الجمعية النسائية الخيرية بحفرالباطن
Women 's Charity Association In Hafr Al - Batin

درة
Dorra

سياسات وإجراءات تقنية المعلومات

فهرس المحتويات

سياسات وإجراءات تقنية المعلومات للجمعية الخيرية النسائية (درة)

الفصل رقم (1): البريد الإلكتروني (Email)

المادة (1): هدف ونطاق السياسة

1. توضيح الاستخدام المناسب وغير المناسب لنظام البريد الإلكتروني الخاص بالجمعية من أجل تقليل تعطل الخدمة المقدمة بالإضافة للامتثال للسياسات والقوانين المعمول بها.
2. تنطبق هذه السياسة على جميع أنظمة وخدمات البريد الإلكتروني التي تملكها الجمعية.
3. تنطبق هذه السياسة على جميع مستخدمي حساب البريد الإلكتروني سواءً كان مؤقتا أو دائمًا.

المادة (2): المسؤولية

1. مسؤولية صيانة وتحديث نظام البريد الإلكتروني وكذلك إنشاء عناوين بريد جديدة أو إيقاف عناوين حالية تقع على عاتق قسم تقنية المعلومات ضمن إدارة التميز المؤسسي.
2. الاستخدام السليم لنظام البريد يقع على عاتق الموظفين والمستخدمين للبريد الإلكتروني.

المادة (3): السياسات المنظمة

1. يجب أن يتم استخدام البريد الإلكتروني الخاص بالجمعية للأغراض الرسمية الخاصة بأعمال الجمعية فقط.
2. يمنع منعا باتًا أن يستخدم الموظف بريده الإلكتروني الشخصي للمراسلات الرسمية الخاصة بالجمعية، ويتعرض الموظف للمساءلة فيما إذا ثبت ذلك.
3. فيما يخص تفعيل وإغلاق حسابات البريد الإلكتروني، يتم الالتزام بما يلي:

3.1 يتم التحكم في الوصول إلى البريد الإلكتروني الخاص بالجمعية من خلال حسابات فردية وكلمات السر. كل مستخدم مطالب بأن يقرأ ويوقع نسخة من سياسة الاستخدام المقبول للبريد الإلكتروني قبل الحصول على اسم المستخدم وكلمة المرور، وتقع على عاتق الموظف حماية معلومات الدخول إلى نظام البريد الإلكتروني الخاص به.

3.2 الحساب الإلكتروني يتبع دائمًا إجراء التسمية بحيث يبدأ بالحرف الأول من اسم الموظف، ثم نقطة، ثم كتابة العائلة كاملة، ويستثنى من ذلك موافقة المدير التنفيذي لجمعية درة.

3.3 على جميع الموظفين أو العاملين الذين انضموا حديثًا والذين يطلبون بريدًا إلكترونيًا ملء "نموذج حساب المستخدم " وتوقيع "نموذج تفهم السياسات الخاصة بالبريد الإلكتروني".

3.4 من الممكن لجميع موظفي الجمعية الحصول على حساب البريد الإلكتروني.

3.5 يمكن أن يتم منح حسابات البريد الإلكتروني لطرف آخر من غير الموظفين على أساس كل حالة على حدة والتي تشمل المتطوعين أو المتدربين أو أطراف تعمل بشكل مؤقت في مشاريع خاصة للجمعية، ويجب تقديم طلبات الحصول على هذه الحسابات المؤقتة لمدير إدارة التميز المؤسسي على أن تكون محددة بفترة زمنية.

3.6 الجمعية ليست ملزمة بتخزين أو إعادة توجيه الوارد للبريد الإلكتروني للأفراد الذين ينهون ارتباطهم بالجمعية.

3.7 عند انتهاء خدمة الموظف يتم الحصول على موافقة قسم تقنية المعلومات بتسليم البريد الإلكتروني وإقفاله ضمن نموذج إخلاء الطرف المعتمد.

4. التوقعات العامة من المستخدمين:

4.1 ترسل الجمعية في كثير من الأحيان مراسلات رسمية عبر البريد الإلكتروني لموظفين الجمعية ونتيجة لذلك، يتوقع من الموظفين المواظبة على قراءة بريدهم بشكل يومي ومستمر ليتم اطلاعهم على أخر التعميمات والإعلانات وكذلك لإنجاز الأعمال المطلوبة من الموظف عبر البريد الإلكتروني.

4.2 تقع مسؤولية تنظيم وتنظيف البريد الإلكتروني على عاتق الموظف.

4.3 توخي الحذر الشديد عند نقل المعلومات السرية أو الحساسة عبر البريد الإلكتروني.

5. يحق للجمعية مساءلة مالك البريد الإكتروني عند الاستعمال غير السليم له، ويمكن أن يشمل أي من النقاط التالية:

5.1 إن المراسلات التي تتم من خلال البريد الإلكتروني الخاص بالجمعية هي مراسلات رسمية وتؤثر على الجمعية، لذا يجب على الموظفين التقيد بالمعايير المهنية ومراعاة السلوك الاحترافي في استخدام البريد الإلكتروني.

5.2 استخدام البريد الإلكتروني لأغراض غير قانونية أو غير مشروعة مثل مخالفة حقوق الطبع والنشر أو أعمال تشوه السمعة أو الافتراء، الاحتيال، المضايقة، الترهيب، والعبث بالحاسوب (كنشر فيروسات الحاسوب) يعد من الأمور الممنوعة والخاضعة للمساءلة القانونية.

5.3 استخدام البريد الإلكتروني لأي غرض يخالف السياسات، الإجراءات أو الأوامر الإدارية للجمعية يعرض المستخدم للمساءلة.

5.4 إن مرفقات البريد الإلكتروني هي المصدر الرئيسي لفيروسات الحاسوب وينبغي التعامل معها بمنتهى الحذر.

5.5 يمنع تبادل كلمات مرور حساب البريد الإلكتروني مع شخص آخر، أو محاولة الحصول على كلمة مرور حساب البريد الإلكتروني لشخص آخر. حيث إن حسابات البريد الإلكتروني هي فقط لاستخدامها من قبل المستخدم المسجل.

6. المراقبة والسرية

6.1 تعود ملكية البريد الإلكتروني للجمعية. وهذا يعطي الجمعية الحق في مراقبة أي وكل حركات البريد الإلكتروني التي تمر من خلال النظام. قد تشمل هذه المراقبة وليس على سبيل الحصر:

6.2 يتم أرشفة البريد الإلكتروني وحفظ نسخ احتياطية على الرغم من إنتهاء خدمات صاحب الحساب، وذلك لمدة خمسة أعوام، لمنع فقدان بيانات الأعمال، وتلبية احتياجات العمل التنظيمية والقانونية، وتوفير المعلومات التجارية.

6.3 إذا كان هناك سبب وجيه للشك في الأنشطة التي لا تتوافق مع القوانين المعمول بها لهذه السياسة، قد يتم استرجاع سجلات البريد الإلكتروني واستخدامها لتوثيق النشاط وفقًا للإجراءات القانونية الواجبة. وسيتم إخطار الموظف بذلك إذا كان ممكنًا وإن لم يكن ممكنًا لأي سبب فسيتم استرجاع السجلات دون الرجوع للموظف.

7. الإبلاغ عن إساءة حدثت من خلال البريد الإلكتروني

7.1 ينبغي الإبلاغ عن أي إساءات مستلمة من خلال البريد الإلكتروني فورًا إلى قسم تقنية المعلومات. إذا كان الموظف قد تلقى رسالة هجومية، فلا يجوز إعادة إرسالها، حذف، أو الرد عليها. بدلًا من ذلك، تقدم مباشرة إلى رئيس قسم تقنية المعلومات للبحث فيها.

