دولة فلسطين
وزارة الحكم المحلي

دليل
سياسات تكنولوجيا المعلومات
في الهيئـــات المحليـــة

2022 - 2023

دليل سياسات تكنولوجيا المعلومات في الهيئات المحلية الفلسطينية

الفهرس

1. مقدمة

تعمل وزارة الحكم المحلي وبصورة مستمرة على تطوير عمل الهيئات المحلية الفلسطينية، وتشكل تكنولوجيا المعلومات وتعزيز دورها في تطوير وتحسين الخدمات التي تقدمها الهيئات المحلية ودعم تحولها إلى بلديات الإلكترونية ،إحدى أولويات واهتمامات الوزارة.
يتبين من خلال عمليات المتابعة المستمرة لواقع تكنولوجيا المعلومات في الهيئات المحلية ضرورة وجود سياسات توجيهية ناظمة لدى الهيئات المحلية في مجال تكنولوجيا المعلومات؛ ومن هنا جاء إعداد هذا الدليل ليكون مرجعاً توجيهياً للهيئات المحليّة في اعتماد سياساتها في تكنولوجيا المعلومات، بما يتناسب مع واقعها وبما لا يتعارض مع أيٍّ من السياسات الوطنية ذات العلاقة. تعتبر الاستراتيجيات والسياسات الوطنية ذات العلاقة بالتحول الرقمي وتكنولوجيا المعلومات مرجعا استرشاديا أساسيا في إعداد سياسيات تكنولوجيا المعلومات على المستوى المحلي، وعليه فقد تم الرجوع إليها بهذا الخصوص، ومنها: "سياسة أمن المعلومات المصادق عليها من قبل مجلس الوزراء الفلسطيني في العام 2021".

تتقاطع سياسة امن المعلومات بشكل واضح مع السياسات والإجراءات المتبناة بهذا الدليل كمبادئ توجيهية عامة مثل سياسة معايير امن المعلومات الواجب اتخاذها وتحديد المعلومات الحساسة الخاصة بالهيئات المحلية (سياسة سرية المعلومات وتصنيف المعلومات) وكيفية التعامل معها وحمايتها ضمن أفضل الطرق المعتمدة دوليا، وكيفية تقليل مخاطر ضياعها أو تلف هذه المعلومات (سياسة إدارة المخاطر وسياسة صلاحية الوصول) من خلال السيطرة على طرق تخزينها والوصول لهذه المعلومات (سياسة استخدام وامن الحوسبة السحابية) سواء كانت من مصادر خارجية أو داخلية باستخدام (سياسة التشفير وصلاحية الوصول وسياسة الأمن المادي و البيني). كذلك إن وضع سياسة استخدام مصادر خارجية أو الطرف الثالث يساعد بتحديد الصلاحيات الواجب منحها أو حجبها بهدف حماية المعلومات المصنفة حساسة وكيفية إدارة العلاقة مع الأطراف الخارجية وكيفية حماية المعدات والخوادم.
بالطبع، هنالك خصوصية واضحة للهيئات المحلية تمت مراعاتها بهذا الدليل الذي يهدف الى توفير مستند مرجعي لإدارة تكنولوجيا المعلومات وتحديد السياسات والإجراءات للأعمال ذات الصّلة وكذلك تعزيز الضوابط على تلك السياسات والإجراءات وتوثيقها وتحديد الصلاحيات والمسؤوليات المرتبطة بها؛ وعليه يتولى مراقب الدّليل تفويض مسؤولية تنفيذ السياسات والإجراءات المنصوص عليها بهذا الدّليل إلى شخصٍ مختصّ في التّعامل مع المسؤوليات داخل دائرة تكنولوجيا المعلومات.
باختصار، يشتمل هذا الدليل على ست عشرة (16) سياسة خاصة بتكنولوجيا المعلومات في الهيئات المحلية الفلسطينية والتي وضعت لتساعد الدوائر المعنية بتحديد الاتجاه المناسب للتعامل بشكل متكامل مع امن المعلومات وبما يتناسب مع أفضل الممارسات الدولية مثل نظام الأيزو الدولي.
أمّا بخصوص الآليّات لتحديد المسؤوليات فهناك بالإضافة إلى الإيضاحات المرتبطة بكلّ سياسةٍ على حدى، يوجد تفاصيل عن ثلاث لجانٍ رئيسة يجب تشكيلها من أجل وضع الآليّات لتنفيذ ومراقبة الأداء وتسهيل اتخاذ قراراتٍ متعلقة بحالات التغيير الطارئ مثلاً أو مراجعة إجراءات محددة بالسياسات:

1. **اللجنة التوجيهية**: مسؤول الدائرة، مسؤول الخدمة، مسؤول الدائرة التي تطلب الخدمة "مالك الخدمة" ومدير المشتريات.
2. **لجنة الطوارئ:** مسؤول الدائرة يقوم بتحديد أعضائها.
3. **لجنة التقييم:** مسؤول الدائرة يقوم بتحديد أعضائها.

إن هذه السياسات قابلة للتعديل بناءً على احتياجات المستخدم وما يمكن أن ينطبق على الأجهزة المستخدمة بالهيئة المحلية، وبما أنّ عالم تكنولوجيا المعلومات متغير بشكلٍ دائم فينبغي على إدارة دائرة تكنولوجيا المعلومات القيام بعملية مراجعة دورية لهذا الدليل؛ وذلك بهدف تقييم مدى ملاءمته وقابليته للتطبيق، أو حاجته إلى التعديل وفقاً للتغيرات التي قد تطرأ في الهيئة المحلية أو البيئة المحيطة بها.

وبالتالي، على كل هيئة محلية دراسة هذه السياسات قبل وضعه قيد التطبيق على أن يتم تفعيل الدّليل بدءاً من تاريخ اعتماده من قبل الهيئة المحلية، كذلك يعمل هذا الدّليل على إعطاء المستخدم إيضاحات حول الأدوار الرئيسة المنوّطة بدائرة تكنولوجيا المعلومات وضرورة التقييد بهذه الأدوار الرئيسة لتعمل كمرجعية واضحة في الأمور المتعلقة بهذا الدّليل وآليّات تطويره كما نبين بالأقسام التالية:

مراقب الدليل

هو مسؤول إدارة تكنولوجيا المعلومات، ويجب أن توجَّه كافة الاستفسارات والأمور المتعلقة بهذا الدّليل ونطاقه وأهدافه إلى مراقب الدّليل، كما إنَّ مسؤولية الحفاظ على الدّليل ومحتوياته وتوزيعه كلياً أو جزئياً بالإضافة إلى تحديثه وتطبيقه على نحوٍ صحيح هي من صلاحيات مراقب الدّليل.

انتهاكات السياسة

يجب على جميع موظفي دائرة تكنولوجيا المعلومات الامتثال التّام لهذا الدّليل بعد أن يتم اعتماده رسمياً من قبل الدائرة والهيئة المحلية . إنّ الهيئة المحلية تحتفظ بالحق في مراجعة الامتثال لهذه السياسة من حينٍ لآخر وسيتم اتخاذ أي إجراء تأديبي ينشأ عن انتهاك هذه السياسة وفقًا للقوانين والإجراءات المُحددة بالهيئة المحلية وقد تؤدي الإجراءات التأديبية إلى فصل الموظفين، وإنهاء علاقات العمل في حالة المتعاقدين أو الاستشاريين.

حق الاطلاع على الدليل

إنّ كافة العاملين المعنيين في الهيئة المحلية لهم حريّة الاطلاع على هذا الدّليل بعد الحصول على موافقة مسبقة من مراقب الدليل، ويجب أن يتاح للمديرين كافّة فضلاً عن العاملين في تكنولوجيا المعلومات الاطلاع على الدّليل.

تنفيذ الدليل:

يتولّى مراقب الدّليل تفويض مسؤولية التّأكد من التّنفيذ والالتزام بسياسات وإجراءات عمليات إدارة تكنولوجيا المعلومات.
يمكن لمراقب الدّليل تفويض مسؤولية تنفيذ سياسات وإجراءات إدارة تكنولوجيا المعلومات وفقاً لما هو وارد بهذا الدّليل إلى شخصٍ مختصٍ في التّعامل مع المسؤوليات داخل إدارة تكنولوجيا المعلومات.

