الوثيقة الشاملة

إدارة تقنية المعلومات

الاصدار الثالث 2022م

زمزم
zmzm

المحتويات

وثيقة الدليل الشامل إدارة تقنية المعلومات

إعداد:

هاني فلمبان

تاريخ الإصدار

2022/1/1م

الرقم

003

المقدمة

المقدمة:

تعمل إدارة تقنية المعلومات على تحقيق رؤية الجمعية الاستراتيجية، والمساهمة في رفع الكفاءة والفاعلية من خلال توفير التقنيات المناسبة لأعمال الجمعية.

كما تساهم إدارة تقنية المعلومات في تطوير العمليات الداخلية، والمساعدة في نشر المعرفة، وتزويد المعنيين بالمعلومات اللازمة لصنع القرار.

كما يقع على عاتقها حماية بيانات الجمعية وأجهزة الموظفين من الهجمات السيبرانية المختلفة.

ثانياً: التعريفات

يقصد بالكلمات والعبارات التالية المعاني المذكورة مقابل كل منها:

الجمعية	جمعية زمزم للخدمات الصحية التطوعية الخيرية
الإدارة	إدارة تقنية المعلومات
السياسات	الإطار العام والحاكم لأعمال الإدارة
اللائحة	هي بيان تفصيلي للسياسات
الخوادم	أجهزة مركزية تعمل عليها أنظمة حاسوبية تستخدم من قبل مجموعة من الموظفين أو غير الموظفين
الكمبيوتر	جميع أجهزة الحاسب الآلي المكتبية والمحمولة والتابلت والهجين
جهاز شبكة	أجهزة تتصل بها الكمبيوترات وتستخدم لربط الأجهزة داخل دوائر الاتصال، وربط الشبكات بعضها ببعض مثل السويتش والراوتر، كما تشمل الخوادم المركزية المتصلة بها.
أمن المعلومات	الإجراءات والسياسات التي تهدف لحماية البيانات من الضياع أو التلف أو التخريب
الصيانة الوقائية	صيانة استباقية للأجهزة بدون وجود عطل بهدف تحسين الأداء وتلافي الأعطال
ملحقات الكمبيوتر	الطرفيات المرتبطة بالكمبيوتر سلكيا أو لا سلكيا لتؤدي مهمة محددة
الخدمات السحابية	هي خوادم أو أنظمة تشغل بواسطة مراكز بيانات متخصصة تسمح بتشغيل أنظمة إلكترونية وتخزين بيانات الجمعية واسترجاعها حسب احتياجها

2. السياسات

السياسات:

ت	السياسة	أداة تنفيذها
1	سياسة الاستخدام المقبول: وضع الأطر والقواعد العامة للاستخدام المقبول للأجهزة والبرامج في جمعية زمزم.	المراقبة الإلكترونية
2	سياسة استخدام الأجهزة الشخصية في العمل: الأطر العامة لاستخدام الأجهزة الشخصية لأداء أعمال الجمعية سواء في وقت الدوام الرسمي أو خارجه	المراقبة الإلكترونية
3	سياسة أمن المعلومات: الأطر الخاصة لفريق تقنية المعلومات لضبط مسئولياتهم والصلاحيات المخولة لهم في نطاق عملهم	أنظمة النسخ الاحتياطي ومكافحة الفيروسات والحماية من الاختراق
4	سياسة الاستجابة للحوادث: توضيح ما الذي يتوجب عمله في حال حدوث اختراق أمني أو انتهاك للمعلومات بشكل أو بآخر	النظام الإداري
5	سياسة التعافي من الكوارث: توضيح آلية استرجاع الأنظمة والأجهزة للعمل بعد حدوث كارثة حسب أولوية الاحتياج	إجراءات العمل
6	سياسة إدارة الوصول: توضيح كيفية إدارة الصلاحيات للحسابات من حيث آلية إنشاءها أو تعديلها أو إلغائها	نظام الدعم الفني والبريد الإلكتروني وAD
7	سياسة تسمية الحسابات: وضع الأسس والقواعد لتسمية الحسابات عند إنشائها في AD أو في AAD بناء على الدور الوظيفي للحساب، والمرجعية في إنشائها.	الإجراءات المنصوصة

دورية التحديث

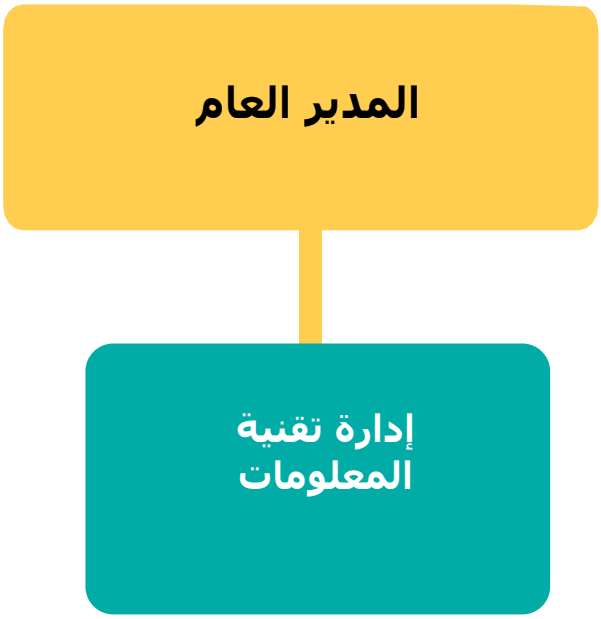
	نصف سنوي		سنوي

التحديثات

جهة الاعتماد	المسؤول عنه	الهدف منه	تاريخه	نوع التعديل
رئيسي		تحديث سياسات التقنية	مدير الإدارة	

المرجعية الإدارية:

يتبع المعهد قطاع المدير العام.



سياسة الاستخدام المقبول

الإصدار (3) – التاريخ (1 يناير 2022)

الغرض من السياسة

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

نطاق السياسة

تنطبق هذه السياسة على كل من:

- الموظفون بدوام كامل.
- الموظفون بدوام جزئي.
- المتطوعون.
- المتعاقدون الذين لهم صلاحية استخدام الأجهزة أو الأنظمة التابعة لجمعية زمزم.

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.

تغطي هذه السياسة ما يلي:

- أجهزة الحساب 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

عدم الامتثال للسياسة

عدم الامتثال لهذه القواعد يعطي الجمعية الحق في تطبيق ما تراه مناسب من عقوبات والتي قد تصل إلى إنهاء الخدمات.

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.

حفظ البيانات والملفات:

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 OnDrive الخاص بالموظف على Office 365 أو على الفريق الخاص بالإدارة على Microsoft Teams.

لا يجوز تخزين الملفات على وسائط تخزين شخصية أو على خدمات سحابية شخصية مثل Google Drive أو ما شابهها، أو على جهاز الكمبيوتر في غير ما تم تحديده (كسطح المكتب مثلا).