7.2 لا تتحمل الجمعية أية مسؤولية عن الأضرار المباشرة / أو غير المباشرة الناجمة عن استخدام المستخدم لخدمات البريد الإلكتروني. المستخدم وحده المسؤول عن المحتوى الذي نشر. الجمعية ليست مسؤولة عن أي دعوى أو مطالبة من أي طرف خارجي، أو ضرر ناجم عن استخدام خدمات البريد الإلكتروني الجمعية.

8. عدم الامتثال للسياسة

8.1 سيتم التعامل مع عدم الالتزام بهذه السياسة كغيرها من المخالفات المرصودة بالجمعية وبما يتوافق مع نظام العمل والأنظمة المتبعة الأخرى.

المادة (4): الإجراءات ذات العلاقة

1. إنشاء بريد إلكتروني، ويكون ذلك باتباع الخطوات التالية:

1.1 عند تعيين موظف أو الحاجة لإنشاء بريد إلكتروني لأغراض العمل يقوم مقدم الطلب باستكمال نموذج إنشاء بريد إلكتروني.

1.2 يتم تقديم الطلب إلى مدير الإدارة المعنية والحصول على موافقته.

1.3 يتم تقديم الطلب إلى المدير التنفيذي للجمعية والحصول على موافقته.

1.4 يقوم المدير التنفيذي للجمعية بالتوجيه لمدير إدارة التميز المؤسسي ومنه إلى رئيس قسم تقنية المعلومات لإنشاء البريد الإلكتروني.

1.5 يقوم موظف تقنية المعلومات بإنشاء البريد الإلكتروني واطلاع الموظف على سياسة البريد الإلكتروني وتسليمه له.

2. إيقاف بريد إلكتروني، ويكون ذلك باتباع الخطوات التالية:

2.1 يتم التنسيق بين إدارة التميز المؤسسي وإدارة الشؤون الإدارية والمالية للتأكد من احتواء نموذج إخلاء طرف الموظف على تسليم البريد الإلكتروني الخاص بالجمعية.

2.2 عند الحاجة لإيقاف بريد إلكتروني إما باستقالة الموظف أو انتهاء العلاقة مع صاحب البريد الإلكتروني، يقوم الموظف باستكمال الخطوات اللازمة لتسليم البريد الإلكتروني كما هو معتمد في نموذج إخلاء الطرف

2.3 يقوم موظف تقنية المعلومات باستلام البريد الإلكتروني والتنسيق مع مدير الموظف المنتهية العلاقة معه للتأكد من الحاجة لاستمرار عمل البريد الإلكتروني أو إيقافه نهائيًا.

الفصل رقم (2): البرامج والأنظمة الإلكترونية

المادة (5): هدف ونطاق السياسة

1. تهدف هذه السياسة إلى ضبط الأعمال الخاصة بالبرامج والأنظمة المستخدمة في الجمعية.
2. تنطبق هذه السياسة على جميع البرامج والأنظمة المستخدمة في الجمعية.

المادة (6): المسؤولية

1. مسؤولية صيانة وتحديث البرامج والأنظمة وكذلك إدارتها تقع على عاتق قسم تقنية المعلومات.
2. مسؤولية دقة البيانات في البرامج والأنظمة تقع على عاتق مستخدمي البرامج والأنظمة.

المادة (7): السياسات المنظمة

1. يمنع إعطاء صلاحيات تحميل البرامج للمستخدمين وتقتصر الصلاحية فقط لموظفي قسم تقنية المعلومات.
2. إن شراء أية أنظمة جديدة أو برمجيات هي فقط من صلاحيات قسم تقنية المعلومات.
3. جميع الأنظمة والبرامج المزودة للمستخدمين هي من ممتلكات الجمعية.
4. يمنع استخدام أية نسخ غير أصلية في الجمعية لتجنب المخالفات التي من الممكن أن تتسبب في المساءلة القانونية للجمعية.
5. لا يفضل شراء نسخ البرامج الفردية التي لا يمكن استخدامها إلا مرة واحدة والتوجه إلى نسخ المنظمات التي تتيح الاستخدام المتكرر للبرامج.
6. في حالة طلب تطوير برنامج جديد من الإدارات أو الأقسام في الجمعية لتسهيل العمليات فإن الطلب يقدم إلى صاحب الصلاحية للاعتماد تطوير البرنامج قبل بدء التطوير من قبل قسم تقنية المعلومات.
7. في حالة طلب أي من البرامج الجاهزة فيجب أن تقوم قسم تقنية المعلومات من التحقق من البرنامج ومراعاة ملائمته لمتطلبات الإدارة المعنية بالإضافة إلى اندماجه في الأنظمة المستخدمة حاليًا في الجمعية.
8. في حالة عدم الاحتياج للبرنامج كاستقالة الموظف أو لإي سبب كان، يجب إعلام قسم تقنية المعلومات لاتخاذ الإجراء اللازم وإزالة البرنامج عن جهاز المستخدم.

المادة (8): الحوسبة السحابية

1. يمكن أن يتم اتخاذ القرار باستخدام الحوسبة السحابية بموافقة صاحب الصلاحية كما هو موضح في مصفوفة الصلاحيات.
2. قبل اتخاذ القرار باستخدام الحوسبة السحابية يجب على قسم تقنية المعلومات دراسة القرار من منظمة الأمن السيبراني ومن المنظور التجاري ومن المنظور التقني قبل تقديم التوصية إلى مدير إدارة التميز المؤسسي ومنه إلى المدير التنفيذي للجمعية وصاحب الصلاحية في اختيار التقنية.

الفصل رقم (3): الدعم الفني

المادة (9): هدف ونطاق السياسة

1. تهدف هذه السياسة إلى ضمان تسهيل أعمال مستخدمي تقنية المعلومات في الجمعية، ومواجهة المشاكل والملاحظات التي تواجههم أثناء تنفيذ أعمالهم.
2. يتم تطبيق هذه السياسة على كامل طلبات الدعم الفني التي تصل إلى قسم تقنية المعلومات.

المادة (10): المسؤولية

1. يقع تطبيق هذه السياسة على عاتق مدير قسم تقنية المعلومات، ويجب على قسم تقنية المعلومات توفير موظف للدعم الفني لموظفي الجمعية.
2. مدير قسم تقنية المعلومات هو المسؤول الفني عن جميع عمليات الشراء للأجهزة والشبكات من الناحية الفنية.

المادة (11): السياسات المنظمة

1. يحتفظ قسم تقنية المعلومات بسجل لطلبات الدعم الفني، بحيث يتم تسجيل كامل طلبات الدعم الواردة لقسم تقنية المعلومات، ويتم متابعة التنفيذ من خلال هذا السجل.
2. لدى وصول طلب دعم فني، سوف يتولى قسم تقنية المعلومات محاولة حل المشكلة من خلال الهاتف وحتى للوصول إلى جهاز الحاسوب عن بعد، إذا استمرت المشكلة، سيقوم موظف قسم تقنية المعلومات بزيارة موقع المشكلة ومباشرة الحل.
3. ليس من ضمن مسؤولية قسم تقنية المعلومات إصلاح أجهزة الحاسوب الشخصية أو الأجهزة الطرفية الشخصية للموظفين في الجمعية.
4. يقدم الدعم الفني على ما يلي:

4.1 Hardware Support: يتم توفير الدعم لجميع الأجهزة الحاسوب، بما في ذلك اللوحات الرئيسية (MainBoards)، والأجهزة الطرفية، وكروت الشبكة، والأقراص الصلبة، وأجهزة التخزين،...إلخ. وسيتم تشخيص جميع حالات مشاكل الأجهزة المشتبه بها وفقًا لذلك. وسيقوم موظف قسم تقنية المعلومات بإصلاح عيوب الأجهزة بأفضل ما يمكن، وحيثما كان ممكنًا، سيتم إعطاء بديل للمستخدم في حالات الضرورة.

