

١,٩ الرسائل المشتبه بها

١. ينبغي الحذر عند تلقي رسائل بريد إلكتروني من خارج الجمعية (وأحيانا تبدو أنها من داخل الجمعية).
٢. في حال تلقيت رسالة مشبوهة فعليك التواصل فورا مع فريق تقنية المعلومات.
٣. العلامات التالية قد تكون مؤشر على كون الرسالة مشتبه بها (وقد يكون هناك علامات أخرى غير مذكورة هنا):
- المرسل غريب.
- لغة الرسالة غريبة أو غير معتادة.
- بها مرفقات ويطلب فتحها.
- بها رابط أو زر ويطلب الضغط عليه.

٢,٩ المرفقات

١. يفضل عدم إرسال مرفقات مع رسائل البريد الإلكتروني، وبدلا من ذلك يفضل دائما إدراج الملف من OneDrive بحيث يتم إدراج الملف كرابط غالبا. هناك عدة مزايا لعدم إرفاق الملفات بشكل مباشر بالرسالة الإلكترونية.
٢. في حال كانت الرسالة موجهة لجهة أو شخص خارج الجمعية فيمكن إرفاق الملف في الرسالة.
٣. عند استقبال رسالة بها مرفق فيجب التأكد أولا من مصدرها قبل فتح المرفق، والتأكد من أن المرسل قد أرسل لك رسالة وبها مرفق معين.
٤. في جميع الأحوال، الجدول التالي يوضح ما الذي ينبغي فعله بالنسبة لكل نوع ملفات:

نوع الملف	آمن	خطر	يفتح بشروط
Microsoft Word (.doc.,docx)	نعم		احذر من تفعيل الماكرو أو الروابط الخارجية المضمنة
Microsoft Excel (.xls, .xlsx)	نعم		احذر من تفعيل الماكرو أو الروابط الخارجية المضمنة
Microsoft PowerPoint (.ppt, .pptx)	نعم		احذر من الروابط الخارجية المضمنة أو تشغيل الفيديو المضمن في حال تلقيت الملف من مصدر مجهول
Text only (.txt)	نعم		
Rich text format (.rtf)	نعم		آمن، ولكن احذر من الروابط الخارجية المضمنة
Portable Document format (.pdf)	نعم		احذر من الروابط المضمنة
Image files (.gif, .jpg, .png, .bmp)	نعم		
Video files (.mp4, .avi, .swf)	نعم		
HTML files (.htm, .html)		نعم	
Executable Files (.exe)		نعم	
Visual Basic Script (.vbs)		نعم	

سياسة استخدام الأجهزة الشخصية في العمل

أولاً: الغرض من السياسة

١. الغرض من هذه السياسة وضع الأطر العامة لاستخدام الأجهزة الشخصية لأداء أعمال الجمعية سواء في وقت الدوام الرسمي أو خارجه.
٢. هذه القواعد وضعت لضمان حماية الجمعية والمستخدمين من المخاطر المتعلقة بأمن المعلومات، والإخلال بها قد يعرض الجمعية والمستخدمين والبيانات للأخطار المختلفة، أو لمشكلات قانونية أخرى.

ثانياً: نطاق السياسة

١. تنطبق هذه السياسة على:
- الموظفين بدوام كامل.
- الموظفين بدوام جزئي.
- المتعاقدون مع الجمعية.
- المتطوعون.

٢. لا يستثنى من هذه السياسة أحد.

ثالثاً: الأجهزة الشخصية المسموح باستخدامها في العمل

٣. أجهزة الحاسب المحمول (لابتوب).
٤. أجهزة الحاسب المكتبية الشخصية.
٥. الهواتف الذكية.
٦. الأجهزة اللوحية (التابلت).

رابعاً: عدم الامتثال للسياسة

عدم الامتثال للقواعد والتعليمات الواردة بالسياسة يعرض الموظف لتطبيق الجزاءات الواردة بلائحة تنظيم العمل ويحق للجمعية في تحريك الدعوى القضائية للمطالبة بالتعويض.

خامساً: الأعمال المصنفة كأعمال للجمعية

١. الأجهزة الشخصية المستخدمة في العمل لا تخضع بشكل كامل لسياسة الاستخدام المقبول، ولكن يجب مراعاة ما ذكر فيها وفي السياسات الأخرى لتقنية المعلومات أثناء استخدام الأجهزة الشخصية في العمل.
٢. تعتبر جميع الأعمال التي تتعلق بالجمعية أو تحدث باستخدام شبكة الجمعية أو أحد حساباتها الرسمية، تعتبر عمل رسمي للجمعية بغض النظر عن الجهاز المستخدم، أو الوقت الذي أنجزت فيه، وبذلك تخضع هذه الأعمال لسياسات تقنية المعلومات.
٣. الأعمال الأخرى التي لا ينطبق عليها ما ذكر أعلاه، لا تتحمل الجمعية مسؤوليتها، ولا تعتبر أعمال للجمعية.