تعزيز الدليل

1. يجب أن يكون هذا الدليل بمثابة وثيقة حيّة بحيث يتم إضافة سياسات وإجراءات بها عند الضرورة، وإنه من المتوَّقع أن تتطلب السياسات والإجراءات القائمة إلى تعديل وكذلك يتطلّب الأمر إضافة سياسات وإجراءاتٍ جديدة.
2. يجب أن تتم كافة التعديلات والتحديثات على هذا الدّليل وفقاً لإجراءات التحديث الواردة في هذا الجزء.

نطاق الدليل

نطاق تطبيق هذا الدّليل وما يتصل به هو من اختصاص دائرة تكنولوجيا المعلومات تحت الإشراف المباشر من مسؤول إدارة تكنولوجيا المعلومات.

صيانة الدليل وتكرار معدل المراجعة

يجب أن يتم مراجعة واعتماد الدليل على فترات منتظمة لتعكس التغييرات في أنشطة أعمال الهيئة المحلية، فيتناول الجدول التالي معدل تكرار المراجعة المقترح ومسؤولية أداء المراجعة ومسؤولية المعتمد النهائي:

المراجعة	معدل تكرار المراجعة (المقترح)	مسؤولية المراجعة	مسؤولية الموافقة
السياسات	كل 12 شهر	مسؤول الدائرة	مدير عام الهيئة المحلية
الإجراءات	كل 12 شهر	مسؤول الدائرة	مدير عام الهيئة المحلية

إجراءات التحديثات

لمراجعتها والموافقة عليها:

الغرض من عمليّة المراجعة والموافقة هو السماح بتقييم "نظام الجودة" من أجل الدقة والمحتوى الفني والاكتمال لاحتياجات الهيئة المحلية؛ فيشير إكمال التوقيع إلى أنّ المستند قد تمت مراجعته والموافقة عليه من قبل الحد الأدنى من المراجعين والموافقين المحددين في سياسة مراقبة مستندات الهيئة المحلية، كما يشير توقيع المراجع إلى قبول المستند والموافقة عليه في شكله النهائي.

سجل مراقبة عمليات التحديث:

- يجب وضع أيٍّ من المتغيرات التي تطرأ على هذا الدليل مؤرخة ومتسلسلة.
- يتم إدخال تاريخ إجراء التحديث إلى جانب رقم التغيير في كلِّ صفحةٍ من صفحات دليل تكنولوجيا المعلومات.
- يتولى مراقب الدّليل التحقق من معرفة جميع الموظفين بالتحديثات ورقم آخر إصدار من إصدارات الدليل.
- تاريخ بدء التطبيق.
- يجب الاستعانة بالجدول الآتي وتوقيعه لإجراء جميع التحديثات على الدليل.

اسم الملف		**رمز الوثيقة**	
تاريخ الإصدار		**رقم الإصدار**	**1**

الشخص المعين	**أعدت بواسطة**	**تمت مراجعته من قبل**	**تمت الموافقة عليه من قبل**
اسم:			
موقع:			
إمضاء:			
تاريخ:			

التعديلات			
غرض	**ملخص التعديل**	**تاريخ إصدار التعديل**	**موافقة**

2. تعريفات

2.1 أنواع تهديدات أمن المعلومات

1. **اختراق النظام:** اختراق جهاز كمبيوتر مضيف ، حيث يمكن الوصول إلى البيانات المخزنة وتعديلها ويمكن تعطيل عمليات الكمبيوتر أو تعديلها أو إزالتها.
2. **بوت نت**: من أكبر التهديدات التي تواجه الإنترنت اليوم ، وهي مرتبطة بمعظم أشكال جرائم الإنترنت، معظم الرسائل الاقتحامية ، والحرمان من الخدمات ، وهجمات DDOS ، وبرامج التجسس ، والنقرات الاحتيالية ، والهجمات الأخرى تنشأ من شبكات الروبوتات والمنظمات الخفية التي تقف وراءها.
3. **التصيد:** يقوم المحتال بإرسال رسائل بريد إلكتروني إلى الإنترنت باستخدام بريد إلكتروني يزعم أنه من مؤسسة مالية أو موقع تجارة إلكترونية يمتلك سمعة طيبة؛ فتحث رسالة البريد الإلكتروني المستلم على النقر فوق ارتباط لتحديث ملفه الشخصي أو إجراء بعض المعاملات، وينقل الرابط الضحية إلى موقع ويب مزيف مصمم ليبدو وكأنه حقيقي؛ وبالرغم من ذلك يتم توجيه أي معلومات شخصية أو مالية تم إدخالها مباشرة إلى المحتال.
4. **الحرمان من الخدمة هجوم "DoS ":** هو هجوم يهدف إلى إيقاف تشغيل جهاز أو شبكة اتصال، مما يجعله غير قابل للوصول إلى المستخدمين المقصودين؛ حيث يتم إنجاز هجمات DOSعن طريق إغراق الهدف بحركة المرور، أو إرسال المعلومات التي تؤدي إلى انطلاق حادث.
5. **سرقة الهوية:** أي شخص يستخدم الإنترنت عُرضة لسرقة بياناته الشخصيّة من أجهزة الكمبيوتر الشخصيّة الخاصة به، فيمكن للمتسلل أو الأفراد انتحال شخصية فرد بحساب شرعي والحصول على بياناته أو أمواله بشكل غير قانوني.
6. **السّرقة:** سرقة أجهزة الكمبيوتر والوصول إلى بيانات القرص الصلب.
7. **المطّلعون:** الاحتيال من الداخل ، والذي يشمل الموظفين أو المسؤولين الموثوق بهم في شكل وصول إلى بيانات مقيدة، أو مهام إدارية غير مصرح بها، أو معاملات غير قانونية.
8. **الهجمات السلبيّة:** يتم اعتراض المعلومات دون تعديل، والتنصت هو إحدى طرق الهجمات السلبية.
9. **الهجمات النّشطة:** تتضمن الهجمات النّشطة اعتراض المعلومات وتعديلها ويمكن تغيير حقول البيانات أو إدراجها أو حذفها أو تكرارها أثناء الإرسال.
10. **هندسة اجتماعية:** تتم سرقة البيانات بتقليد موظف الهيئة المحليّة أو العميل، حيث يقنع المتصل المستجيب الذي يقدم له / لها معلومات سرية.

10. الهجمات المتعلقة بالفيروسات

10.1. **حصان طروادة** : يأتي مع برامج أخرى.

10.2 **الدودة**: هو عبارة عن برنامج الاستنساخ الذاتي، حيث يقوم بإنشاء نسخ من نفسه غالبًا ما تسمى الديدان التي تنتشر باستخدام دفاتر عناوين البريد الإلكتروني بالفيروسات.

10.3. **فيروس** : يعيد إنتاج نفسه عن طريق إرفاقه بملفات أخرى قابلة للتنفيذ.

10.4. **قنبلة المنطق** : هو فيروس يكون خاملاً حتّى يتم تشغيله بواسطة حدث (التاريخ ، إجراء المستخدم ، المشغل العشوائي ، إلخ).