4.2 Software Support: يتم توفير الدعم لجميع البرامج الأساسية وأنظمة التشغيل المثبتة على أجهزة الحاسوب والخوادم وأجهزة الحاسوب المحمولة والتي تكون قد حملت من خلال فريق تقنية المعلومات، وتستبعد جميع البرامج غير المعتمدة أو غير الأصلية أو الألعاب أو خلفيات سطح المكتب أو أية برامج لا يتواجد لها دعم من الشركة المصنعة.

4.3 Remote Support: تدار جميع عمليات الاتصال عن بعد مركزيًا من قبل قسم تقنية المعلومات.

4.4 Network&Security Support: تدار جميع العمليات الخاصة بالشبكة أو الخوادم و العمليات الخاصة بحماية الشبكة من عمليات القرصنة بشكل مركزي من قبل قسم تقنية المعلومات، وذلك لضمان خدمة أفضل ونظرًا لإهمية العمليات و تقليص مشاكلها وعلى فريق المساندة الفنية تعيين تذكرة لفريق الشبكات موضحا المشكلة.

5. يجب أن يقوم قسم تكنولوجيا المعلومات بإعطاء الأهمية المطلوبة للمشاكل التقنية التي تواجه أعمال الجمعية، وفيما يلي أهم وصف لأهم المشكلات التقنية:

الأولويات	الوصف
عالية	المشاكل التي تمنع المستخدم من العمل المتواصل. مثل: • تعطل الموقع الإلكتروني للجمعية والخدمات التي تقدم من خلاله. • تعطل البرامج أو البريد الإلكتروني ولا تعمل لعدة مستخدمين. • نظام تشغيلي WINDOWSمعطل. • الشبكة لا تعمل لعدة مستخدمين.
متوسطة	المشاكل التي يمكن للمستخدم مواصلة العمل وذات أثر جزئي. مثل: • عدوى الفيروسات لجهاز مستخدم واحد. • وظيفة رئيسية من جهاز الحاسوب ليس التشغيلية لمستخدم واحد. • عدم إمكانية فتح ملف مهم من قبل المستخدم رغم صلاحيته للولوج إليه.
منخفضة	ليست بالمشاكل التي تعطل سير العمل على الإطلاق • أسئلة الموظفين عن آلية عمل وظيفة معينة. • مساعدة في تشغيل برنامج معين. • طلبات التطوير والتحسين وارتقاء النسخ المستخدمة.

6. يمنع منعًا باتًا عمل أية تغييرات أو إصلاحات دورية على الشبكة أو على أي من الخدمات الرئيسية والتي تؤثر على سير العمل في أوقات العمل الرسمية ويجب رفع طلب بفترة لا تقل عن ثلاثة أيام واعتمادها من قبل مدير قسم تقنية المعلومات لتنفيذها. وتشمل ما يلي:

6.1 معدات وأجهزة الشبكة (Routers, Switches, ...)

6.2 خوادم الجمعية كافة والخدمات التي تقدمها.

6.3 إصدار أو تعديل إحدى خدمات الموقع الإلكتروني أو الأنظمة المحوسبة.

الفصل رقم (4): الحماية من الفيروسات

المادة (12): هدف ونطاق السياسة

1. تهدف هذه السياسة إلى توفير إرشادات بشأن التدابير التي يجب اتخاذها من قبل الموظفين للمساعدة في تحقيق الكشف عن الفيروسات بطريقة فعالة والوقاية منها.
2. تنطبق هذه السياسة على كافة أجهزة الحاسوب التي تتصل عبر الاتصال السلكي لشبكة الجمعية، اتصال لاسلكي، اتصال مودم، وهذا يشمل كل من أجهزة الحاسوب المملوكة للجمعية وأجهزة الحاسوب المملوكة شخصيًا متصلًا بشبكة الجمعية.

المادة (13): المسؤولية

1. تقع مسؤولية حفظ الشبكة والخوادم الرئيسية ومنع دخول الفيروسات إلى الشبكة الداخلية على قسم تقنية المعلومات.
2. يجب على قسم تكنولوجيا المعلومات تحميل برنامج مكافحة الفيروسات على أجهزة الجمعية كافة، وإبقائه محدثًا، وبإصدارات جديدة، وفعالة.
3. تقع مسؤولية حماية الأجهزة من تنزيل ملفات مصابة والتأكد من مصادر حصوله للملفات على عاتق مستخدم الجهاز.

المادة (14): السياسات المنظمة

1. يجب أن يتم تحميل أجهزة الجمعية بنفس برنامج مكافحة الفيروسات ليتسنى لقسم تقنية المعلومات إدارة ومراقبة الاختراقات التي تحصل على الأنظمة. هذا البرنامج يجب أن يكون نشطًا، ويتم جدولة اختبارات إصابة الأجهزة بالفيروسات وعند نهاية الاختبار يقدم تقرير عن الوضع العام.
2. يتم إيجاد برنامج إدارة حماية الأجهزة على خادم الجمعية وتتابع الأجهزة المصابة من خلاله.
3. يمنع إعطاء صلاحية تشغيل وإقفال برنامج مكافحة الفيروسات للمستخدمين.
4. إذا شك الموظف أن جهاز الكمبيوتر مصابا بفيروس، يجب إعلام قسم تقنية المعلومات على الفور، ولا يجوز للموظف محاولة تدمير أو إزالة فيروس، أو أي دليل على أن الجهاز مصاب بفيروس، دون توجيه من قسم تقنية المعلومات.
5. قواعد الوقاية من الفيروسات، على الموظف دائمًا التأكد من: -
   - 5.1 أن برنامج مكافحة الفيروسات يعمل.
   - 5.2 عدم فتح أي ملفات أو وحدات الماكرو مرفقة برسالة بريد إلكتروني من مصدر مجهول أو مشبوه.
   - 5.3 فحص الملفات بحثًا عن الفيروسات قبل استخدامه.
   - 5.4 عدم النقر على الروابط المرفقة في الإيميلات قبل فحصها لأنها قد تحتوي على فيروسات قابلة للتنفيذ (.exe)

5.5 عدم تنزيل أو نسخ أو تثبيت الملفات من مصادر غير معروفة، مشبوهة، أو غير جديرة بالثقة أو الوسائط القابلة للتغيير مثل (الأقراص الممغنطة CD, DVD, Blueray، الأقراص الصلبة الخارجية، Flash Memory، وغيرها)

5.6 إذا تم التوجيه بحذف رسائل البريد الإلكتروني يعتقد أنها تحتوي على فيروس، على الموظف أن يتأكد أيضًا من حذف الرسالة من العناصر المحذوفة أو من سلة المهملات.

الفصل رقم (5): استخدام الإنترنت

المادة (15): هدف ونطاق السياسة

1. تهدف هذه السياسة إلى ضمان الاستخدام السليم للإنترنت لتعزيز غايات وأهداف الجمعية.
2. كما تهدف إلى الحد من الاستخدام غير السليم للإنترنت بحيث يؤثر على سير العمل في الجمعية.

المادة (16): المسؤولية

1. تقع على عاتق قسم تقنية المعلومات مسؤوليات حماية الشبكة الداخلية من الأخطار التي تنتشر من خلال شبكة الإنترنت كاستخدام:
   - 1.1 Firewall والمعروف أحيانًا بالجدار الذي يقوم بفلترة البيانات الصادرة والواردة.
   - 1.2 Proxy والذي يقوم بمراقبة الاتصالات لكل جهاز حاسب مربوط على الشبكة الداخلية.
   - 1.3 Content Filteration وهو الذي يحدد ويمنع بعض جهات الاتصال.
2. تقع على عاتق قسم تقنية المعلومات مسؤوليات توفير وزيادة خطوط أو سرعات الاتصال بالإنترنت عند الحاجة.