صلاحيات الدخول على البيانات ومشاركتها

قائمة صلاحيات الدخول Access Control List (ACL) موجودة على ملف إكسل ACL.xlsx
للاستفسارات حول صلاحيات الدخول، أو طلب صلاحية دخول لنظام أو الاطلاع على ملفات معينة فضلا التواصل مع مدير تقنية المعلومات.

الصيانة والصيانة الوقائية

يتم صيانة البيانات والأجهزة الحاسوبية وملحقاتها بشكل دوري في آخر ربع من كل سنة. ولطلب صيانة طارئة فضلا رفع طلب في نظام الدعم الفني.
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.
يحق لموظفي تقنية المعلومات الاستعانة بفنيين من خارج الجمعية للعمل تحت إشرافهم في الحالات التي تتطلب الاستعانة بشركات دعم خارجي.

توجيهات أمنية عامة

- 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 ولأغراض العمل فقط.
- يجب أن تكون جميع أجهزة الحاسب الآلي محمية بكلمة مرور، حتى الأجهزة في الأماكن العامة مثل غرف الاجتماعات.
- جميع الأجهزة يفعل عليها شاشة توقف تعمل بعد 10 دقائق من ترك الجهاز، وتتطلب استخدام كلمة مرور لتجاوزها.
- 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.
- 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).

الاستخدام غير المقبول

جميع الأعمال التالية غير مقبولة بشدة:

- انتهاك حقوق النشر أو الماركات المسجلة أو أية حقوق ملكية فكرية، بما في ذلك – وليس مقتصراً على – البرامج المقرصنة أو استخدام الصور بدون ترخيص.
- الدخول على بيانات الجمعية أو أنظمتها لهدف لا يتعلق بإنجاز أعمال الجمعية.
- إدخال برامج ضارة أو خبيثة لأجهزة الجمعية أو لأجهزة موظفي الجمعية.
- استخدام برامج لتجاوز أنظمة الحماية أو كسرها.
- استخدام أجهزة الجمعية أو أنظمتها لأغراض شخصية أو تجارية خاصة.
- استخدام أجهزة الجمعية في الألعاب أو الترفيه خلال أو خارج ساعات العمل.
- مشاهدة أو استعراض مواد مخلة من خلال أجهزة الجمعية أو شبكتها الحاسوبية.
- استخدام تقنية الجمعية أو شعارها أو نماذجها للقيام بأعمال احتيال.
- تقديم ضمانات أو خطابات ضمان باسم الجمعية.
- التسبب في حدوث خرق أو تعمد خرق إجراءات أمن الجمعية.
- تعطيل اتصال الشبكة.
- المحاولات غير المصرح بها لاعتراض البيانات من خلال الشبكة.
- التحايل على الإجراءات الأمنية أو محاولة تجاوز إجراءات المصادقة على المستخدم (اسم المستخدم وكلمة المرور).

- أي محاولة لتعطيل أعمال الجمعية سواء داخليا أو افتراضيا.
- تسريب البيانات الشخصية للموظفين داخل أو خارج الجمعية.
- تعطيل أجهزة الجمعية عن طريق توصيلها بشكل خاطئ عمداً أو فصلها عن الشبكة.

سياسة كلمات المرور

- تماشيا مع متطلبات أمن المعلومات فإن كلمة المرور يجب أن:
- تكون 8 حقول فأكثر، وتحتوي على حرف إنجليزي واحد كبير على الأقل، وحرف إنجليزي صغير واحد على الأقل، ورمز واحد على الأقل.
- يجب تغيير كلمة المرور كل 90 يوم، ولا يجوز استخدام آخر 3 كلمات مرور.
- تجنب استخدام كلمات مرور ضعيفة مثل الأرقام، أو الأحرف المكررة أو المتسلسلة مثلا 123456، أو المعلومات الشخصية كتاريخ الميلاد أو أسماء الأبناء، أو معلومات معروفة مثل اسم الجمعية أو عنوان أو رقم هاتفها، وغير ذلك.

تنبيهات بخصوص كلمات المرور

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

المسؤولية عن الحساب والحسابات المشتركة

الموظف مسؤول بشكل كامل عن حسابه في جمعية زمزم وكلمة المرور الخاصة به، ولا يجوز له أن يشاركها مع أي موظف كان أو غيره. وهو المسؤول بشكل مباشر عن كل ما يصدر عن حسابه.
ولا يحق للموظف استخدام حساب موظف آخر للقيام بأي عمل بدون إذن رسمي.
بعض الحسابات مشتركة ويمكن للجميع استخدامها، مثل حساب غرف الاجتماعات، أو حسابات غرف خدمات الشاي.
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.

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.

مراسلة جهات أو افراد خارجيين

حيث أن البريد الإلكتروني لجمعية زمزم يعطي صفة رسمية عند مراسلة جهات وأفراد خارجيين، فيمكنك 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.

الرسائل الجماعية

لا يجوز استخدام بريد الجمعية لإرسال رسائل 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.
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.

إعادة توجيه البريد الإلكتروني

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.
في حال أعددت رسالة وترغب في سريتها أو منع إعادة توجيهها فيجب أن تحدد هذا الخيار قبل إرسال الرسالة لمنع طباعتها أو إعادة توجيهها.

القوائم البريدية

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 لأي غرض وبأي وسيلة.
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 توجيه بريد إلكتروني إلى المدير العام توضح فيه مبررات استخدام القائمة البريدية.

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.

أمن البريد الإلكتروني

الرسائل المشتبه بها

ينبغي الحذر عند تلقي رسائل بريد إلكتروني من خارج الجمعية (وأحيانا من داخلها). وفي حال تلقيت رسالة مشبوهة فعليك التواصل فورا مع فريق تقنية المعلومات. 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.

المرفقات

يفضل عدم إرسال مرفقات مع رسائل البريد الإلكتروني، وبدلا من ذلك يفضل دائما إدراج الملف من OneDrive بحيث يتم إدراجه الملف كرابط غالبا. هناك عدة مزايا لعدم إرفاق الملفات بشكل مباشر بالرسالة الإلكترونية.

في حال كانت الرسالة موجهة لجهة أو شخص خارج الجمعية فيمكن إرفاق الملف في الرسالة.
عند استقبال رسالة بها مرفق فيجب التأكد أولا من مصدرها قبل فتح المرفق، والتأكد من أن المرسل قد أرسل لك رسالة وبها مرفق معين.

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

الإصدار (3) – التاريخ (1 يناير 2022)

الغرض من السياسة

الغرض من هذه السياسة وضع الأطر العامة لاستخدام الأجهزة الشخصية لأداء أعمال الجمعية سواء في وقت الدوام الرسمي أو خارجه. 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.

نطاق السياسة

تنطبق هذه السياسة على:

- الموظفين بدوام كامل.
- الموظفين بدوام جزئي.
- المتعاقدون مع الجمعية.
- المتطوعون.