2.2 تعريفات عامة

1. **المجلس:** يقصد به مجلس الهيئة المحلية.
2. **الاتصال عبر الإنترنت:** تبادل المعلومات باستخدام الإنترنت أو شبكة الاتصالات المتنقلة لأي غرض، مثال عليه: مشاركة المعلومات والتسويق والمشاركة العامة .
3. **اتفاقية مستوى الخدمة "SLA":** يكون جزءاً من عقد مكتوب بين مقدم خدمة داخلي وعميل خارجي يحدد بدقة الخدمات المطلوبة، ودرجة الخدمة المتوقعة، والمزوّد الذي سيقدم الخدمات ويضع المقاييس التي يتم من خلالها قياس الخدمة ، والتعويضات أو العقوبات في حالة عدم تحقيق مستوى الخدمة المتفق عليه.
4. **إجراء**: وصف الضّوابط التي يجب تنفيذها.
5. **إدارة التغيير**: هي عملية لطلب أو تطوير أو إقرار أو تنفيذ تغيير مخطط له أو غير مخطط له داخل البنية التّقنيّة لتكنولوجيا المعلومات والاتصالات في الهيئة المحلية.
6. **الإدارة العليا:** وهي مجموعة من كبار الموظفين الذين قد يشمل رؤساء أقسام معينين وكبير المسؤولين الإداريين في الهيئة المحلية لاتخاذ قرارات الإدارة الداخليّة.
7. **إدارة الكوارث:** هي عمليّة إدارة أيَّ خللٍ يطرأ فجأة و يؤثر على مجريات عمل الهيئة المحليّة و تقديم الخدمة للزبائن مما يلحق الضرر بالمؤسسة، كتعطل النظام البلدي أو شبكة الاتصالات؛ فالهدف من إدارة الكوارث هو تقليل الضّرر الناتج عن تعطّل الخدمة باستخدام خطط و طرق بديلة لتقديم الخدمة للزبائن لحين إصلاح الخلل.
8. **الاستعانة بمصادر خارجيّة**: تستخدم مصطلحات **التعهيد أو الطرف الثالث** بنفس المعنى بهذه السياسة وتعني استخدام مقدم خدمة خارجي لإدارة خدمات تكنولوجيا المعلومات وهو أحد أنواع الموردين.
9. **اسم المستخدم**: يُشار إليه بدلاً من ذلك **باسم الحساب** و**معرّف تسجيل الدّخول** ومعرّف المستخدم، وعادةً ما يكون اختصارًا لاسم المستخدم الكامل أو اسمه المستعار.
10. **اسم المضيف**: هو (التسمية) الاسم (المعينة لجهاز) مضيف على شبكة ويستخدم لتمييز جهاز واحد من جهاز آخر على شبكة معينة أو عبر الإنترنت.
11. **إطار عمل إدارة مخاطر الموردين**: نهج منهجي وشامل لتقييم المخاطر المستمرة والمتغيرة وتوفير ضمان بأنَّ المخاطر المتعلقة بالموردين تدار بشكلٍ صحيح.
12. **إغلاق طلب التغيير:** إجراء إداري يوثق الانتهاء من تنفيذ طلب التغيير بنجاح .
13. **إلغاء التكرار(Deduplication)**: تقنية نسخ احتياطي لتوفير استهلاك المساحة التي تسببه بيانات النسخ الاحتياطي للنسخ الاحتياطية الكاملة والمتزايدة، وذلك عن طريق الاحتفاظ فقط بملفٍ واحد (نسخة واحدة) لتاريخٍ ووقتٍ محددين.
14. **الأمن الإلكتروني:** الموارد المستخدمة لحماية الشبكات بأكملها، وأنظمة الكمبيوتر، والمكونات الرقمية الأخرى، والبيانات المخزنة داخل الهيئة المحلية من الولوج والتعامل غير المصرح به.
15. **الأمن الرقمي:** مصطلح عام يصف الموارد المستخدمة لحماية بيانات الهيئة المحليّة والأصول الأخرى المتعلقة بتقنية المعلومات والاتصالات، حيث تتضمن هذه الأدوات برامج مكافحة الفيروسات، وكلمات مرور قوية، وجدار حماية.
16. **أنظمة البريد الإلكتروني غير التابعة للهيئة**: استخدام أنظمة الاتصال غير التابعة للهيئة (مثل أنظمة البريد الإلكتروني المستندة إلى الإنترنت ، على سبيل المثال: Yahoo وMSN وغيرها).
17. **البرمجة:** تتضمن أيًا من حزم البرامج التي يستخدمها الكمبيوتر لإجراء عملية معينة.
18. **البريد الإلكتروني "EMAIL"**: الرسائل، بما في ذلك النصوص والرسومات والمرفقات، وقد تتضمن وظائف أخرى مثل التقويمات وقوائم المهام التي يتم إرسالها من شخصٍ إلى آخر عبر أحد الأجهزة/الأنظمة الحاسوبية. كما يشمل الرسائل المُرسلة عبر الشبكة المحلية (LAN) التابعة للهيئة أو خدمة الاتصال الهاتفي عبر مزود خدمة الإنترنت (ISP)، كما يمكن إرسال البريد الإلكتروني تلقائيًا إلى عدد كبير من العناوين (القائمة البريدية).
19. **البنية الأساسية لتقنية المعلومات والاتصالات**: وهي تقنيات الشبكات، والخادم، والتخزين، وقواعد البيانات، والحلول التي تديرها إدارة تقنية المعلومات.
20. **بوابة المعرفة:** هي وحدة أساسيّة في نظام الدّعم الفنّي وتسمّى بالإنجليزية (**Knowledgebase in the Heldesk**) والذي يمكن الوصول إليها عن طريق بوابة إلكترونية، وتحتوي على مكتبة أسئلة و أجوبة تقدم للموظف طالب الخدمة الحلول للمشاكل المتكررة، و مقالات يمكن الاستفادة منه؛ فالهدف الرئيسي من بوابة المعرفة

هي خدمة و مساعدة موظفي دائرة الدعم الفني و موظفي الدوائر الأخرى على توفير حلول سريعة للمشاكل و القضايا المتكررة بتدوينها داخل البوابة الإلكترونية بطريقة سلسة.

21. **البيانات الحرجة**: البيانات التي يمكن أن تعطل تقديم الخدمات بشدّة عند فقدها، مثل: البيانات المالية، والبيانات الشخصيّة للمواطنين أو المستخدمين .
22. **البيانات الهامّة (الحسّاسة)**: هي البيانات التي يمكن أن تعطِّل الخدمات بشدة عند فقدها وتشمل البيانات الماليّة والبيانات الشخصيّة للعميل وما إلى ذلك من معلومات.
23. **البيانات الوصفية**: هي بيانات تصف وتعرف بيانات أخرى.
24. **تخفيف المخاطر**: هي عملية تحاول الحدّ من الضّرر بعد حدوث الخطر.
25. **التّشفير**: هي عبارة عن استخدام عمليّة خوارزميّة لتحويل البيانات إلى نموذجٍ يكون فيه احتمال تحديد المعنى دون استخدام عملية سريّة أو مفتاح.
26. **تصحيح البرنامج:** تحديث أو تصحيح أو تحسين أو توسيع منتج برمجي حالي صادر عن البائع، أو تغيير نظام تشغيل، أو تطبيق يثبّته البائع عادةً.
27. **التّصيّد:** نشر منشورات عبر الإنترنت مسيئة أو استفزازية بشكلٍ متعمَّد بهدف إغضابِ شخصٍ ما، وإثارة رد فعل غاضب و/أو تشجيع مناقشة سلبيّة أو غير مثمرة.
28. **تضارب المصالح**: أي عضو في لجنة التّوظيف أو منخرط بعملية التوظيف ولديه علاقة عائلية مباشرة(زوج\ زوجة\ ابن\ابنه)، أو لديه مصالح مباشرة وغير مباشرة تجاريّة أو ماليّة مع المتقدِّم للوظيفة، أو منصب بالهيئة المحليّة .
29. **التغيير**: إضافة أو تعديل أو محو أو إزالة ما قد يؤثر في الخدمات التقنيّة للهيئة، ويتضمن إجراء تعديلات على البنية الأساسية لتقنية المعلومات والتطبيقات والأنظمة والعمليات والوثائق وواجهات الموردين، إلخ.
30. **تكامل البيانات**: هي عملية جمع البيانات من مصدرين أو أكثر بهدف تقديمها في مخرج واحد.
31. **التوافقية:** قدرة الأنواع المختلفة من الحواسيب والشبكات وأنظمة المعلومات والتطبيقات لتعمل معاً بشكلٍ فعّال دون الحاجة لاتصال مسبق ونقل البيانات بطريقةٍ فعّالة.
32. **التّوجيهات:** هي مجموعة من المتطلبات الخاصّة بالنّظام أو المتطلبات الإجرائية المحددة التي يجب أن يفي بها الجميع.
33. **الجدار الناري:** هو نظام أمان للشبكة، حيث يراقب حركة مرور الشبكة الواردة والصادرة وهو عبارة عن تطبيق يقوم بفحص البيانات على الشبكة من خلال سياسة (مجموعة من القواعد) لمنع الدخول غير المسموح به مع السماح بالاتصالات المسموح بها من وإلى الشبكة والأجهزة الإلكترونية.
34. **جهات الخارجيّة:** هي ما يطلق عليها أيضاً "الطرف الثالث" وهو عبارة عن كيان خارجي لديه عقد خدمة مع الهيئة المحليّة لتقديم مهام محددة تتعلق بإدارة تقنية المعلومات والاتصالات.
35. **الحساب الرئيسي:** حساب وسائل التواصل الاجتماعي الأساسي الخاصّ بالهيئة المحليّة ضمن كلِّ قناة من قنوات التواصل الاجتماعي المختارة ، ويديره ويصونه ويغذيه مسؤول حساب وسائل التواصل الاجتماعي.
36. **حساب منفصل:** حساب على وسائل التواصل الاجتماعي يتم إنشاؤه من قبل إدارة الهيئة المحليّة بالإضافة إلى حساب الهيئة المحلية ويديره ويحتفظ به ويغذي مسؤول حساب وسائل التواصل الاجتماعي.
37. **خادم FIN**: يكون خادم مالي/سحابي.
38. **خطّة إدارة الخطر**: هي مبادرة تنظيميّة توضِّح منهج إدارة المخاطر للمشروع عبر تقديم مصطلحات موحدة، وتحديد أدوار ومسؤوليات واضحة، وآليات الوصول ومستوى الخدمة التي توافق عليها الهيئة المحلية ، وتتضمن معلومات المورد.
39. **دائرة الدعم الفني/التقني (helpdesk):**هي وحدة تابعه إلى قسم تكنولوجيا المعلومات تتكون عادةً من موظفين في الدائرة لديهم معرفة تامة بالنظم التقنية، وكذلك بالسياسات والإجراءات لدى الهيئة وتعتبر الحلقة الأولى في التعامل مع طلبات الدعم والتغيير التقني.
40. **دائرة تقنية المعلومات والاتصالات**: يستخدم اختصارا بدلاً عنها مصطلح "الدائرة ".
41. **الدائرة:** دائرة تقنية المعلومات بالهيئة المحلية.
42. **درجة تحمل المخاطر**: هو الرّغبة في تجنّب (منع) أو قبول (تخفيف) المخاطر.
43. **رئيس القسم:** يُقصد به مسؤول الدائرة أو المسؤول المعين من الهيئة المحلية ، والذي يمكن أن يكون عضواً في فريق الإدارة العليا.
44. **رئيسي وثانوي:** وصف لمستوى التغيير الذي تحدده مكونات المخاطر ومدى التأثير.