المادة (17): السياسات المنظمة

1. لحماية سلامة شبكة الجمعية والبيانات المحفوظة على شبكتها فإن قسم تقنية المعلومات سيراقب استخدام الإنترنت، وكافة البيانات التي تمر من خلال شبكة الجمعية وكذلك جميع أجهزة الحاسوب.
2. الجهات المخولة لمراجعة تقرير تصفح الإنترنت هم مسؤول النظام، والإدارة العليا، ويتم التعامل مع التقارير بسرية تامة.
3. في حال إثبات أي استخدام غير لائق أو تعرض أي من أجهزة الجمعية للإختراق وإصابته بالفيروسات من خلال الاستخدام الخاطئ للإنترنت سيتم تصعيد الحالة للإدارة المعنية للتحقيق في الحالة وحصر المواقع المشبوهة التي تم زيارتها من خلال خدمات الإنترنت المقدمة من الجمعية.
4. لا يسمح لموظفي الجمعية تصفح، نقل، تحميل، تنزيل، طباعة أو عرض أو نشر الأنواع التالية من المواد على شبكة تقنية المعلومات الخاصة بالجمعية:
   - 4.1 صور أو أي مادة إعلامية خادشة بالحياء العام.
   - 4.2 المواد التي تحتوي على السب العلني أو المواد الهجومية، وتشجيع العنف، والتعصب، والكراهية.
   - 4.3 المواد غير القانونية أو مواقع الاحتيال.
   - 4.4 أي بيانات قابلة لتحويلها إلى أي من المواد المسيئة خلقيًا وأخلاقيًا.

   سيتم التعامل مع هذه المواد بعدم السماح لها من المرور من خلال الشبكة، ولكن لكثرة وتعدد هذه الأنواع فعلى الموظفين إعلام الدعم الفني عند ملاحظتها.

5. يحتفظ قسم تقنية المعلومات بحق منع الوصول إلى مواقع الإنترنت وإغلاق البروتوكولات التي يتم الظن بأنها غير لائقة للمرور من شبكة الجمعية، ومن الأمثلة على ذلك منع البروتوكولات والفئات الآتية:
   5.1 المواقع والمواد الخادشة بالحياء العام.
   5.2 مواقع التواصل الإجتماعي والفيديوهات والأغاني.
   5.3 مواقع المقامرة.
   5.4 مواقع التجسس.
   5.5 مواقع بيع الأدوية المحظورة.
   5.6 مواقع تبادل الملفات
   5.7 مواقع تكثر فيها SPAM, phishing والاحتيال.
   5.8 مواقع يكثر فيها القذف والمقالات العنصرية.

6. يقوم قسم تقنية المعلومات بتفعيل برامج الفلترة الخاصة بالجدار الناري للشبكة، وتفعيل دور ال Proxyبحيث يتم الولوج للإنترنت من خلال حسابات للمستخدمين، وكذلك تفعيل سياسة استخدام الإنترنت بالتحقق من بيانات المستخدم من خلال Active Directory.

7. لأغراض أمنية، على المستخدمين عدم مشاركة معلومات الحساب أو كلمة المرور للوصول إلى الإنترنت مع شخص آخر، حسابات الإنترنت يجب أن تستخدم فقط من قبل المستخدم المصرح له للإغراض المصرح بها فقط. والمحاولة لاستخدام حسابات أشخاص آخرين ممنوع بشكل قطعي وفي حالة إثبات ذلك من تقرير تدفق البيانات فإن الموظف يعرض نفسه للمساءلة.

8. إذا ظن الموظف بإن اسم المستخدم وكلمة المرور الخاصة به يتم استخدامها من قبل شخص آخر فعليه إبلاغ قسم تقنية المعلومات لإعادة تعيين كلمة مرور جديدة.

9. سيتم التعامل مع انتهاكات سياسة استخدام الإنترنت مثل غيرها من المخالفات في الجمعية. وقد تشمل، ولكنها لا تقتصر على، واحد أو أكثر من الإجراءات التأديبية وفقًا للسياسات المطبقة في الجمعية، و / أو اتخاذ إجراءات قانونية وفقًا للقوانين المعمول بها والاتفاقات التعاقدية.

10. إن أي مواقع مغلقة ويوجد هناك حاجة لفتحها لغايات العمل فسيتم فتحها بعد دراسة المتطلب والتأكد من خلوه من المواد الضارة شريطة اعتماده من مدير الإدارة المعنية.

الفصل رقم (6): الجدار الناري (Fire wall)

المادة (18): هدف ونطاق السياسة

1. تهدف هذه السياسة إلى وصف كيفية عمل الجدار الناري (Firewalls) في الجمعية لتنقية حركة مرور البيانات الآتية من الإنترنت من أجل التخفيف من حدة المخاطر والخسائر المرتبطة بالتهديدات الأمنية على شبكة الجمعية الداخلية مع الحفاظ على مستويات مناسبة من الولوج إلى شبكة الإنترنت.
2. هذه السياسة تشير بشكل مباشر إلى دور الجدار الناري في تحديد الدخول إلى موارد الإنترنت والإنذار عند وجود أي هجوم ووصف الحد الأدنى المتطلب من عمله بالإضافة إلى التقارير اللازمة منه. ويعتبر الحد الأدنى من الخدمات الأمنية التي من المتوقع الحصول عليها بتطبيق الجدار الناري ما يلي: -
   2.1 السيطرة على حركة البيانات بين الشبكة الداخلية الموثوق بها وشبكة الإنترنت غير الموثوق بها.
   2.2 منع حركة البيانات غير المرغوب بها من وإلى شبكة الإنترنت.
   2.3 إخفاء الأنظمة الداخلية المستضعفة من الإنترنت.
   2.4 إخفاء المعلومات، مثل أسماء النظام، بنية الشبكة، أسماء ورموز المستخدمين.
   2.5 تسجيل حركة البيانات من وإلى الشبكة الداخلية.
   2.6 توفير مصادقة قوية بمطابقة المصرحين لهم باستخدام الإنترنت.
   2.7 توفير شبكة خاصة الربط الظاهري (VPN).
3. تتضمن نطاق هذه السياسة كافة الأجهزة المرتبطة بشبكة الجمعية الداخلية.

المادة (19): المسؤولية

1. تقع مسؤولية تشغيل الجدران النارية (Firewalls) بين الإنترنت والشبكة الداخلية للجمعية على عاتق قسم تقنية المعلومات من أجل خلق بيئة عمل آمنة لأجهزة الجمعية وموارد الشبكة الأخرى. الجدار الناري هو مجرد عنصر واحد من منهج أمن وحماية الشبكات.
2. تمنح صلاحية الدخول إلى برنامج التحكم بالجدار الناري فقط لرئيس قسم تقنية المعلومات وذلك من خلال كلمة سر ثابتة لجميع أجهزة الجدار الناري على أن تكون كلمة سر قوية وصعبة كما هو مبين في سياسة كلمات المرور.

المادة (20): التعاريف

1. الجدار الناري: هي مجموعة من الأجهزة أو البرامج المرتبطة بالشبكة، وتقع في خادم بوابة الشبكة، تقوم بحماية موارد الشبكة الخاصة من مستخدمين من الشبكات الأخرى. (يتضمن هذا المصطلح أيضًا السياسة الأمنية التي يتم استخدامها مع البرامج). الجدار الناري قد يمنح / يبطل الوصول استنادًا إلى مصادقة المستخدم، مصدر وعنوان الشبكة الوجهة، والوقت من اليوم، وخدمة الشبكة أو أي مزيج من هذه. كما يمكن أن يعمل كمفلتر ليكون بمثابة تصفية للمحتوى.
2. VPN: هو عبارة عن شبكة تستخدم البنية التحتية للاتصالات العامة، مثل الإنترنت، لتزويد المكاتب البعيدة أو المستخدمين الفرديين لوصول آمن إلى شبكة الجمعية الداخلية. وتعتبر VPN شبكة افتراضية خاصة تقدم من خلال مزود الإنترنت أو من خلال شراء أجهزة خاصة وتفعيلها بين نقطتين وحاليًا أصبحت إحدى خدمات الجدار الناري.