يستثنى من هذه السياسة:

لا يوجد حاليا

الأجهزة الشخصية المسموح باستخدامها في العمل:

- أجهزة الحاسب المحمول (لابتوب).
- أجهزة الحاسب المكتبية الشخصية.
- الهواتف الذكية.
- الأجهزة اللوحية (التابلت).

عدم الامتثال للسياسة

عدم الامتثال لهذه القواعد يعطي الجمعية الحق في تطبيق ما تراه مناسب من عقوبات والتي قد تصل إلى إنهاء الخدمات.

الأعمال المصنفة كأعمال للجمعية

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.

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.

الأعمال الأخرى التي لا ينطبق عليها ما ذكر أعلاه، لا تتحمل الجمعية مسؤوليتها، ولا تعتبر أعمال للجمعية.

أمن الجهاز الشخصي

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.

يجب تفعيل استخدام كلمة مرور على الجهاز الشخصي المستخدم في العمل، ويجب أن تكون كلمة المرور تتبع تعليمات كلمات المرور في سياسة الاستخدام المقبول.

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.

يجب عدم استخدام أي جهاز شخصي تمت كسر حمايته أو يحتوي برمجيات ضارة.

صيانة وإدارة الجهاز الشخصي

في حال احتاج الجهاز الشخصي المستخدم في العمل للصيانة، يجب أولا التواصل مع الدعم الفني لضمان أمن وسلامة وخصوصية بيانات الجمعية.

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.

في حال ضياع الجهاز الشخصي الذي يحتوي على بيانات ومعلومات الجمعية يجب على الموظف التواصل مع إدارة تقنية المعلومات في خلال 4 ساعات على الأكثر من تأكد ضياع أو سرقة الجهاز.

الاتصال بالشبكات اللاسلكية التابعة للجمعية

الأجهزة الشخصية أثناء ساعات العمل يمكن أن ترتبط بشبكة الزوار اللاسلكية لإنجاز أعمال الجمعية، وكذلك زوار الجمعية لأغراض العمل يمكنهم الارتباط بهذه الشبكة. فقط الأجهزة التي تمتلكها الجمعية وتقع تحت مسؤولية إدارة تقنية المعلومات بشكل مباشر يمكنها الارتباط بشبكة واي فاي الرسمية للجمعية.

الاتصال بالشبكات اللاسلكية الأخرى

بالنسبة لشبكة المنزل اللاسلكية، فيجب أن يكون الراواتر محمي بكلمة مرور قوية، وكذلك الواي فاي، ويجب تفعيل جدار ناري شخصي للحماية.

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).

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

تراخيص البرامج

يمكن للموظف تنزيل حزمة برامج مايكروسوفت أوفيس 365 وكل ما يتبعها، ويستخدم حساب جمعية زمزم لتسجيل الدخول، وبذلك يصبح من حقه استخدام تلك البرمجيات تحت ترخيص الجمعية.

في بعض الحالات يتم تركيب حزمة مكافحة الفيروسات من قبل الجمعية في جهاز الموظف.
في حال ترك الموظف العمل في الجمعية يجب عليه تسجيل الخروج من كل هذه البرامج، وإزالتها.

سياسة أمن المعلومات لفريق تقنية المعلومات

الإصدار (3) – التاريخ (1 يناير 2022)

الغرض من السياسة

الغرض من هذه السياسة وضع الأطر الخاصة لفريق تقنية المعلومات لضبط مسئولياتهم والصلاحيات المخولة لهم في نطاق عملهم، 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.

نطاق السياسة

تنطبق هذه السياسة على:

- فريق الدعم الفني.
- مدير الشبكة Administrator
- أخصائي الشبكة مع صلاحية User Admin
- أخصائي البرمجة.
- أخصائي المحاسبة.

يستثنى من هذه السياسة:

لا يوجد حاليا.

عدم الامتثال للسياسة

عدم الامتثال لهذه القواعد يعطي الجمعية الحق في تطبيق ما تراه مناسب من عقوبات والتي قد تصل إلى إنهاء الخدمات.

سياسة البيانات

الجدول التالي يوضح أنواع البيانات ومدى حساسية كل منها:

ت	نوع البيانات	سري؟	أساسي؟	مفتوح؟
1	بيانات المستفيدين الأساسية	نعم		
2	بيانات طلب العلاج للمستفيدين	نعم		
3	بيانات المتبرعين الأساسية	نعم		
4	بيانات تفاصيل التبرعات	نعم		
5	بيانات بطاقات الدفع الإلكترونية	نعم		
6	بيانات الموظفين الأساسية		نعم	
7	بيانات الموظفين المالية	نعم		
8	بيانات حركات الموظفين الوظيفية		نعم	
9	بيانات الموردين		نعم	
10	بيانات حركات الموردين المالية	نعم		
11	البيانات المالية	نعم		

النسخ الاحتياطي

جداول النسخ الاحتياطي

- نسخ احتياطي يومي
- نسخ احتياطي أسبوعي
- نسخ احتياطي شهري
- نسخ احتياطي سنوي
- نسخ احتياطي يدوي
- نسخ احتياطي للخدمات السحابية

حفظ النسخ الاحتياطية

- النسخ الاحتياطي اليومي: نسخة واحدة لكل يوم للأسبوع الحالي.
- النسخ الاحتياطي الأسبوعي: نسخة واحدة لكل أسبوع لهذا الشهر وللشهر السابق.
- النسخ الاحتياطي الشهري: نسخة احتياطية واحدة لكل شهر لهذه السنة وبعمق 6 أشهر.
- النسخ الاحتياطي السنوي: نسخة واحدة لكل سنة.

تخزين النسخ الاحتياطي

السيرفرات في مركز البيانات في مقر الجمعية الرئيسي

- تحفظ النسخ اليومية والأسبوعية في وسيط تخزين SAN مخصص في داخل مركز البيانات.
- تحفظ النسخ الشهرية والسنوية في وسيط تخزين Tape وتحفظ في خزنة في مبنى تنمية الموارد.

البيانات على سيرفرات Azure

- تحفظ جميع النسخ على S-Vault Backup 1 TB Space على Azure Stack

قواعد البيانات على D365

- تحفظ نسخة شهرية على SAN داخل الجمعية.

نظام النسخ الاحتياطي

يستخدم برنامج Symantec Backup Exec - Veritas للنسخ الاحتياطي، ويتم إعداد خطط النسخ الاحتياطي حسب ما ذكر أعلاه، وتراقب التقارير وتصحح الأخطاء بشكل يومي من قبل إخصائي الشبكة المكلف.

اختبار النسخ الاحتياطي

يتم اختبار النسخ الاحتياطي عن طريق استرجاع ملفات عشوائية إلى مكان تجريبي.

يجرى الاختبار كل 3 أشهر مرة واحدة على الأقل.