45. **السجّل الرّسمي:** أي سجل للمعلومات المسجلة سواءً أكان في شكلٍ مطبوع ، أو بالوسائل الإلكترونية ، ويشمل كمثال: مراسلات ، مذكرة، خريطة وتسجيل صوتي، وشريط فيديو.
46. **سجل انتقالي:** يعني أي سجل له فائدة مؤقتة، ويكون مطلوبًا فقط لإكمال إجراء روتيني أو حتى يتم استبداله.
47. **السيطرة الأمنية**: أي شيء يتم استخدامه كجزء من استراتيجية الاستجابة الأمنية التي تعالج تهديداً لتقليل المخاطر(يُعرف أيضًا باسم الإجراء المضاد أو الحماية).
48. **صلاحيّة التّحكّم:** وسائل وآليّات إدارة الوصول إلى الموارد واستخدامها من ِقبل المستخدمين.
49. **طلب التغيير**: هو طلب موثّق للتعديل في الأنظمة أو البنية الأساسية لتقنية المعلومات والاتصالات، وفي العادة يتم إرسال الطلب من خلال دائرة الدّعم الفني، ويتم تنفيذ ذلك من خلال عمليّة إدارة تغيير تقنيات المعلومات والاتصالات.
50. **طلبات الخدمة:** هي الطّلبات المُقدَّمة لدائرة الدّعم الفنّي من قِبل الموظفين لتوفير خدمة جديدة أو حلاً لمشكلة قائمة، و التي قد تشمل توفير معدات جديدة، أو نظم و برامج جديدة، أو خدمة الاتصال بالشبكة، أو صلاحيات على نظم معينة.
51. **طلبات الدّعم:** هي الطّلبات المقدَّمة لحل مشكلة قائمة في خدمة أو نظام أو برنامج، مثل: مشكلة بالاتصال بالشبكة، أو صلاحيات على برنامج.
52. **الطوارئ:** أي انقطاع في الأنظمة أو الخدمات الدّاخليّة يتطلب تغيير عاجل، مثل تعطّل الأنظمة وانقطاع الخدمة وإعادة تشغيل النّظام بشكل غير متوقع، و يجب الموافقة على تغيير الطوارئ من قِبل مسؤول الدّائرة .
53. **عاجل:** أي تغيير تم تنفيذه قبل إقرار التغيير بصورة رسمية بهدف مواصلة عمليات الهيئة المحليّة وخدماتها. يجب الموافقة على البنود العاجلة من قِبل مسؤول الإدارة.
54. **عادي:** أي تغيير مطلوب ومجدول يتم إجراؤه على الأنظمة والخدمات، سيتم تقديمه ولكن لا ينفذ قبل اجتماعات إدارة التغيير.
55. **عبارة المرور**: تشبه كلمة المرور في الاستخدام لكنّها غالباً تكون أطول لإضفاء مزيداً من الأمان، وتتكون من جملة أو مجموعة كلماتٍ متعددة ليسهل حفظها، وتحتوي على مجموعةٍ من الأحرف الكبيرة والصغيرة، والأحرف الرقمية، وعلامات الترقيم.
56. **العمل العرضي**: يشير إلى طلب مخصص لموظفين إضافيين لم يتم الإشارة إليهم في المخطط التنظيمي أو المناصب الشاغرة لفترة محددة.
57. **فرد من العائلة:** الزوج ، والوالد ، بما في ذلك زوجة الأب والوصي القانوني، الطفل بما في ذلك ابن الزوج / الزوجة ، أخ أو أخت، وأي شخص يعيش مع عضو مجلس أو موظف بشكل دائم .
58. **فريق شبكات وأنظمة المعلومات:** هو فريق دائرة تقنية المعلومات المسؤول عن الأنظمة والشّبكات وتصميمها وتقديم الدّعم الفني لها.
59. **قانون الجرائم الإلكترونية:** القانون الفلسطيني رقم 14 لسنة 2018م بشأن الجرائم الإلكترونية.
60. **اللّجنة التوجيهيّة لتقنية المعلومات والاتصالات**: لجنه تختص بدراسة أتمتة عمليات محددة وتحويل العمليات والخدمات والموافقة على الاستثناءات.
61. **مالك الخدمة** : هو مسؤول القسم الذي يستعين بمصادر خارجية لوظيفة / عملية.
62. **المجلس الاستشاري للتغييرات الطارئة**: مجموعه فرعية من المجلس الاستشاري للتغيير للتعامل مع الحالات الطّارئة.
63. **المجلس الاستشاري للتغييرات**: يضم مجموعه من الأشخاص يمثلون جميع الجهات ضمن دائرة خدمة تكنولوجيا المعلومات يحددهم مسؤول الدائرة، وقد تشمل اللجنة أشخاص من خارج الدّائرة أو الهيئة المحليّة .
64. **المجلس**: الأشخاص المنتَخبون للإشراف على الهيئة المحليّة.
65. **المراسلة الفوريّة (تُسمى أحيانًا IM أو IMING)**: هي القدرة على معرفة ما إذا كان هنالك شخصٌ معينٌ متصلاً بالإنترنت أو الإنترانت بسهولة، وكذلك تبادل الرسائل مع هذا الشخص.
66. **مرافق البريد الإلكتروني**: الأجهزة/الأنظمة الحاسوبية المرتبطة بأداة تمكين البريد الإلكتروني، والتي تم إعدادها من أي أصلٍ من الأجهزة والبرامج المستخدمة لتخزين المعلومات الإلكترونية و/أو إرسالها و/أو مراقبتها، بما في ذلك جميع معدات تقنية المعلومات التي تتصل بشبكات الهيئة المحلية أو يمكنها الاتصال بها، سواء أكانت مملوكة للهيئة أم لا.
67. **مسؤول الخدمة**: موظف لديه الخبرة الكافية لتقييم العلاقة مع الموردين والإشراف عليهم وإدارتهم.
68. **مسؤول الدائرة**: موظف يعمل مدير دائرة أو رئيس قسم تقنية المعلومات في الهيئة المحليّة .