المادة (21): السياسات المنظمة

1. المنهج المتبع لتحديد مجموعة القواعد للجدار الناري هو رفض جميع البروتوكولات وتداول البيانات وتصفح الإنترنت إلا ما هو مسموح به صراحة في هذه السياسة. الجدار الناري يسمح بحركة البيانات الصادرة والواردة حسب الآتي:
   1.1 الصادر: جميع حركة البيانات لخدمات الإنترنت الخارجة من الجمعية.
   1.2 الوارد: فقط حركة البيانات التي تدعم مهام الأعمال في الجمعية.
2. يسمح بفتح البروتوكلات أو الخدمات المغلقة من خلال الجدار الناري في حالة طلبها من قبل الموظفين واعتمادها من قبل رئيس قسم تقنية المعلومات بعد دراسة الحالة، ويتم اعتمادها فقط على أن تكون ضمن حدود مخاطر مقبولة وإلا يتم رفضها مع توضيح السبب وتبيين المخاطر من ذلك مع إعطاء حلول بديلة.
3. يمكن للموظفين طلب الوصول من الإنترنت للخدمات الموجودة على الشبكة الداخلية وذلك من خلال خدمة ال VPN التي تتيح التواصل الآمن للخدمات الداخلية عن بعد.

المادة (22): الإجراءات ذات العلاقة

1. **طلب استثناء خدمات مغلقة بالجدار الناري، ويكون ذلك باتباع الخطوات التالية:**
   1.1 عند الحاجة لفتح البروتوكلات أو الخدمات المغلقة من خلال الجدار الناري يتم طلب الخدمة من قبل صاحب الحاجة من خلال إنشاء بطاقة دعم فني.
   1.2 يقوم موظف تقنية المعلومات بالحصول على موافقة رئيس قسم تقنية المعلومات.
   1.3 يقوم رئيس قسم تقنية المعلومات بالموافقة على الطلب بعد دراسته والنقاش مع الأطراف المعنية حيث يلزم.
   1.4 يقوم موظف تقنية المعلومات بتفيذ الإجراء المطلوب.
   1.5 يتم توثيق العملية والموافقات اللازمة ضمن سجل خدمات قسم تقنية المعلومات.

الفصل رقم (7): كلمة المرور أو كلمة السر (Password)

المادة (23): هدف ونطاق السياسة

1. الهدف من هذه السياسة هو توفير المبادئ التوجيهية اللازمة لجميع العاملين في الجمعية لإنشاء كلمات مرور مناسبة واستخدامها وحمايتها بطريقة مناسبة.
2. كلمة المرور هي عنصر مهم في أمن البيانات والشبكات، استخدام تركيبة اسم المستخدم وكلمة المرور تعمل على تحديد ومصادقة عمل المستخدم على الأنظمة المختلفة في الجمعية والوصول إلى المعلومات، وتعتبر عملية المصادقة على دخول المستخدم لأنظمة الجمعية الحل الأجدر بالثقة بأن الأنظمة والبيانات تستخدم بشكل مناسب لمتطلبات العمل، ولذلك كلمة المرور يجب أن تبنى وتحمى وتستخدم بطريقة صحيحة لضمان مستويات عالية على أمن المعلومات.
3. تنطبق هذه السياسة على جميع موظفي الجمعية الذين لديهم أي شكل من أشكال حسابات التطبيقات أو الحاسوب الذي يتطلب كلمة مرور. أمثلة من الحسابات ما يلي:
   - 3.1 أجهزة اللابتوب وأجهزة الحاسوب المكتبية.
   - 3.2 الشبكة الداخلية أو الإنترنت.
   - 3.3 نظام البريد الإلكتروني.
   - 3.4 الموقع الإلكتروني للجمعية.

المادة (24): المسؤولية

1. تقع المسؤولية على عاتق المستخدمين لاتباع المبادئ التوجيهية في بناء كلمة المرور.
2. تقع المسؤولية على عاتق المستخدمين لحماية كلمة المرور الخاصة بهم وعدم تناقلها بين الأفراد.
3. تقع المسؤولية على عاتق قسم تقنية المعلومات لضمان تنفيذ هذه السياسة بشكل صحيح وبشكل آلي.

المادة (25): السياسات المنظمة

1. كلمة السر هي تسلسل من الحروف أو الأرقام أو الرموز غير متباعدة تستخدم لتحديد مستخدم الحاسوب الذي يطلب الوصول إلى نظام الحاسوب فيما إذا كان هو حقًا المستخدم بعينه. بشكل نموذجي الحاسوب أو نظام المستخدم محمي بشكل آمن باسم فريد (غالبًا ما يسمى هوية المستخدم) الذي يمكن أن يكون ظاهرًا وذلك من أجل التحقق من هوية المستخدم، أما كلمة السر، لا يعرفها سوى المستخدم، يتم إنشاؤها من قبل المستخدم وتكون دائمًا مخفية اعتماداً على كيفية إعداد الإنظمة.
2. إنشاء كلمة المرور وإعادة استخدامها تكون متغيرة وفقًا لتصنيف الأنظمة أو البيانات المراد حمايتها.
3. لا ينبغي أن تستند كلمات المرور على معلومات معروفة أو يمكن الوصول إليها بسهولة، بما في ذلك المعلومات الشخصية، أو أن تكون إحدى الكلمات القياسية.
4. يجب أن تتكون كلمات المرور المستخدمة للوصول إلى بيانات مصنفة على أنها "سرية" أو النظم التي تستضيف هذه البيانات من ثمانية رموز كحد أدنى باللغة الإنجليزية، علاوة على ذلك، يجب استخدام كافة أشكال الحروف (Upper case and Lower Case) والأرقام والرموز الخاصة.

5. يجب أن تتكون كلمات المرور المستخدمة للوصول إلى بيانات مصنفة على أنها "خاصة" أو النظم التي تستضيف هذه البيانات من ستة رموز كحد أدنى باللغة الإنجليزية، علاوة على ذلك، يجب استخدام كافة أشكال الحروف (Upper case and Lower Case) والأرقام والرموز الخاصة.
6. ليست هناك حاجة لكلمات السر للوصول إلى البيانات المصنفة على أنها "عامة" أو النظم التي تستضيف هذه البيانات.
7. مدة صلاحية كلمة المرور لا يمكن أن تزيد عن مائة وثمانين يومًا (ستة أشهر) ولا يمكن إعادة إدخالها مرة أخرى إلا بعد مرور 3 استخدامات لكلمات مرور أخرى على الأقل.
8. يتم إخطار المستخدمين برسالة إلكترونية بانتهاء صلاحية كلمة المرور قبل إسبوع من نهاية صلاحيته، وتبقى الرسالة ظاهرة عند كل دخول لاحق حتى يتم إجراء تغيير باختيار كلمة مرور جديدة.
9. تعامل كلمات المرور على أنها معلومات سرية. تحت أي ظرف من الظروف لا يجوز للموظفين إفشاء كلمة المرور الخاصة بهم أو الإشارة إليها إلى شخص آخر، بما في ذلك موظفي قسم تقنية المعلومات، والإداريين والرؤساء، وغيرهم من زملاء العمل والأصدقاء وأفراد الأسرة.
10. تحت أي ظرف من الظروف لا يجوز طلب كلمة المرور من موظفي قسم تقنية المعلومات إلا بموجب طلب رسمي يقدم لقسم تقنية المعلومات ومعتمد من مدير إدارة الموظف وفي هذه الحالة يتم إعادة إنشاء كلمة مرور جديدة.
11. لا يجوز الاحتفاظ بكلمة المرور بسجل مكتوب غير محمي إن كان ورقي أو ملف إلكتروني، وإن كان من الصعب على الموظف تذكر كلمة المرور الخاصة به فعليه حمايته في مكان آمن إن كان مكتوب ورقيًا أو أن يكون مشفرًا إن كان محفوظ في ملف إلكتروني.
12. إذا كان الموظف يعرف أو يشتبه أنه تم اختراق كلمة المرور الخاصة به، فإنه لا بد من إخبار قسم تقنية المعلومات وتغيير كلمة المرور على الفور، أما إذا لم يستطع الموظف تغيير كلمة المرور الخاصة به فسيقوم قسم تقنية المعلومات بإعادة تعيين كلمة مرور مؤقتة للمستخدم لإنشاء كلمة مرور جديدة بنفسه.