غرفة مركز البيانات

غرفة مركز البيانات مؤمنة بوابة حديدية مزودة بقفل يعمل بالخصائص الحيوية ويسجل عمليات الدخول التي تحدث. ولا يسمح بدخولها إلا لأخصائي الشبكة المخول ورئيس قسم الشبكة والدعم الفني. وفي حال عمليات الصيانة يجب تواجد أخصائي الشبكة طوال الوقت مع فني الصيانة.

مزودة الغرفة بوسائل إطفاء الحريق بالغاز الخاص بمراكز البيانات، ومزودة بأجهزة تكييف متخصصة تعالج نسبة الرطوبة ودرجة الحرارة. كما أجهزة تكييف احتياطي في حال تعطل التكييف الرئيسي.

يتم مراقبة الغرفة عبر كاميرات مراقبة تعمل طوال الوقت، وتراقب درجات الحرارة وحالة الغرفة عبر نظام مراقبة متخصص، ويتم إشعار أخصائي تقنية المعلومات بأي تغييرات في الغرفة.

تخزين كلمات المرور

- لا تقوم الجمعية بتخزين كلمات المرور أو مفاتيح التشفير في مجلدات أو ملفات على سيرفرات داخلية أو خارجية.
- كلمات مرور موظفي الجمعية تخزن في Active Directory.
- كلمات مرور مستخدمي المواقع تخزن مشفرة في قواعد بيانات MS SQL.

تنصيب البرامج

أخصائي تقنية المعلومات هو المسؤول عن تنصيب أي برمجيات على أجهزة الجمعية وسيرفراتها، ولا يسمح للمستخدمين تنصيب أي برنامج عدا ما قام به أخصائي تقنية المعلومات.

البرامج المسموح بتنصيبها على أجهزة الجمعية هي:

- حزمة برامج أوفيس 365
- أدوبي أكروبات ريدر
- متصفح الإنترنت فاير فوكس

البرامج التالية تنصب في أجهزة موظفي بعض الإدارات:

- MS Dynamic AX – أجهزة موظفي الإدارة المالية.
- جوجل كروم – أجهزة موظفي الثروة البشرية.
- حزمة أدوبي للتصميم والمونتاج – أجهزة المصممين.

يمكن تنصيب بعض البرامج الأخرى حسب احتياج الموظف، وتخضع لموافقة مدير تقنية المعلومات، ويسجل في ملحق البرنامج والجهاز والمستخدم.

لا يسمح بأي شكل تنزيل أي برنامج من غير موقع الشركة صاحبة البرنامج.

لا يسمح بتنصيب أي برنامج بدون شراء الترخيص المناسب له، وفي حال الاحتياج يسمح ببعض البرامج التي تسمع بالتشغيل لفترة تجريبية، ثم يحذف وتشترى رخصة البرنامج إن تقرر استخدامه.

تراخيص البرمجيات وأنظمة التشغيل

تحتفظ إدارة تقنية المعلومات بمعلومات التراخيص لكل البرمجيات التي تستخدمها الجمعية بما في ذلك مفاتيح التشغيل لأنظمة التشغيل وغيرها من البرامج.

تحديث البرامج وأنظمة التشغيل

يتولى رئيس قسم الشبكة والدعم الفني مسؤولية متابعة تحديث البرامج وأنظمة التشغيل حسب الحاجة والضرورة. وفي حال الاحتياج لشراء رخصة جديدة لتحديث النظام فيتم ذلك بالتنسيق مع مدير تقنية المعلومات. تنصيب التحديثات يتم من قبل فريق تقنية المعلومات – عدا التحديثات الآلية الأمنية التي تتم آليا – خلال عمليات الصيانة الوقائية، أو بناء على طلب المستخدم.

استبدال الأجهزة

يتم استبدال السيرفرات بعد نهاية فترة الضمان من الشركة الموردة.

يتم استبدال أجهزة الحاسب الآلي بعد انتهاء العمر الافتراضي للجهاز، ويتابع قسم الشبكة والدعم الفني عمر الأجهزة خلال عمليات الصيانة والوقائية ويرفع بعدد الأجهزة التي تحتاج إلى استبدال لإدراجها في موازنة السنة الجديدة.

طلب شراء الأجهزة الجديدة التي ستحل مكان الأجهزة المستهلكة يتم من مدير إدارة تقنية المعلومات، وكذلك بالنسبة للسيرفرات. طلبات شراء الأجهزة الأخرى تتم من خلال مدير الإدارة المعني.

اعتبارات أمنية أخرى

معلومات البطاقات الائتمانية

جميع عمليات التبرع بواسطة البطاقات الائتمانية وبطاقات مدى تتم بشكل آمن ومشفر عبر شركة وساطة مالية معتمدة من البنك المركزي ومرخصة، وتودع التبرعات في حسابات الجمعية.

إذا اختار المتبرع أن يخزن معلومات بطاقته الائتمانية في متجر جمعية زمزم، فإن هذه المعلومات تخزن بشكل مشفر في قواعد البيانات، ولا يتم الكشف عنها لأي جهة أخرى عدا البنك عند إجراء عملية تبرع مالي.

المعلومات الشخصية

المعلومات الشخصية للمتبرعين أو المستفيدين من خدمات الجمعية أو الموظفين تخزن في قواعد البيانات بشكل مشفر، ولا يتم الكشف عنها أو مشاركتها مع آخرين إلا في حدود ما تتطلبه عملية الاستفادة من خدمات الجمعية أو التقارير الدورية للتبرعات.

استثناءات من هذه السياسة

- فقط فريق إدارة تقنية المعلومات هو المخول بتنصيب برنامج على أجهزة الجمعية ولا ينطبق عليهم المنع.

سياسة الاستجابة للحوادث

الإصدار (3) – التاريخ (1 يناير 2022)

الغرض من السياسة

الغرض من هذه السياسة توضيح ما الذي يتوجب عمله في حال حدوث اختراق أمني أو انتهاك للمعلومات بشكل أو بآخر. الحوادث المقصودة في هذه السياسة هي التي تتعلق باختراق الشبكة من قبل مخترقين داخليين أو خارجيين، والتي قد تتضمن – ولا تقتصر على – تعطيل الشبكة، و/أو الوصول إلى بيانات غير مصرح الوصول لها، أو إتلاف البيانات أو تغييرها بما يخل بمحتواها.

الجدول التالي الاستجابة المطلوبة عند الأحداث

الفعل	المسؤول	المسؤول الاحتياطي	زمن الاستجابة
تحليل الاختراق	مدير تقنية المعلومات	تقنية المعلومات	آنيا
إزالة إمكانية الوصول	مدير تقنية المعلومات	تقنية المعلومات	آنيا
إصلاح أو استبدال النظام أو الجهاز المعطل	مدير تقنية المعلومات	تقنية المعلومات	
مراجعة الإجراءات	مدير تقنية المعلومات	تقنية المعلومات	بعد الإصلاح أو الاستبدال
التواصل مع الفريق الداخلي	المدير العام	مساعد المدير العام	بعد إزالة إمكانية الوصول
التواصل مع الجمهور الخارجي	رئيس مجلس الإدارة	العلاقات العامة	عند الحاجة

سياسة التعافي من الكوارث

الإصدار (3) – التاريخ (1 يناير 2022)

الغرض من السياسة

الغرض من هذه السياسة هو توضيح آلية استرجاع الأنظمة والأجهزة للعمل بعد حدوث كارثة حسب أولوية الاحتياج.