69. **مسؤول أمان المعلومات**: أحد كبار الموظفين في دائرة تقنية المعلومات والاتصالات، وله مهمة محددة للحفاظ على خصوصية وأمان المعلومات المختلفة التابعة للهيئة.
70. **مسؤول حساب وسائل التواصل الاجتماعي:** موظف تعيّنه أو تنتدبه الهيئة المحليّة لإدارة حساب الهيئة المحلية الرسمي أو حساب منفصل فرعي على وسائل التواصل الاجتماعي ، بما في ذلك كتابة المحتوى ونشره ومراقبة نشاط الحساب وإدارته وقياسه.
71. **مسؤول دائرة تقنية المعلومات**: يقصد به مدير الدائرة \ رئيس قسم تقنية المعلومات في الهيئة المحلية.
72. **معدّات الكمبيوتر الأساسية:** خوادم ملفات الشّبكة ، ومحطّات العمل المتصلة بالشبكات التي تقوم بعمل نسخ احتياطية للنظام بعد ساعات العمل ، وأجهزة الكمبيوتر التي تتلقى البيانات بعد ساعات العمل.
73. **المعدّات:** تشمل أجهزة الكمبيوتر، والشّاشات، ولوحات المفاتيح، وأجهزة المودم، وبطاقات الذاكرة، ووحدات محرك الأقراص، والطابعات، والكابلات، وجميع العناصر الأخرى التي تتطلب اتصالاً فعلياً بجهاز كمبيوتر أو بشبكة كمبيوتر.
74. **معلومات المواطن:** أي سجل يحتوي على معلومات شخصية "غير عامّة" عن مواطن / شخص يحصل على خدمة (مستمرة أو متوقفة) من الهيئة المحليّة . يشمل ذلك النماذج الورقية أو الإلكترونية أو غيرها من الأشكال التي يتم التعامل معها أو صيانتها من قِبل الهيئة المحلية أو نيابة عنها.
75. **المعلومات غير العامّة**: جميع العناصر والمواد والمعلومات غير العامّة (سواء كانت مكتوبة أم لا، وما إذا كانت مؤهلة للحصول على براءة اختراع أو محميّة بحقوق نشر أم لا) التي تخص الهيئة المحليّة وتتعلق إما بالأعمال الحالية أو المستقبلية للهيئة، ويتم الاحتفاظ بها سريةً وغير مُعلنة من قِبل الهيئة المحلية .
76. **منطقة مؤمنة:** هي تجميع واجهات الشبكة في مجموعات للمساعدة في إدارتها وتصنيف تدفق البيانات على الشبكة.
77. **منع المخاطر:** محاولة إيقاف / تجنب المخاطر قبل حدوثها.
78. **المواد المرفوضة:** المحتوى الذي يتعارض مع المبادئ التي أرستها القوانين الفلسطينية وخاصّة المواد ذات الطبيعة الإباحية أو المهينة أو الجنسية الصريحة أو التي تسيء إلى دين أو عرق.
79. **الموارد البشرية**: الموظفون العاملون في دائرة تقنية المعلومات والاتصالات.
80. **الموارد والأصول:** أي شيء يتم استخدامه ويعتبر أساسي وضروري للقيام بالعمل، وتشمل الأصول العناصر الملموسة وغير الملموسة ، مثل: المعدات، ورموز، والبرامج، والبيانات، والمرافق، والموظفين.
81. **المورد :** مزود خدمة خارجي يقدم منتجات أو حلول أو خدمات تقنية المعلومات والاتصالات للبلدية.
82. **الموظف:** شخص يعمل في الهيئة المحلية على أساس التفرغ الكامل أو الجزئي.
83. **موظفون مؤقتون:** الموظف الذي يتم تعيينه لفترة زمنيّة مستمرة محددة مسبقاً مع تاريخ بدء وانتهاء معين، مثل: الموظف الموسمي، أو الموظف المعين لفترة لتغطية إجازة الموظف الدائم.
84. **الموقع الإلكتروني:** مكان إتاحة المعلومات أو الخدمات على الشبكة الإلكترونية من خلال عنوان معين تملكه الهيئة المحلية.
85. **الموقع الآمن**: موقع مختلف فعليًا عن موقع الإنشاء والاستخدام الأصلي، ويتضمن إجراءاتٍ أمنيةٍ، مثل الباب المؤمّن وسجلات للزّوار.
86. **النسخ الاحتياطي المتزايد**: هو النسخ الذي يتم بعد إجراء النسخ الاحتياطي الكامل، وفيه يتم نسخ الملفات التي تم تغييرها أو الملفات الجديدة فقط لتقليل الوقت الذي يستغرقه النسخ الاحتياطي لشيء ما بناءً على وقتٍ محدد.
87. **نظام الدّعم الفنّي (helpdesk):** هو البرنامج المستخدم لإدارة و تنظيم عمل الدوائر الأخرى مع دائرتيّ الشبكات و الأنظمة، وأنظمة الأعمال الأخرى وهو مكون من جزئين، الأول جهاز حاسوب مركزي (Server) و ما يتصل به من معدات، و الجزء الثاني هو البرنامج و قاعدة البيانات التي تحتوي على جميع المعلومات.
88. **نظام تكنولوجيا المعلومات (IT):**جميع أجهزة الاتصال الإلكترونيّة التي يستخدمها مجلس الهيئة المحليّة أو الموظفون أو المقاولون، والتي تشمل على سبيل المثال لا الحصر: جميع شبكات الكمبيوتر، والهاتف، والأجهزة، والتطبيقات، وكذلك الأجهزة المحمولة.
89. **هدف نقطة الاسترجاع أو الاسترداد (RPO):** هي الكميّة القصوى من البيانات التي قد تُفقَد عند استعادة الخدمة بعد حدوث انقطاع، ويتم التعبير عن هدف نقطة الاسترجاع كفترة زمنية قبل حدوث العطل.
90. **هدف وقت الاسترجاع أو الاسترداد (RTO):** هو أقصى وقت مسموح به لاسترجاع خدمة تقنية المعلومات بعد حدوث انقطاع.

91. **واسطة:** الجهاز الذي يتم تخزين البيانات عليه مثل الأشرطة والأقراص الصلبة والأقراص المضغوطة / أقراص DVD.
92. **وسائل التواصل الاجتماعي:** تشكّل التّقنيات التفاعليّة وسيطاً يشارك من خلاله الأشخاص الرسائل والصور الفوتوغرافية والمعلومات الأخرى علناً، لاسيما في المجتمعات أو المنتديات عبر الإنترنت، كما يمكن أن تشمل هذه القنوات ، مواقع الويب ، و Facebook ، و Twitter ، و YouTube، و Instagram، و LinkedIn ، بالإضافة إلى المدونات، وتطبيقات الهاتف المحمول.
93. **وسيط التّخزين**: الجهاز الذي تُخزن البيانات عليه، مثل: الأشرطة، والأقراص الصلبة، والأقراص المضغوطة (CD)/أقراص الفيديو الرقمي (DVD).
94. **وظيفة / عملية:** نشاط لديه القدرة في حالة تعطله على التأثير بشكل كبير على عمليات الهيئة المحلية أو سمعتها والاستمرار بتقديم خدمات فعّالة للمواطنين.
95. **مسؤول أصول تقنية المعلومات والاتصالات:** موظفٌ معينٌ في دائرة تقنية المعلومات والاتصالات يكون مسؤولاً عن إدارة الأصول بالكامل بالإضافة إلى العمليات والأنشطة التي تشملها. يتولى مسؤول أصول تقنية المعلومات والاتصالات إدارة عقود الإنفاق التكنولوجي على أصول تكنولوجيا المعلومات والاتصالات ودعمها وتنظيمها، حيث يضمن مسؤول أصول تقنية المعلومات والاتصالات التالي:

أ. تحديد شكل التّواصل بين الهيئة المحليّة ومورديها وتسهيله من أجل تقديم المنتجات والخدمات وفق الخطّة وفي حدود الميزانية.
ب. تقديم المشورة للإدارة والموظفين بشأن العمليّات والنّماذج والتحسينات وأفضل الممارسات المتعلقة بإدارة أصول تقنية المعلومات والاتصالات.