الفصل رقم (8): أجهزة الحاسوب المكتبية (Desktop Computers)

المادة (26): هدف ونطاق السياسة

1. تهدف هذه السياسة إلى حماية أجهزة الحاسوب المكتبية والرقابة عليها بشكل مناسب.
2. تطبق هذه السياسة على كافة الأجهزة المكتبية في جمعية درة.

المادة (27): المسؤولية

4. تقع مسؤولية تحميل البرامج والإعدادات على عاتق قسم تكنولوجيا المعلومات، وتكون االأجهزة محصنة باسم مستخدم وكلمة مرور خاصة بالدعم الفني للتمكن من الوصول إلى الحاسوب المكتبي في حال فقدان كلمة المرور الخاصة بالمستخدم.
5. تقع مسؤولية تحديد مواصفات الأجهزة على عاتق قسم تقنية المعلومات وفقًا للمعايير المثبتة للأجهزة.

المادة (28): السياسات المنظمة

1. قبل تسليم أي جهاز حاسوب مكتبي على الموظف توقيع نموذج الحصول على جهاز حاسوب مكتبي والموافقة على السياسة الخاصة به.
2. لا يجوز شراء أي جهاز كمبيوتر مكتبي دون تعميد قسم تقنية المعلومات والتأكد من مطابقته للمواصفات الواجب توفرها لتلبية عمل الموظف.
3. يتم تحديد مواصفات الأجهزة بناءً على طبيعة عمل الموظف.
4. لا تعطى أية صلاحيات لتثبيت أو تحميل البرامج للموظف، ولكن يتم ذلك بالرجوع إلى قسم تقنية المعلومات للمساعدة.
5. لا يتم تحميل أي من أجهزة الجمعية بنسخ لبرامج ليست أصلية وأية متطلبات يتم طلبها حسب سياسة البرامج الإلكترونية.
6. على الموظف الحرص من أن برنامج الحماية من الفيروسات مثبت ومحدث ويعمل بصورة صحيحة.
7. على الموظف إطفاء الجهاز عند مغادرة المكتب.
8. يتم إستبدال الأجهزة في الحالات الآتية: -

8.1 أن يكون عمر الجهاز أكثر من خمسة سنوات ولا يعمل بشكل يلبي احتياجات العمل.

8.2 أن تكون مواصفات الجهاز لا تلبي المتطلبات الأساسية لتشغيل البرامج ولا يمكن رفع مواصفاته لتلبية المتطلبات.

8.3 أن يكون الجهاز قد تعطل ولا يمكن إصلاحه، وفي حال كان الموظف مسؤول عن تلف الجهاز نتيجة الإهمال أو الاستعمال الخاطئ فيتم إحتساب قيمة الجهاز السوقية وتغريمه بذلك.

الفصل رقم (9): أجهزة الحاسوب المحمولة (Laptops)

المادة (29): هدف ونطاق السياسة

1. تهدف هذه السياسة إلى حماية أجهزة الحاسوب المحمولة والرقابة عليها بشكل مناسب.
2. تطبق هذه السياسة على كافة أجهزة الحاسوب المحمولة في جمعية درة.

المادة (30): المسؤولية

1. تقع مسؤولية تحميل البرامج والإعدادات على عاتق قسم تكنولوجيا المعلومات، وتكون االأجهزة محصنة باسم مستخدم وكلمة مرور خاصة بالدعم الفني للتمكن من الوصول إلى الحاسوب المحمول في حال فقدان كلمة المرور الخاصة بالمستخدم.
2. تقع مسؤولية تحديد مواصفات الأجهزة على عاتق قسم تقنية المعلومات وفقًا للمعايير المثبتة للأجهزة.

المادة (31): السياسات المنظمة

1. قبل تسليم أي أجهزة حاسوب محمول على الموظف توقيع نموذج الحصول على جهاز حاسوب محمول والموافقة على السياسة الخاصة به.
2. لا يجوز شراء أي جهاز كمبيوتر محمول دون تعميد قسم تقنية المعلومات والتأكد من مطابقته للمواصفات الواجب توفرها لتلبية عمل الموظف.
3. جميع أجهزة الحاسوب المحمولة وتوابعها هي ملك الجمعية ويتم توفيرها للموظفين لفترة من الوقت. ويشترط من مستخدمي أجهزة الحاسوب المحمول أن يكون لأغراض العمل ويجب على الموظفين الامتثال والموافقة على كل ما يلي:
   3.1 يجب أن الموظفين عدم محاولة تثبيت البرامج أو تغيير تكوين النظام بما في ذلك إعدادات الشبكة دون الرجوع المسبق إلى قسم تقنية المعلومات.
   3.2 لن يكون الموظف مسؤولا عن مشاكل الحاسوب المحمول الناجمة عن الاستخدام العادي ذات الصلة بالعمل، ومع ذلك، سيكون الموظف مسؤولا عن أي مشاكل ناجمة عن إهماله.
   3.3 يحق لقسم تقنية المعلومات إمكانية الوصول إلى أي جهاز كمبيوتر محمول، و / أو الاكسسوارات التي تم إعطاؤها بناءً على طلب الإدارة.
4. إذا كانت البيانات الموجودة على الحاسوب المحمول مهمة وحرجة بالنسبة لاحتياجات العمل فيجب على الموظف أن يقوم بنسخ هذه البيانات على الملف الخاص به أو الملف الخاص بالإدارة الموجود على خادم الملفات الخاص بالجمعية.
5. على الموظف الحرص من أن برنامج الحماية من الفيروسات مثبت ومحدث ويعمل بصورة صحيحة حيث إن أجهزة الكبيوتر المحمولة أكثر عرضة للإصابة بالفيروسات لاتصالها بشبكات خارجية غير محمية.
6. على الموظف الحرص من عدم وضع المشروبات أو السوائل بجانب الجهاز المحمول تفاديًا للحوادث التي تؤدي إلى تلف الأجهزة

7. عدم ترك الحاسوب المحمول في السيارة وذلك لأن درجات الحرارة الشديدة أو التغيرات المفاجئة في درجات الحرارة تتلف جهاز الحاسوب المحمول.
8. عند استخدام الحاسوب المحمول يجب وضعه على سطح صلب ومسطح لتعميم دخول الهواء لتبريده ولا يجب وضعه على أسطح من القماش كالأسرة.
9. نظرًا للتنقل المستمر بأجهزة الحاسوب المحمولة فهي معرضة للسرقة أكثر من غيرها من الأجهزة ولذلك فعلى الموظف تفادي الحالات الآتية:
   9.1 عدم ترك جهاز الكبيوتر المحمول في السيارة وإن وجب ذلك فعليه وضعه في صندوق السيارة.
   9.2 حمل الجهاز المحول في الحقيبة المخصصة له في حالات السفر وعدم ترحيله مع حقائب السفر إلى داخل الطائرة.
   9.3 إقفال المكتب في حال عدم وجود الموظف أو تركيب القفل الخاص لربطه بالمكتب وفي حال تركه في المكتب عليه وضعه في خزانة وأن يكون مخفيا عن الأنظار وإغلاق الخزانة بمفتاح.
10. يتم إستبدال الأجهزة في الحالات الآتية: -
   10.1 أن يكون عمر الجهاز أكثر من أربعة سنوات ولا يعمل بشكل يلبي احتياجات العمل
   10.2 أن تكون مواصفات الجهاز لا تلبي المتطلبات الأساسية لتشغيل البرامج ولا يمكن رفع مواصفاته لتلبية المتطلبات
   10.3 أن يكون الجهاز قد تعطل ولا يمكن إصلاحه، وفي حال كان الموظف مسؤول عن تلف الجهاز نتيجة الإهمال أو الاستعمال الخاطئ فيتم إحتساب قيمة الجهاز السوقية وتغريمه بذلك

الفصل رقم (10): الطابعات

المادة (32): هدف ونطاق السياسة

1. تهدف هذه السياسة إلى وضع الضوابط لاستخدام الطابعات بحيث يقتصر استخدامها لأغراض العمل وأهدافه الجمعية.
2. تطبق هذه السياسة على جميع الموظفين الذين يحتاجون إلى خدمة الطابعات في مقر إدارة الجمعية أو أي مكان يخص العمل.