أولوية الاسترجاع

يتم استرجاع الأنظمة وفق الأولوية وحسب الترتيب من الأعلى إلى الأسفل (بسبب احتياج كل خدمة لما قبلها) في الجدول التالي.

الخدمة	متطلبات الخدمة
الطاقة الكهربائية	الشبكة العامة للكهرباء، البطاريات الاحتياطية
الاتصال بالإنترنت	مزودي خدمة الإنترنت، راوتر
الشبكة الداخلية	Core Switch مع استرجاع إعداداته السابقة إن لزم
Servers	
Domain Controller	DC Server or additional DC
Backup system	
MS Teams Phone System	
MS Dynamics 365	
ZMZM Portal	
PCs	

استرجاع البيانات

مواقع النسخ الاحتياطية

System	Backup Location
ZMZM Portals	Azure Svault
ZMZM Servers on Azure	Azure Svault
Switches configuration	مجلد "الشبكة" ضمن ملفات "فريق تقنية المعلومات/قسم الشبكات"
Router Configuration	مجلد "الشبكة" ضمن ملفات "فريق تقنية المعلومات/قسم الشبكات"

استبدال المعدات التالفة/المفقودة

الأولوية عند الحاجة لاستبدال المعدات التالفة أو المفقودة هي لأجهزة الشبكة والسيرفرات، ثم لأجهزة وأنظمة الاتصالات.

لتوفير الأجهزة بشكل سريع يتم التواصل مع المورد المعتمد (مؤسسة إدريس محمد فتني التجارية – 0504326703)

خطط الطوارئ

الخدمة	الخدمة البديلة
الاتصالات	MS Teams على أجهزة الموبايل الشخصية
الاتصال بالإنترنت	الخط البديل أو اتصال لاسلكي عبر راوتر يعمل بشريحة

سياسة إدارة الوصول

الإصدار (3) – التاريخ (1 يناير 2022)

الغرض من السياسة

الغرض من هذه السياسة توضيح كيفية إدارة الصلاحيات للحسابات من حيث آلية إنشاءها أو تعديلها أو إلغائها، بناء على طلبات رسمية من إدارة الثروة البشرية.

نطاق السياسة

تنطبق هذه السياسة على:

- حسابات الموظفين الرسميين
- حسابات الموظفين المتعاونين
- حسابات المتطوعين
- حسابات الشركاء والزوار
- حسابات إدارة الشبكة والخدمات

يستثنى من هذه السياسة:

لا يوجد حاليا

حسابات الموظفين الرسميين

يتم إنشاء حساب للموظف الرسمي بناء على طلب رسمي من إدارة الثروة البشرية من خلال تقديم طلب في نظام الدعم الفني يتضمن المعلومات الأساسية (الاسم عربي وإنجليزي، الإدارة والقسم التابع لها، المسمى الوظيفي).

عند إنشاء الحساب لأول مرة، فيتم إعطاء الموظف الرسمي صلاحية الوصول إلى:

- ملفات الإدارة والقسم الذي يتبع له تحت قسم (ملفات) فريق الإدارة التابع له.
- الملفات العامة تحت فريق جمعية زمزم (قراءة فقط).
- صلاحية على نظام معين بناء على طلب من مدير الإدارة المعنية من خلال البريد الإلكتروني أو من خلال طلب دعم الفني.

يتم إغلاق الحساب وإزالة إمكانيات الوصول بناء على طلب رسمي من الثروة البشرية عبر نظام الدعم الفني.

حسابات الموظفين المتعاونين

يتم إنشاء حساب للموظف المتعاون بناء على طلب رسمي من إدارة الثروة البشرية من خلال تقديم طلب في نظام الدعم الفني يتضمن المعلومات الأساسية (الاسم عربي وإنجليزي، الإدارة والقسم التابع لها، المسمى الوظيفي).

يتم إعطاء صلاحيات للموظف المتعاون بناء على طلب رسمي من خلال البريد الإلكتروني من مدير الإدارة المعنية مع إشعار الثروة البشرية.

قد يتضمن الوصول إلى:

- ملفات الإدارة والقسم الذي يتبع له تحت قسم (ملفات) فريق الإدارة التابع له.
- الملفات العامة تحت فريق جمعية زمزم (قراءة فقط).
- صلاحية على نظام معين بناء على طلب من مدير الإدارة المعنية من خلال البريد الإلكتروني أو من خلال طلب دعم الفني.

يتم إغلاق الحساب وإزالة إمكانية الوصول بناء على طلب رسمي من الثروة البشرية عبر نظام الدعم الفني.

حسابات المتطوعين

يتم إنشاء حسابات المتطوعين بناء على طلب رسمي من إدارة التطوع من خلال نظام الدعم الفني، يوضح فيه اسم المتطوع ومدة التطوع.
تحدد صلاحية الحساب بناء على مدة التطوع المذكورة في الطلب، ويغلق الحساب آليا في نهاية المدة المحددة.
صلاحيات المتطوعين تحدد من قبل مدير الإدارة المعنية ومن خلال بريد إلكتروني يوضح حدود الصلاحيات المعطاة لهم.

حسابات الشركاء والزوار

يتم إنشاء حسابات للشركاء والزوار عند الحاجة بصلاحيات محددة للغاية (كالوصول إلى الإنترنت، أو الدخول على سيرفر محدد لأداء مهمة معينة) بناء على بريد رسمي يوجه لمدير إدارة تقنية المعلومات يوضح فيه:

- اسم الشريك/الجهة
- مدة العمل
- المهام التي سينجزها

يغلق الحساب فور انتهاء المهمة المحددة، ومن مسؤولية مدير الإدارة المعنية إخطار مدير تقنية المعلومات بذلك.

حسابات إدارة الشبكة والخدمات

الحسابات العامة (مثل غرف الاجتماعات) وحسابات الخدمات الآلية (مثل حساب إدارة الطباعة) تنشأ بناء على طلب يرفعه رئيس قسم الشبكة والدعم الفني لمدير إدارة تقنية المعلومات.

سياسة تسمية الحسابات

الإصدار (3) – التاريخ (1 يناير 2022)

الغرض من السياسة

الغرض من هذه السياسة وضع الأسس والقواعد لتسمية الحسابات عند إنشائها في AD أو في AAD بناء على الدور الوظيفي للحساب، والمرجعية في إنشائها.

السياسة العامة:

يستحق كل موظف رسمي الحصول على حساب خاص باسمه للتعامل من خلاله مع بقية منسوبي الجمعية وذلك حسب القواعد أدناه.