96. **NIST:** المعهد الوطني للمعايير والتقنية التابع للحكومة الأمريكية.
97. **BDC:** وحدة تحكم مجال النسخ الاحتياطي.
98. **ICT :** دائرة تقنية المعلومات
99. **PDC :**وحدة تحكم المجال الأساسية.
100. **RMF**: إطار عمل إدارة المخاطر.
101. **WSUS:** خادم تحديث ويندوز.

.1

1. سياسة شراء أصول تكنولوجيا المعلومات

1.1 المقدمة والأهداف

1.1.1 بيان السياسة

وُضعت هذه السياسة لتتناول الحصر الكامل لأصول الهيئة المحليّة المُستخدمة للوصول إلى البُنية التحتيّة لتكنولوجيا المعلومات الخاصّة بالهيئة المحليّة، والتي يجب تقييمها للوقوف على وضعها الحالي وتحديد الثغرات والاحتياجات لاتخاذ قرارات لشراء حلولٍ جديدة (أجهزة وبرامج). يجب إحاطة دائرة تكنولوجيا المعلومات والاتصالات/مسؤول أصول تكنولوجيا المعلومات والاتصالات بالمعلومات أو التغييرات في الملكية، وبتخصيص هذه الأصول، وبالتغييرات في التكوين، وبالاستخدام خارج مقارّ الهيئة المحليّة .

1.1.2 الهدف

للحفاظ على الحماية المناسبة لأصول الهيئة المحليّة المتعلقة بتكنولوجيا المعلومات والاتصالات، يجب تحديد جميع الأصول التي تتحمل دائرة تكنولوجيا المعلومات والاتصالات أو مسؤول تكنولوجيا المعلومات والاتصالات المسؤولية الأمنية عنها بما يضمن استمرار الحماية الأمنية الكافية.

1.1.3 نطاق العمل

تشمل هذه السياسة جميع مستخدمي أصول الهيئة المحلية المتعلقة بتكنولوجيا المعلومات والاتصالات، بما في ذلك الموظفين (بدوامٍ كاملٍ وجزئيّ) والموردين وشركاء الأعمال والعاملين المتعاقدين والوحدات الوظيفية، بغضّ النّظر عن الموقع الجغرافي. كما تشمل أيضاً جميع بيئات أنظمة معلومات الهيئة المحليّة التي يتم تشغيلها من خلال أو عن طريق التّعاقد مع جهةٍ خارجيةٍ وشراءِ الحلول الجديدة (الأجهزة والبرامج).

1.1.4 المسؤوليّات

1. مسؤول قسم تكنولوجيا المعلومات والاتصالات هو المسؤول عن الإشراف والحفاظ على تنفيذ هذه السياسة.
2. تُعِدّ دائرة تكنولوجيا المعلومات والاتصالات بالتعاون مع دائرة إدارة الأصول (دائرة الشؤون المالية) سجلاً شاملاً للأصول لجميع معدات تكنولوجيا المعلومات والاتصالات والبنية التّحتيّة ذات الصّلة وتتولّى إدارته.
3. يتحمل كل مسؤول ورئيس دائرة وموظف ومتعاقد مسؤولية ضمان احتساب جميع أصول الهيئة المحلية .
4. قسم تكنولوجيا المعلومات والاتصالات هو القسم الوحيد في الهيئة المحليّة المسؤول عن سلامة أنظمة وبيانات تكنولوجيا المعلومات والاتصالات في الهيئة المحليّة.
5. يجب مراجعة السّياسة من قِبل اللّجنة التوجيهية لتكنولوجيا المعلومات والاتصالات بالهيئة المحليّة على أساس سنوي وإعطاء الموافقة على أي تغييرات.
6. يجب إطلاع جميع الموظفين على الأخطار ونوعيّاتها المرتبطة باستخدام أصول ومعدات تكنولوجيا المعلومات والاتصالات والبنية التّحتيّة

1.2 السياسات والإجراءات

1.2.1 ينبغي تحديد الأصول الحيوية لتكنولوجيا المعلومات بحيث تشمل تحديد:

أ. مكوّنات ربط الشّبكة (أجهزة التوجيه والمُبدِّلات والموزعات وما إلى ذلك).
ب. الخوادم (البريد والملفات وشبكة الويب وما إلى ذلك).
ت. مكوّنات الاتصال الخارجي (أجهزة المودم).
ث. مكوّنات الأمان (خوادم المصادقة وجدران الحماية).
ج. أجهزة الكمبيوتر الشّخصيّة والمحمولة.

1.2.2 توثيق المعلومات المتعلقة بالأصول الحيوية لتكنولوجيا المعلومات بشكلٍ مناسب في نظام معلومات إدارة المخزون "IMIS"، والتي يجب أن تشمل:

أ) التّعريف: يجب تعريف كلّ أصلٍ حيويٍّ لتكنولوجيا المعلومات والاتصالات بشكلٍ مميز. ويجب أن يتضمن نظام التعريف المُستخدم تحديد بأن:

- يكون موقع أصول تكنولوجيا المعلومات والاتصالات معروفاً.
- يكون مورد أصل تكنولوجيا المعلومات والاتصالات معروفًا (يجب أن تكون معلومات المورد متاحةً).
- تكون عقود الصّيانة لأصول تكنولوجيا المعلومات مُحددةً.
- يكون الأشخاص المسؤولون عن الأصول معروفين.
- يكون أخر ست (6) خانات من التعريف أرقام حسب ما تقتضيه **سياسة اصطلاحات تسمية الأجهزة** .

ب) الوصف: يجب أن يتوفر وصفٌ موجزٌ لكلّ أصلٍ حيويٍ لتكنولوجيا المعلومات والاتصالات، ويجب أن يتضمن الوصف معلوماتٍ عامّة عن أصول تكنولوجيا المعلومات والاتصالات الحيوية، مثل: وظيفتها الرئيسة واستخدامها، وحالتها التي تعبر عن الأصل إذا كان في **المخزون**، أو **التشغيل**، أو **الإصلاح**، أو **التخلص**.
يمكن أن تستند الطّريقة المُثلى للتّخلص من الأصول إلى معدل الاستخدام، أو القيمة المالية، أو عمر الأصول، أو فئة الأصول.

ج) التكوين: يجب أن تكون المعلومات المتعلّقة بتكوين كل أصلٍ حيوي لتكنولوجيا المعلومات متاحةً، كما يجب تضمين وثائق التكوين الفني ودعمها بمتطلبات العمل التي توضح سبب تكوين أصل تكنولوجيا المعلومات والاتصالات على ذلك النّحو.

د) الرّوابط (عند الاقتضاء): يجب تضمين معلومات حول الروابط مع أصول تكنولوجيا المعلومات الحيوية الأخرى. ويجب أن تحتفظ دائرة تكنولوجيا المعلومات بسجل مخزون تكنولوجيا المعلومات، ويتعين تحديثه بجميع الإضافات إلى أصول تكنولوجيا المعلومات.

ه) يجب إدخال جميع أصول تكنولوجيا المعلومات الحيويّة في نظام معلومات إدارة المخزون "IMIS" بشكلٍ فردي مع توضيح ما يلي:

1. **النّموذج والنّوع**: نموذج ونوع أصل تكنولوجيا المعلومات.
2. **الرّقم التّسلسلي**: الرّقم التّسلسلي لأصل تكنولوجيا المعلومات.
3. **التّعريف**: رقم تعريف فريد (عند الاقتضاء).
4. **الموقع**: موقع أصل تكنولوجيا المعلومات.
5. **المورد**: اسم المورد.