المادة (33): المسؤولية

1. يكون قسم تكنولوجيا المعلومات هو المسؤول عن تحديد مواصفات الطابعات ومتابعة سلامتها واستخدامها في أعمال الجمعية.
2. تقع مسؤولية تطبيق السياسة والالتزام بها على جميع موظفي الجمعية.
3. تقع المسؤولية على عاتق المستخدمين لاستخدام الطابعات بشكل فعال والمحافظة عليها وعدم استخدامها بشكل يؤدي إلى تعطيلها.

المادة (34): السياسات المنظمة

1. إن السياسة العامة للطابعات تقتضي باستخدام الطابعات المركزية بشكل أساسي وذلك لكفائتها العالية والتكاليف التشغيلية الفعالة لها.
2. يجوز بقرار من المدير التنفيذي استخدام طابعات لموظفين محددين لحاجة العمل.
3. يتم توفير الطابعات المركزية حسب متطلبات العمل وعلى النحو الآتي: -

المنطقة	توفر الطابعات في المنطقة
المدير التنفيذي للجمعية	طابعة A4 (Laser) متعددة الوظائف ملونة.
باقي موظفي الجمعية	طابعة A4 و3A (Laser) متعددة الوظائف مع إمكانية المسح الضوئي

4. لا يجوز شراء أي طابعة دون تعميد قسم تقنية المعلومات والتأكد من مطابقتها للمواصفات الواجب توفرها.
5. يجب توحيد خصائص الطباعة من جهة واحدة والتي تكون من قبل قسم تقنية المعلومات.
6. يجب ربط جميع الطابعات ببرنامج التحكم بالطابعات من قبل موظفين تقنية المعلومات وتعريف سعر النسخة لمراقبة تكاليف كل طابعة وإنشاء التقارير بشكل شهري وتوزيعها على المعنيين.
7. يجب وضع صلاحيات على الطابعات الملونة ومراقبة استخدامها شهريًا.
8. لا يجوز طبع الملفات الشخصية أو الصور الخاصة وسوف يتم تقديم تقارير دورية تظهر إساءة الاستخدام إلى الجهات المعنية كمدراء الإدارات لتنبيه أو إنذار الموظف الذي يسيس استخدام أصول الجمعية.

الفصل رقم (11): النسخ الاحتياطية

المادة (35): هدف ونطاق السياسة

1. يكمن الهدف من هذه السياسة إلى التركيز على حفظ بيانات الجمعية المخزنة سواءً كملفات على خادم الملفات (File Server) أو قواعد بيانات أو بريد إلكتروني كنسخ احتياطية وفي بعض الحالات من الممكن أخذ النظام بجميع محتوياته إذا كانت الإعدادات حرجة ويصعب إعادتها.
2. إيجاد معيار لعملية حفظ البيانات تبدأ من أجهزة الموظف إلى أجهزة الخادم الرئيسية في الجمعية.
3. إيجاد معيار لعملية إستخراج النسخ الاحتياطية على أقراص وآلية حفظها.
4. إيجاد معيار في عنونة الأقراص التي يتم إستخراج البيانات إليها.
5. تطبيق خطة النسخ الاحتياطي على كافة بيانات الجمعية للتأكد من توافر قواعد الأمن من حذف البيانات، وحفظ البيانات من السرقة وضمان السرية وبالتالي سهولة استرجعها.

المادة (36): المسؤولية

1. تقع مسؤولية تطبيق السياسة والالتزام بها على قسم تقنية المعلومات، ويخضع من يثبت بحقه التقصير إلى المساءلة في حال الاستهانة بها ومن أبرز المسؤوليات التي يجب القيام بها ما يلي:
   1.1 جدولة المواعيد لأخذ النسخ الاحتياطية وأخذ النسخ الاحتياطية حسب الجدول الزمني
   1.2 إلصاق البطاقات التعريفية على الأقراص ومن ثم إرسال الأقراص التي تم نسخ البيانات عليها إلى خارج الموقع.
   1.3 مراقبة الأخطاء التي تحدث في نظام النسخ الاحتياطية وإتخاذ الإجراءات التصحيحية.

المادة (37): السياسات المنظمة

1. التعاريف:
   1.1 النسخ الاحتياطية: هي نسخ يتم أخذها من الخادمات الرئيسية بهدف حماية البيانات من الضياع في أي من حالات الحريق، السرقة، الحذف المقصود أو الخاطئ، ويتم حفظ هذه النسخ في مكان آمن لمدة من الزمن بهدف الرجوع إليها عند الطلب.
   1.2 النسخ الاحتياطي الكامل: هذا النوع ينسخ جميع الملفات في النظام وملفات البرامج وملفات البيانات، إلا أن هذا النوع يحتاج إلى وقت طويل لنسخ الملفات ولا يمكن إجراءه بشكل يومي.
   1.3 النسخ الاحتياطي التزايدي: يعتمد هذا النوع على نسخ كامل لأول مرة ومن ثم ينسخ فقط الملفات التي تغيرت بعد آخر عملية نسخ كامل، ويمتاز بسرعة النسخ ويمكن إجراءه بشكل يومي، ولكن يحتاج إلى وقت أطول في إرجاع البيانات.
2. يتم عمل نسخة احتياطية تزايدية يومية لملفات الخادم الرئيسي في الجمعية.
3. يتم عمل نسخة احتياطية سحابية شهرية لكامل ملفات وأنظمة الجمعية.
4. يتم وبشكل سنوي عمل نسخة احتياطية لكامل ملفات وأنظمة الجمعية وحفظها في أقراص تخزين وحفظها خارج الجمعية.

الفصل رقم (12): الاتصال بالشبكة اللاسلكية

المادة (38): هدف ونطاق السياسة

1. الهدف من هذه السياسة حماية بيانات الجمعية الخاصة والسرية الموجودة على أجهزة الجمعية من خلال تحديد المعايير والإجراءات والقيود بالنسبة لطالبي الاتصال بشبكة الجمعية اللاسلكية، وكذلك إيجاد المعايير اللازمة للاتصال بالأجهزة التي ليست ملكا للجمعية ولا تخضع لمعايير وسياسات الحماية الخاصة بالجمعية.
2. تنطبق هذه السياسة على جميع طالبي الخدمة سواءً كانت على أجهزة كمبيوتر أو أجهزة إلكترونية خاصة بالجمعية ومضافة على خادم الجمعية أو أجهزة أخرى ليست ملكًا للجمعية وغير مضافة على خادم الجمعية.

المادة (39): المسؤولية

1. تقع مسؤولية تزويد الخدمة وتقديم الدعم الفني على عاتق قسم تقنية المعلومات.