تنطبق هذه السياسة على:

- حسابات الموظفين الرسميين والمتعاونين
- حسابات المتطوعين
- حسابات الشركاء والزوار
- حسابات إدارة الشبكة والخدمات

يستثنى من هذه السياسة:

لا يوجد حاليا

حسابات الموظفين الرسميين والمتعاونين

يتم إنشاء الحساب للموظف الرسمي والمتعاون بناء على طلب رسمي من إدارة الثروة البشرية من خلال نظام الدعم الفني يوضح فيه اسم المستخدم باللغة العربية والإنجليزية - رقم الجوال - المسمى الوظيفي - الإدارة التي يعمل بها.

القاعدة في إنشاء اسم الحساب كالتالي:

firstname.lastname@zmzm.org

حسابات المتطوعين

يتم إنشاء الحساب للموظف المتطوع بناء على طلب رسمي من إدارة التطوع من خلال نظام الدعم الفني ويوضح في وصف الحساب اسم الإدارة المتطوع فيها
القاعدة في إنشاء اسم الحساب كالتالي:
Volunteer.XX@zmzm.org

حسابات الشركاء والزوار

يتم إنشاء حساب مؤقت بصلاحيات محددة للشركاء والزوار الذي يعملون مع جمعية زمزم، وبموافقة مدير تقنية المعلومات بعد بريد إلكتروني رسمي من الإدارة ذات الاحتياج، مع إشعار الثروة البشرية.

يغلق الحساب فور انتهاء المهمة أو العمل المكلف به الزائر.

القاعدة في إنشاء حساب للشركاء والزوار كالتالي:

Guest.Department.XX@zmzm.org

حسابات الخدمات والحسابات العامة

يتم إنشاء حساب للخدمات العامة مثل غرف الاجتماعات وغيرها والتي تكون متاحة للاستخدام من الجميع بناء على توجيه من مدير تقنية المعلومات، وتعطى صلاحيات محدودة للغاية تقتصر على تصفح الإنترنت واستخدام MS Teams

القاعدة في إنشاء حسابات الخدمات والحسابات العامة كالتالي:

roomXX.srv@zmzm.org

٥. العمليات

٥-١ عملية الصيانة الوقائية للأجهزة التقنية

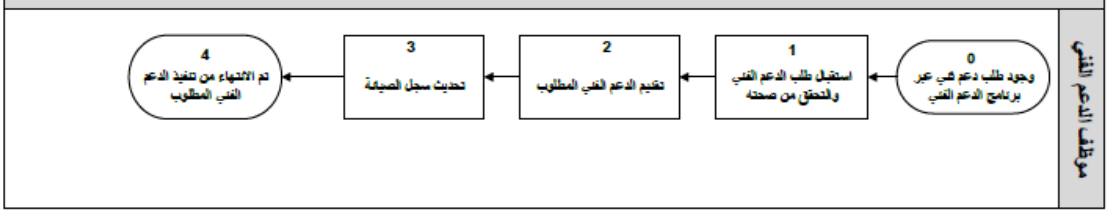
اسم العملية			عملية الصيانة الوقائية للأجهزة التقنية		رقم العملية	1	
المدخلات	م	تصنيف	الخطوات	المسؤول	رقم الخطوة التالية	النموذج/النظام الإلكتروني	المخرجات
* سجل الأجهزة التقنية	0	البداية	بداية كل عام ميلادي		1	برنامج الدعم الفني	* سجل الصيانة الوقائية
	1	خطوة	إعداد واعتماد الخطة السنوية الشاملة للصيانة الوقائية	رئيس قسم الشبكات والدعم الفني	2	برنامج الدعم الفني	
	2	خطوة	إعلام الإدارات بمواعيد الصيانة الوقائية الخاصة بإداراتهم عن طريق البريد الالكتروني	رئيس قسم الشبكات والدعم الفني	3	برنامج الدعم الفني	
	3	خطوة	إسناد الأجهزة المراد صيانتها لموظفي الدعم الفني	رئيس قسم الشبكات والدعم الفني	4	برنامج الدعم الفني	
	4	خطوة	البدء في تنفيذ الصيانة الوقائية وتحديث السجل الخاص بها	موظف الدعم الفني	5	برنامج الدعم الفني	
	5	خطوة	تقديم الدعم الفني للأجهزة التي بها مشاكل	موظف الدعم الفني	6	برنامج الدعم الفني	
	6	خطوة	إعداد تقرير الصيانة الوقائية	رئيس قسم الشبكات والدعم الفني	7	برنامج الدعم الفني	
	7	النهاية	تم تنفيذ الصيانة الوقائية				
النتائج المتوقعة			تحسن عمل الاجهزة التقنية		مالك العملية	رئيس قسم الشبكات والدعم الفني	
مؤشرات الاداء (KPIs)			تنفيذ الصيانة الوقائية بنسبة ١٠٠% عدد أعطال الصيانة المنفذة		الإدارة	إدارة تقنية المعلومات	

جمعية زمزم
للخدمات الصحية التطوعية الخيرية

٥-٢ عملية الدعم الفني

اسم العملية			عملية الدعم الفني		رقم العملية	2	
المدخلات	م	تصنيف	الخطوات	المسؤول	رقم الخطوة التالية	النموذج/النظام الإلكتروني	المخرجات
* برنامج الدعم الفني	0	البداية	وجود طلب دعم فني عبر برنامج الدعم الفني		1	برنامج الدعم الفني	
	1	خطوة	استقبال طلب الدعم الفني والتحقق من صحته	موظف الدعم الفني	2		
	2	خطوة	تقديم الدعم الفني المطلوب	موظف الدعم الفني	3		* سجل صيانة محدث
	3	خطوة	تحديث سجل الصيانة	موظف الدعم الفني	4		
	4	النهاية	تم الانتهاء من تنفيذ الدعم الفني المطلوب				
النتائج المتوقعة			تحسن عمل الأجهزة التقنية		مالك العملية	موظف الدعم الفني	
مؤشرات الاداء (KPIs)			عدد طلبات الدعم الفني المنفذة		الإدارة	إدارة تقنية المعلومات	