توضيح : ما ورد أعلاه أمرٌ ملزم فقط فيما يتعلق بأصول تكنولوجيا المعلومات الحيوية، ولكن يُنصَح بعمله مع جميع أصول تكنولوجيا المعلومات الأخرى.

1.2.3 التقييم الأولي (داخلياً):

الخطوة الأولى بعد الانتهاء من توثيق جميع الأصول المتعلقة بتكنولوجيا المعلومات والاتصالات هي تحديد: أين نقف؟ وما هي حالة الأصول الحالية، ويتم ذلك من خلال التحقق من "الحد الأدنى من المعايير التشغيلية" المُقترحة لأساسيات نظام تكنولوجيا المعلومات (والتي يمكن لمسؤولي دائرة تكنولوجيا المعلومات والاتصالات تغييرها بناءً على احتياجاتهم) المُكونة من خمس موضوعات فئوية لقياس البنية التّحتية (انظر الملحق رقم 1) وتحديد ما يجب أن تمتلكه الهيئة المحليّة كحدٍّ أدنى لإنجاز المهام اليومية:

1. اتصال الإنترنت.
2. مضاد فيروسات (مُرخص) على جميع أجهزة الكمبيوتر.
3. أحدث البرامج المدعومة من المورد.

4. نسخ احتياطي للملفات.
5. كلمات مرور قويّة لتمكين حماية البيانات.

1.2.4 تحليل الثّغرات:

استناداً إلى التقييم الأولي يتعيّن على فريق تكنولوجيا المعلومات والاتصالات إجراء تحليل للثغرات؛ لتحديد مجالات التّطوير والحلول الممكنة، أو وضع منهجية لمعالجة أوجه القصور، أو إعداد مستندات المخزون مثل طلب المخزون أو إيصال تحويل المخزون أو إرجاع المخزون أو إدارة المعدات القديمة المُحددة، على سبيل المثال: قد يكشف تسجيل الخروج من اتصال الإنترنت عن ضعفٍ في البنية التّحتية للشبكة، أو عن الحاجة إلى جدار حماية، أو عن فقدان مبدّلات الشبكة. قد تكون الثّغرات مرتبطةً بالمشكلاتِ المتعلقة بالدوائر، مثل: الإنترنت الآمن وشبكة Wi-Fi العامة، أو بالحاجة إلى تعزيز الأمان من خلال مشكلة امتثال متعلقة بكلمات المرور. يرجى مراجعة **سياسة إدارة المخاطر** عند وضع التّحليل النهائي.

1.2.5 عمليّة إعداد الموازنة واتخاذ القرار:

استناداً إلى تحليل الثّغرات، يجب أن تتطلّع دائرة تكنولوجيا المعلومات والاتصالات بمسؤولية الإشراف على عمل خطة لتوفير احتياجات الهيئة المحليّة من أجهزة وبرامج وتحديد النفقات المطلوبة وتضمينها في الخطط التّنموية الاستراتيجية التّابعة للهيئة المحلية؛ لمساعدة دائرة تكنولوجيا المعلومات والاتصالات على متابعة الخطط المعتمدة يُقترح الاستعانة بملحق رقم 2 المُرفق. يجب تقديم الخطّة إلى مجلس الهيئة المحليّة للموافقة عليها وتضمين البنود المعتمدة في طلبات الموازنة.

1.2.6 عقد الصّيانة:

يجب أن تشمل عقود الشّراء للمعدات والبرمجيات عقود الصّيانة بحيث لا تتجاوز قيمة عقود الصّيانة السّنوي عن 14% من قيمة الشّراء في العقد الأصلي.

1.2.7 استبعاد أصول تكنولوجيا المعلومات والاتصالات والتّخلص منها:

على دائرة تكنولوجيا المعلومات والاتصالات تطبيق إجراء تخلصٍ خاصٍ بتكنولوجيا المعلوماتِ والاتصالاتِ وضمان استمراره، بحيث يشمل تحديد الأصول، وتقييم الأصول، والاعتماد، وطرق التّخلص، وإعداد التقارير، ويجب التخلص من جميع معدات الكمبيوتر القديمة المُحددة (في نظام معلومات إدارة المخزون "IMIS") وفقًا لإجراءاتٍ أمنيةٍ محددةٍ لحماية البيانات السّرية "غير العامة"، كما يجب إعداد نموذج "طلب التخلص" لتسجيل التّفاصيل المهمة للأصل واعتماده من قِبل دائرة تكنولوجيا المعلومات والاتصالات ودائرة إدارة أصول الهيئة المحليّة أو دائرة الشّؤون المالية.

1.3 السّياسات ذات الصّلة

1. سياسة التّعافي من الكوارث.
2. سياسة إدارة المخاطر.
3. سياسة النسخ الاحتياطي.

2. سياسة إدارة مخاطر تكنولوجيا المعلومات

2.1 المقدمة والأهداف

2.1.1 بيان السياسة

الغرض من هذه السّياسة هو وضع مبادئ توجيهية ومعايير لإدارة المخاطر التي تتعرض لها تكنولوجيا المعلومات التّابعة للهيئة الفلسطينيّة، وتشمل وضع إطار عمل؛ لتحليل وتقييم المخاطر والتخفيف من آثارها من خلال تحديد نقاط الضّعف والتّهديدات المحتملة في هذه البيئة وتقييم هذه المخاطر من أجل مجابهة هذه التّهديدات، ولتضمين الحلول المقترحة لمجابهة هذه المخاطر بحيث تكون متوافقة مع سياسات داعمه لها وتحديداً **سياسة التعافي من الكوارث وسياسة النسخ الاحتياطي وسياسة امن المعلومات.**

2.1.2 نطاق العمل

تنطبق هذه السّياسة على جميع الأجهزة والبنية التّحتية للتكنولوجيا والاتصالات التابعة للهيئة، والتي تديرها دائرة تكنولوجيا المعلومات، أو الخدمات التي تمَّ التّعاقد عليها من الباطن من خلال طرف ثالث، وكذلك جميع مستخدمي أجهزة التّكنولوجيا التّابعة للهيئة.

2.1.3 الهدف

الغرض من هذه السّياسة هو وضع مبادئ توجيهية ومعايير لوضع إطار عملٍ؛ لتحليل وتقييم المخاطر والتّخفيف من آثارها على تكنولوجيا المعلومات وعلى الوحدات التّنظيمية المختلفة بالهيئة المحلية بحيث يساعد تنفيذ هذه السّياسة على:

1. التّأكد من أنَّ الهيئة المحليّة تعمل بمستوى "مقبول" من المخاطر.
2. تمكين الهيئة المحليّة من إنشاء إطار رئيسي لتقييم المخاطر.
3. وضع ضوابط لمحاولة إيقاف وتجنب المخاطر قبل حدوثها و / أو التخفيف منها.
4. إنشاء في **(سياسة التّعافي من الكوارث)** وسائل بديلة للتّشغيل مقدماً مع الحدِّ الأدنى من الانقطاع من خلال حماية البيانات والنسخ الاحتياطي والاستعادة وأمن البيانات.

2.1.4 المسؤوليات

1. مسؤول تكنولوجيا المعلومات والاتّصالات هو المسؤول عن الحفاظ على هذه السّياسة.
2. يجب مراجعة السّياسة من قِبل اللّجنة التّوجيهيّة لتكنولوجيا المعلومات والاتصالات بالهيئة المحليّة أو المجلس البلدي على أساس سنوي وإعطاء الموافقة على أي تغييرات. يجب إعلام جميع الموظفين بالمخاطر المحتملة وأنواعها.