المادة (40): السياسات المنظمة

1. تهدف الشبكات اللاسلكية لتوفير الاتصال بالشبكة في بيئات حيث شبكة الأسلاك ليست عملية أو المستخدمين كثيري التنقل أو الزوار الذين يحتاجون إلى اتصال بالإنترنت.
2. على قسم تقنية المعلومات تطبيق الخدمة بمدارات (VLAN) مختلفة بحيث يتم فصل شبكة الزوار عن شبكة موظفي الجمعية بحيث تكون شبكة الزوار مربوطة بشكل مباشر مع الجدار الناري للولوج إلى الإنترنت. أما شبكة الموظفين تسمح لتبادل البيانات مع الشبكة السلكية.
3. يجب أن تكون عملية الاتصال معرفة من خلال خادم الجمعية للتعرف على أجهزة الموظفين في حين يتم اتصال الزوار والأجهزة غير المعرفة من خلال كلمة مرور مؤقتة تدوم لفترات زمنية معينة.
4. في حال تعثر فصل شبكة الزوار فيجب الفصل الفعلي من خلال مزودي خدمة الإنترنت بحيث يكون هناك خط إنترنت خاص للزوار ولا علاقة له بشبكة الجمعية الداخلية ويتم ربط نقطة الاتصال اللاسلكي به مباشرة.
5. يجب فلترة وإغلاق كافة مواقع الإنترنت الغير مسموح بها حسب سياسة " استخدام الإنترنت" على الشبكة اللاسلكية سواءً كانت على شبكة العاملين أو حتى الزوار.
6. يتم التعامل مع الأجهزة الخاصة بالموظفين كما هو الحال للزوار إلا أن الموظف يحتاج إلى موافقة مسبقة من مدير الإدارة لتزويد الخدمة إليه.

الفصل رقم (13): الموقع الإلكتروني للجمعية

المادة (41): هدف ونطاق السياسة

1. الهدف من هذه السياسة ضبط وتنظيم الأعمال التي تحكم الرقابة على الموقع الإلكتروني للجمعية من حيث محتوياته وآلية التعديل عليها، وضمان تحقيق الموقع الإلكتروني للغايات التي أنشئ لأجلها في تسويق خدمات الجمعية والتعريف بها والعلاقة مع المستفدين والمتبرعين.
2. تنطبق هذه السياسة على جميع كافة الخدمات المقدمة من خلال الموقع الإلكتروني للجمعية، وكافة الأطراف ذات العلاقة بالموقع الإكتروني للجمعية.

المادة (42): المسؤولية

1. تقع مسؤولية ضبط ومراقبة الموقع الإلكتروني للجمعية على عاتق قسم تقنية المعلومات.

المادة (43): السياسات المنظمة

1. يتم تشغيل موقع الجمعية من خلال قسم تقنية المعلومات، ويتم توفير المعلومات اللازمة للموقع من قبل الأطراف ذات العلاقة، حيث يقوم قسم تقنية المعلومات بالإشراف على إدخالها للموقع الإلكتروني للجمعية.
2. تعتبر محتويات الموقع الإلكتروني للجمعية خاصة للأغراض التي تم نشرها لأجلها، ولا يجوز استخدامها من قبل الأطراف الخارجية دون إذن خطي من قبل إدارة الجمعية.
3. يلتزم قسم تقنية المعلومات بحماية الموقع والإشراف على تأمينه بالتنسيق مع الأطراف ذات العلاقة.
4. في حال طلب الموقع الإلكتروني لأي من البيانات الخاصة بالمستفيدين أو المتبرعين، تلتزم الجمعية بالحفاظ على سرية هذه البيانات وعدم الكشف عنها للأطراف الخارجية وبأي شكل يخالف الأنظمة والقوانين في المملكة العربية السعودية.
5. يتم تنظيم المعلومات وعرضها في الموقع الإلكتروني للجمعية بصورة واضحة بحيث تمكن المستفيدين من خدمات الموقع من الوصول السهل إلى المعلومات التي يبحث عنها.
6. يتم تنظيم محتويات الموقع بحيث يشمل بالحد الأدنى على المعلومات التالية:
    - 6.1 التعريف بالجمعية، ورؤيتها، ورسالتها، وخططها.
    - 6.2 الهيكل التنظيمي للجمعية.
    - 6.3 السياسات المنظمة لأعمال الجمعية.
    - 6.4 الحوكمة والشفافية.
    - 6.5 التقارير الدورية والقوائم المالية

6.7 شركاء النجاح مع الجمعية.

6.8 وسائل التواصل مع الجمعية من خلال مختلف قنوات التواصل.

6.9 تفاصيل الخدمات المقدمة من الجمعية.

6.10 بوابات الموقع الإلكتروني، والتفاصيل الخاصة بكل بوابة.

7. يتم الالتزام بعدم التحديث على أي من محتويات وبيانات الموقع الإلكتروني للجمعية دون الحصول على الموافقة اللازمة من صاحب الصلاحية.

8. يتم ضمان تحديث الأخبار الخاصة بالجمعية في الموقع الإلكتروني وبشكل مستمر بعد موافقة صاحب الصلاحية.

الفصل رقم (14): أمن المعلومات

المادة (44): السياسات المنظمة

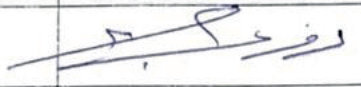
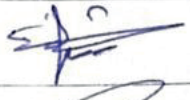
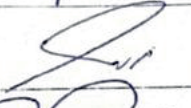
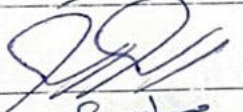
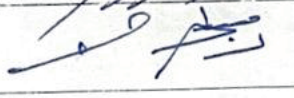
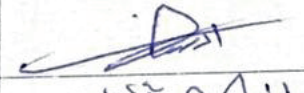
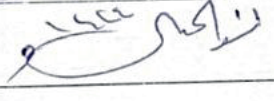
1. تتبع وتلتزم الجمعية بالمتطلبات المعتمدة من الهيئة الوطنية للأمن السيبراني في المملكة، وتسعى بكل السبل لتنفيذها وتوفير البنية التحتية لها.

الاعتمـــــــاد

تم إعتماد السياسات في الاجتماع العمومي الاول لعام ٢٠٢٣ م
يوم الإثنين الموافق ١٣/ فبراير/ ٢٠٢٣م

إجتماع مجلس الاداره ٢
٢٨/ ديسمبر/٢٠٢٢م
الموافق ٢٤ /٥ /١٤٤٤هـ

تصديق أعضاء مجلس الإدارة

الاسم	صفتها بالجمعية	التوقيع	ملاحظات
رفعة بنت هايف الحلاف	رئيسة مجلس الإدارة		
شرعاء بنت قالح القحطاني	نائبة رئيسة مجلس الادارة		
سارة بنت عوض الحربي	المشرفة المالية		
مرزوقة بنت حزام العنزي	عضوه		
مستورة بنت صلاح الحربي	عضوه		
د. ابتسام بنت سند العنزي	عضوه		
نوف بنت الأسود الجبلي	عضوه		

مؤسسة الملك خالد
KING KHALID FOUNDATION

شكـــراً لكـــم

يـسـر الجمعـية النسائية الخيرية دُره أن تتقدم بالشكر على ما قدمتـم مـن إحتضـان وتطويـر طوال مسـيرة العمـل، وإننـا نثمن جميع الجـهـود المـبـذولـة والتـي رفـدت جمـعيتنـا بـالـكثير مـن الإنجـازات المهمـة، وهـذا يدُلّ عـلى رؤيتكـم حـول أهميـة مبدأ تكافؤ الفرص المجتمعي، والتركيـز عـلى بنـاء نظـام قـوي موثر قادر على إطلاق شـــرارة الـــبنّاء بـشـكـل مـتـــوازن ومـتـكامـل.


دُرة
Dorra