٥-٢ خريطة تدفق عملية الدعم الفني



٣-٥ عملية النسخ الاحتياطي

اسم العملية			عملية النسخ الاحتياطي		رقم العملية	3	
المدخلات	م	تصنيف	الخطوات	المسؤول	رقم الخطوة التالية	النموذج/النظام الإلكتروني	المخرجات
	0	البداية	بعد تصميم خطة النسخ الاحتياطي (كامل، تراكمي، تفريقي)	مدير إدارة تقنية المعلومات	1	دليل السياسات التقنية	* نسخة احتياطية حديثة لجميع بيانات الجمعية على وسائط تخزين داخل الجمعية. * نسخة احتياطي حديثة لجميع بيانات الجمعية على أشرطة نسخ احتياطي في موقع آخر (مبى
	1	خطوة	برمجة نظام النسخ الاحتياطي حسب خطة النسخ الاحتياطي	رئيس قسم الشبكات والدعم الفني	2	Symantic Veritas	
	2	خطوة	اختبار عمليات النسخ الاحتياطي	رئيس قسم الشبكات والدعم الفني	3	Symantic Veritas	
	3	خطوة	معالجة وتصحيح مشاكل النسخ الاحتياطي في حال تلقي إشعار من النظام	رئيس قسم الشبكات والدعم الفني	4	Symantic Veritas	
	4	خطوة	استخراج أشرطة النسخ الاحتياطي من الجهاز ونقلها لخزنة مدير الموارد البشرية حسب خطة النسخ الاحتياطي	رئيس قسم الشبكات والدعم الفني	5	نموذج استلام النسخة الاحتياطية	
	5	النهاية	تم الانتهاء من عملية النسخ الاحتياطي				
النتائج المتوقعة			حفظ وحماية معلومات الجمعية		مالك العملية	رئيس قسم الشبكات والدعم الفني	
مؤشرات الاداء (KPIs)			نسبة عمليات النسخ الاحتياطي المنفذة إلى المستهدفة		الإدارة	إدارة تقنية المعلومات	

٣-٥ عملية طلب تنفيذ مشروع تقني

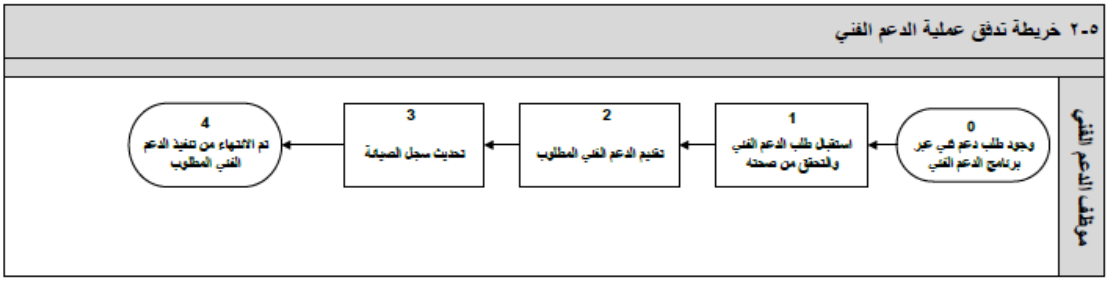
اسم العملية			عملية طلب تنفيذ مشروع تقني		رقم العملية	4	
المدخلات	م	تصنيف	الخطوات	المسؤول	رقم الخطوة التالية	النموذج/النظام الإلكتروني	المخرجات
*قائمة المشاريع التقنية المعتمدة. *طلبات التعديل على المشاريع التقنية.	0	البداية	بعد اعتماد المشاريع التقنية في الخطة التشغيلية		1		*المشروع التقني (الجديد/المعدل)
	1	خطوة	جمع متطلبات المشروع	رئيس قسم الشبكات/رئيس قسم التطبيقات	2	وثيقة تأسيس المشروع	
	2	خطوة	تحليل متطلبات المشروع (حسب الحاجة)	رئيس قسم الشبكات/رئيس قسم التطبيقات	3	وثيقة تأسيس المشروع	
	3	خطوة	تنفيذ المتطلبات	فريق العمل	4	وثيقة تأسيس المشروع	
	4	خطوة	متابعة المشروع	رئيس قسم الشبكات/رئيس قسم التطبيقات	5	وثيقة تأسيس المشروع	
	5	خطوة	التجهيز لتسليم المشروع	رئيس قسم الشبكات/رئيس قسم التطبيقات	6	وثيقة تأسيس المشروع	
	6	النهاية	تسليم وإغلاق المشروع	مدير إدارة تقنية المعلومات		وثيقة تأسيس المشروع	
	0	البداية	بعد تجربة العمل على المشروع التقني في الواقع		1		
	1	خطوة	جمع متطلبات التعديل	رئيس قسم الشبكات/رئيس قسم التطبيقات	2	طلب تعديل مشروع	
	2	خطوة	تحليل التعديلات حسب الحاجة	رئيس قسم الشبكات/رئيس قسم التطبيقات	3		
	3	خطوة	الحصول على الاعتمادات اللازمة	فريق العمل	4		
	4	خطوة	تنفيذ التعديلات	رئيس قسم الشبكات/رئيس قسم التطبيقات	5		
	5	خطوة	التجهيز لتسليم التعديل	رئيس قسم الشبكات/رئيس قسم التطبيقات	6		
	6	النهاية	تسليم التعديل	مدير إدارة تقنية المعلومات		إغلاق المشروع	
النتائج المتوقعة			زيادة نسبة الأعمال المنفذة تقنياً		مالك العملية	رئيس قسم التطبيقات والتطوير/رئيس قسم الشبكات والدعم الفني	
مؤشرات الاداء (KPIs)			عدد المشاريع التقنية المنفذة عدد التعديلات المنفذة (لكل مشروع)		الإدارة	إدارة تقنية المعلومات	

جمعية زمزم
للخدمات الصحية التطوعية الخيرية

٥-٢ عملية الدعم الفني

اسم العملية			عملية الدعم الفني		رقم العملية	2	
المدخلات	م	تصنيف	الخطوات	المسؤول	رقم الخطوة التالية	النموذج/النظام الإلكتروني	المخرجات
* برنامج الدعم الفني	0	البداية	وجود طلب دعم فني عبر برنامج الدعم الفني		1	برنامج الدعم الفني	* سجل صيانة محدث
	1	خطوة	استقبال طلب الدعم الفني والتحقق من صحته	موظف الدعم الفني	2		
	2	خطوة	تقديم الدعم الفني المطلوب	موظف الدعم الفني	3		
	3	خطوة	تحديث سجل الصيانة	موظف الدعم الفني	4		
	4	النهاية	تم الانتهاء من تنفيذ الدعم الفني المطلوب				
النتائج المترقعة			تحسن عمل الأجهزة التقنية		مالك العملية	موظف الدعم الفني	
مؤشرات الاداء (KPIs)			عدد طلبات الدعم الفني المنفذة		الإدارة	إدارة تقنية المعلومات	