سادساً: أمن الجهاز الشخصي

١. في حال تم استخدام الأجهزة الشخصية لإنجاز أعمال، فيقع على عاتق صاحب الجهاز مسؤولية ضمان عدم استخدام جهازه لاختراق شبكة الجمعية أو تحميل ملفات ضارة على شبكتها.
٢. يجب تفعيل استخدام كلمة مرور على الجهاز الشخصي المستخدم في العمل، ويجب أن تكون كلمة المرور تتبع تعليمات كلمات المرور في سياسة الاستخدام المقبول.
٣. يجب أن يحتوي الجهاز على حزمة حماية من الفيروسات والاختراقات، أو برمجيات الحماية من الفيروسات على أقل تقدير. وعند الاحتياج يجب التواصل مع إدارة تقنية المعلومات لترتيب حماية الجهاز.
٤. يجب عدم استخدام أي جهاز شخصي تمت كسر حمايته أو يحتوي برمجيات ضارة أو مقرصنة.

سابعاً: صيانة وإدارة الجهاز الشخصي

١. في حال احتاج الجهاز الشخصي المستخدم في العمل للصيانة، يجب أولا التواصل مع الدعم الفني لضمان أمن

وسلامة وخصوصية بيانات الجمعية.

٢. في حال استخدمت الجمعية نظام لإدارة الأجهزة المحمولة MDMS فيجب على من يرغب في استخدام جهازه الشخصي في العمل الانضمام لهذا النظام بالشكل الذي يضمن حفظ ملفات العمل بشكل آمن، وعدم تعارض الاستخدام الشخصي والعمل في نفس الجهاز.

٣. في حال ضياع الجهاز الشخصي الذي يحتوي على بيانات ومعلومات الجمعية يجب على الموظف التواصل مع إدارة تقنية المعلومات في خلال ٤ ساعات على الأكثر من تأكد ضياع أو سرقة الجهاز.

ثامناً: الاتصال بالشبكات اللاسلكية التابعة للجمعية

١. الأجهزة الشخصية أثناء ساعات العمل يمكن أن ترتبط بشبكة الزوار اللاسلكية لإنجاز أعمال الجمعية، وكذلك زوار الجمعية لأغراض العمل يمكنهم الارتباط بهذه الشبكة.

٢. فقط الأجهزة التي تمتلكها الجمعية وتقع تحت مسؤولية إدارة تقنية المعلومات يمكنها الارتباط بشبكة واي فاي Wi-Fi الرسمية للجمعية.

تاسعاً: الاتصال بالشبكات اللاسلكية الأخرى

١. بالنسبة لشبكة المنزل اللاسلكية، فيجب أن يكون الراوتر محمي بكلمة مرور قوية، وكذلك الواي فاي Wi-Fi، ويجب تفعيل جدار ناري شخصي للحماية.

٢. بالنسبة للشبكات العامة (مقاهي، مطاعم، مطارات، فنادق، ...) فيجب استخدام أي برنامج VPN لتشفير الاتصال بالإنترنت وحجب البيانات عن مزود الإنترنت (حتى لو كان لتصفح الإنترنت بشكل شخصي).

٣. في حال احتياج الموظف للاتصال بسيرفرات الجمعية من خارج الجمعية، فيجب عليه استخدام VPN يتم إعداده من قبل إدارة تقنية الجمعية.

عاشراً: تراخيص البرامج

١. يمكن للموظف تنزيل حزمة برامج مايكروسوفت أوفيس ٣٦٥ وكل ما يتبعها، ويستخدم حساب جمعية زمزم لتسجيل الدخول، وبذلك يصبح من حقه استخدام تلك البرمجيات تحت ترخيص الجمعية.

٢. في بعض الحالات يتم تركيب حزمة مكافحة الفيروسات.

٣. في حال ترك الموظف العمل في الجمعية يجب عليه تسجيل الخروج من كل هذه البرامج، أو إزالتها.

الاعتمادات

مدير تقنية المعلومات
هاني بن عبدالعزيز فلمبان

المدير العام
فهد بن محمد الزهراني