٥-٢ خريطة تدفق عملية الدعم الفني



جمعية زمزم
للخدمات الصحية التطوعية الخيرية

٥-٣ عملية النسخ الاحتياطي

اسم العملية			عملية النسخ الاحتياطي		رقم العملية	3	
المدخلات	م	تصنيف	الخطوات	المسؤول	رقم الخطوة التالية	النموذج/النظام الإلكتروني	المخرجات
	0	البداية	بعد تصميم خطة النسخ الاحتياطي (كامل، تراكمي، تدريجي)	مدير إدارة تقنية المعلومات	1	دليل السياسات التقنية	* نسخة احتياطية حديثة لجميع بيانات الجمعية على وسائط تخزين داخل الجمعية.
	1	خطوة	برمجة نظام النسخ الاحتياطي حسب خطة النسخ الاحتياطي	رئيس قسم الشبكات والدعم الفني	2	Symantic Veritas	
	2	خطوة	اختبار عمليات النسخ الاحتياطي	رئيس قسم الشبكات والدعم الفني	3	Symantic Veritas	
	3	خطوة	معالجة وتصحيح مشاكل النسخ الاحتياطي في حال تلقي إشعار من النظام	رئيس قسم الشبكات والدعم الفني	4	Symantic Veritas	
	4	خطوة	استخراج أشرطة النسخ الاحتياطي من الجهاز ونقلها لخزنة مدير الموارد البشرية حسب خطة النسخ الاحتياطي	رئيس قسم الشبكات والدعم الفني	5	نموذج استلام النسخة الاحتياطية	* نسخة احتياطي حديثة لجميع بيانات الجمعية على أشرطة نسخ احتياطي في موقع آخر (مبنى
	5	النهاية	تم الانتهاء من عملية النسخ الاحتياطي				
النتائج المترقعة			حفظ وحماية معلومات الجمعية		مالك العملية	رئيس قسم الشبكات والدعم الفني	
مؤشرات الاداء (KPIs)			نسبة عمليات النسخ الاحتياطي المنفذة إلى المستهدفة		الإدارة	إدارة تقنية المعلومات	

جمعية زمزم
للخدمات الصحية التطوعية الخيرية
بمنطقة مكة المكرمة
إشراف وزارة العمل والتنمية الاجتماعية
تصريح رقم (٢٠)

٥-٣ عملية طلب تنفيذ مشروع تقني

اسم العملية			عملية طلب تنفيذ مشروع تقني		رقم العملية	4	
المدخلات	م	تصنيف	الخطوات	المسؤول	رقم الخطوة التالية	النموذج/النظام الإلكتروني	المخرجات
*قائمة المشاريع التقنية المعتمدة. *طلبات التعديل على المشاريع التقنية.	0	البداية	بعد اعتماد المشاريع التقنية في الخطة التشغيلية		1		*المشروع التقني (الجديد/المعدل)
	1	خطوة	جمع متطلبات المشروع	رئيس قسم الشبكات/رئيس قسم التطبيقات	2	وثيقة تأسيس المشروع	
	2	خطوة	تحليل متطلبات المشروع (حسب الحاجة)	رئيس قسم الشبكات/رئيس قسم التطبيقات	3	وثيقة تأسيس المشروع	
	3	خطوة	تنفيذ المتطلبات	فريق العمل	4	وثيقة تأسيس المشروع	
	4	خطوة	متابعة المشروع	رئيس قسم الشبكات/رئيس قسم التطبيقات	5	وثيقة تأسيس المشروع	
	5	خطوة	التجهيز لتسليم المشروع	رئيس قسم الشبكات/رئيس قسم التطبيقات	6	وثيقة تأسيس المشروع	
	6	النهاية	تسليم وإغلاق المشروع	مدير إدارة تقنية المعلومات		وثيقة تأسيس المشروع	
	0	البداية	بعد تجربة العمل على المشروع التقني في الواقع		1		
	1	خطوة	جمع متطلبات التعديل	رئيس قسم الشبكات/رئيس قسم التطبيقات	2	طلب تعديل مشروع	
	2	خطوة	تحليل التعديلات حسب الحاجة	رئيس قسم الشبكات/رئيس قسم التطبيقات	3		
	3	خطوة	الحصول على الاعتمادات اللازمة	فريق العمل	4		
	4	خطوة	تنفيذ التعديلات	رئيس قسم الشبكات/رئيس قسم التطبيقات	5		
	5	خطوة	التجهيز لتسليم التعديل	رئيس قسم الشبكات/رئيس قسم التطبيقات	6		
	6	النهاية	تسليم التعديل	مدير إدارة تقنية المعلومات		إغلاق المشروع	
النتائج المتوقعة			زيادة نسبة الأعمال المنفذة تقنياً		مالك العملية	رئيس قسم التطبيقات والتطوير/رئيس قسم الشبكات والدعم الفني	
مؤشرات الاداء (KPIs)			عدد المشاريع التقنية المنفذة عدد التعديلات المنفذة (لكل مشروع)		الإدارة	إدارة تقنية المعلومات	

جمعية زمزم
للخدمات الصحية التطوعية الخيرية
بمنطقة مكة المكرمة
إشراف وزارة العمل والتنمية الاجتماعية
تصريح رقم (٢٠)

٥. العمليات

٥-١ عملية الصيانة الوقائية للأجهزة التقنية

اسم العملية			عملية الصيانة الوقائية للأجهزة التقنية			رقم العملية	1	
المدخلات	م	تصنيف	الخطوات	المسؤول	رقم الخطوة التالية	النموذج/النظام الإلكتروني	المخرجات
* سجل الأجهزة التقنية	0	البداية	بداية كل عام ميلادي		1	برنامج الدعم الفني	* سجل الصيانة الوقائية
	1	خطوة	إعداد واعتماد الخطة السنوية الشاملة للصيانة الوقائية	رئيس قسم الشبكات والدعم الفني	2	برنامج الدعم الفني	
	2	خطوة	إعلام الإدارات بمواعيد الصيانة الوقائية الخاصة بإداراتهم عن طريق البريد الالكتروني	رئيس قسم الشبكات والدعم الفني	3	برنامج الدعم الفني	
	3	خطوة	إسناد الأجهزة المراد صيانتها لموظفي الدعم الفني	رئيس قسم الشبكات والدعم الفني	4	برنامج الدعم الفني	
	4	خطوة	البدء في تنفيذ الصيانة الوقائية وتحديث السجل الخاص بها	موظف الدعم الفني	5	برنامج الدعم الفني	
	5	خطوة	تقديم الدعم الفني للأجهزة التي بها مشاكل	موظف الدعم الفني	6	برنامج الدعم الفني	
	6	خطوة	إعداد تقرير الصيانة الوقائية	رئيس قسم الشبكات والدعم الفني	7	برنامج الدعم الفني	
	7	النهاية	تم تنفيذ الصيانة الوقائية				
النتائج المتوقعة			تحسن عمل الاجهزة التقنية		مالك العملية	رئيس قسم الشبكات والدعم الفني	
مؤشرات الاداء (KPIs)			تنفيذ الصيانة الوقائية بنسبة ١٠٠% عدد أعطال الصيانة المنفذة		الإدارة	إدارة تقنية المعلومات	

العمليات والإجراءات الخاصة .....
ملحق بإجراءات عمليات إدارة الجودة

بيانات التواصل:

مدير إدارة تقنية المعلومات: هاني فلمبان

البريد الإلكتروني:hfelemban@zmzm.org

تحويلة داخلية: 1200

9200 333 77

zmzm.sa