2.2 السياسات والإجراءات

1. تلزم هذه السّياسة دائرة تكنولوجيا المعلومات حماية الأنظمة الإلكترونية التابعة للهيئة والسّيطرة الكاملة عليها بما يشمل أي تعاملات مع "طرفٍ ثالث".
2. وضع إطار عملٍ لتحديد المخاطر التي تؤثر على عمل الهيئة المحليّة، وقدرتها على تقديم خدمات للمواطنين **(انظر إطار عمل إدارة المخاطر "RMF" المُتَّبع من قِبل المعهد الوطني للمعايير والتكنولوجيا التّابع للحكومة الأمريكية والمفصَّل بهذا الدّليل كمثال يمكن تبنّيه من قِبل الهيئة المحليّة)**
3. ينبغي تأسيس سياق لتقييم المخاطر على تكنولوجيا المعلومات بحيث تشمل المخاطر الدّاخلية والخارجيّة، ووضع أهداف لهذا السّياق وتحديد معايير لكل خطرٍ من المخاطر وكيفيّة تقييمها.
4. يتم تعريف هذه المخاطر وفقاً لمتطلبات سير الأعمال في الهيئة المحليّة ، وتقييم مستوى خطورة كل تهديد واتخاذ الإجراءات المناسبة والضّوابط الملائمة ضد التّهديدات بهدف إيقاف وتجنب المخاطر قبل حدوثها و / أو التخفيف منها بعد حدوثها.
5. تقوم لجنة التقييم بعمل خطة البنية التحتية الضرورية وتتضمن تحديد الأصول الضرورية، تعريف العلاقة بينهم،

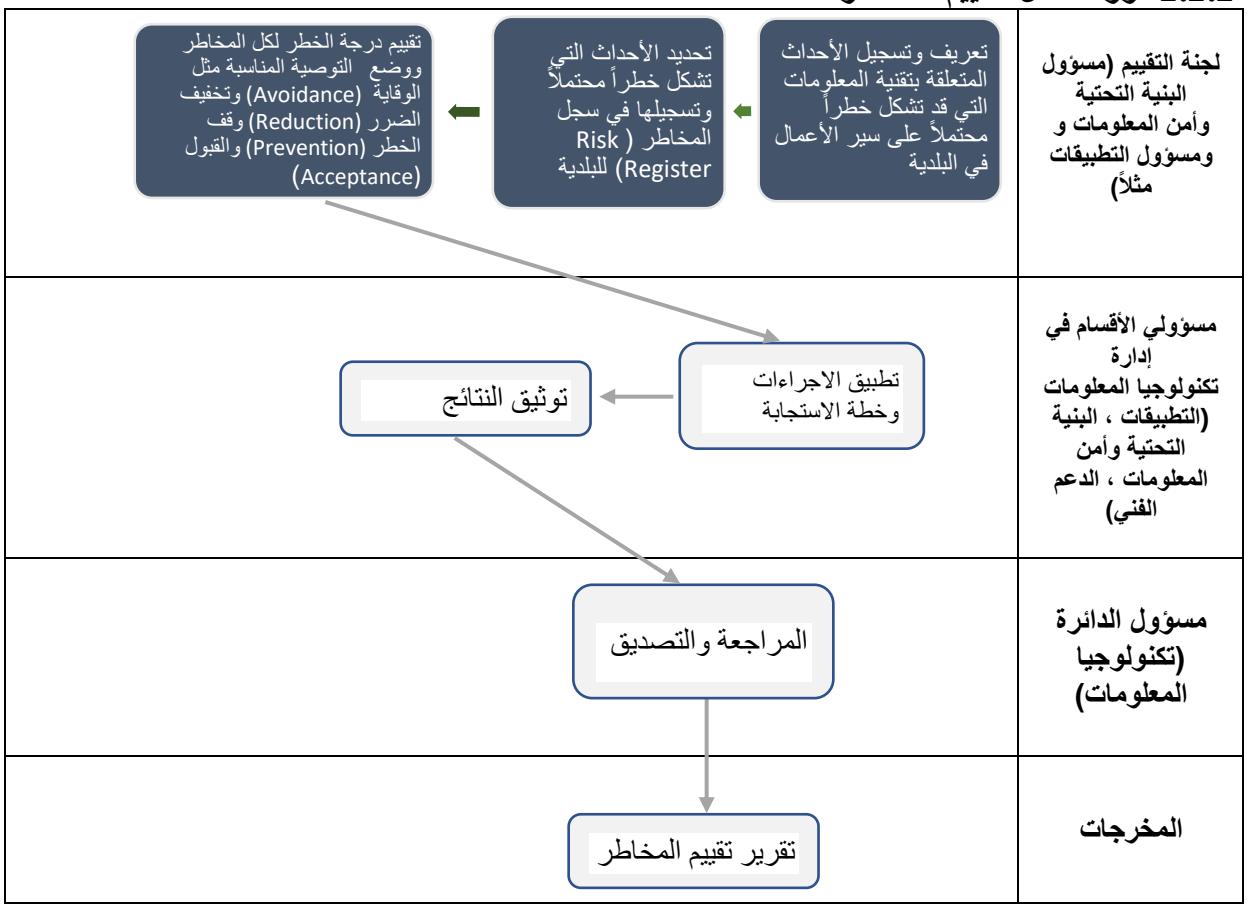
تحديد المصادر المطلوبة لمواجهة التهديدات، تحديد المصادر الخارجية للمساعدة، تحديد آليات تخفيف الخطر وعزل النظم التي تأثرت ومعالجتها، وتقليل ضياع المعلومات.

6. إنشاء في (**سياسة التعافي من الكوارث**) وسائل بديلة للتشغيل مقدماً مع الحدِّ الأدنى من الانقطاع من خلال حماية البيانات، والنسخ الاحتياطي، والاستعادة، وأمن البيانات.
7. يجب أن يكون جميع الموظفين على دراية بالتّهديدات المُحتملة التي حددتها الدّائرة حتّى يتم تدريبهم على كيفيّة التّعامل معها.
8. يتم عمل التقييم بشكلٍ دوريّ (سنوياً على الأقل) لتحديد نقاطِ ضعفٍ جديدة أو تهديداتٍ جديدة.

2.2.1 إجراءات تقييم المخاطر

الرقم	المسؤول	العملية	الوقت	الطريقة	المخرج
1	لجنة التقييم (مسؤول البنية التحتية وأمن المعلومات و مسؤول التطبيقات)	تعريف الأحداث المتعلقة بتكنولوجيا المعلومات التي قد تشكل خطراً محتملاً على سير الأعمال في الهيئة المحلية			سجل **الأحداث**
2	لجنة التقييم	تحديد الأحداث التي تشكل خطراً محتملاً وتسجيلها في سجل المخاطر (Risk Register)			سجل المخاطر المحدث
3	لجنة التقييم	التحليل - تقييم درجة الخطر ووضع التّوصية المناسبة لمعالجة الخطر مثل: 1. الوقاية (Avoidance) 2. الحد وتخفيف الضرر (Mitigation) 3. وقف الخطر (Prevention) 4. القبول (Acceptance)			لا يوجد
4	مسؤولي الأقسام في إدارة تكنولوجيا المعلومات (التطبيقات، البنية التحتية وأمن المعلومات، الدعم الفني)	تطبيق الإجراء وخطة الاستجابة للخطر، وبعد ذلك توثيق النتائج			لا يوجد
5	مسؤول تكنولوجيا المعلومات	مراجعة تقرير تقييم المخاطر وإجراء التعديلات إن وجد			تقرير تقييم المخاطر

2.2.2 دورة العمل لتقييم المخاطر



2.3 السياسات ذات الصلة

1. سياسة التعافي من الكوارث.
2. سياسة النسخ الاحتياطي.
3. سياسة أمن المعلومات.

إطار عمل إدارة المخاطر "RMF"

هناك العديد من الأساليب الدّولية لبناء إطار عمل إدارة المخاطر "RMF"، والعديد منها لديه مقاربات مماثلة لإطار عمل الأمن السيبراني الخاص بالمعهد الوطني للمعايير والتكنولوجيا التّابع للحكومة الأمريكية "NIST" كما هو موضح في القسم التالي، فيتكون إطار العمل الخاصّ بالمعهد الوطني للمعايير والتكنولوجيا التّابع للحكومة الأمريكية من سبع خطوات أساسية:

1.**الإعداد :** فإنّ الخطوة الأولى - حتّى لو كانت أنظمة الهيئة المحليّة تعمل بالفعل - فإنَّ **الإعداد** أمرٌ لا بدَّ منه لتحقيق بقيّة الخطوات، حيث تهدف خطوة التحضير إلى توفير الاستعدادات المناسبة المتعلقة بالمخاطر للهيئة ككل، فيتم تحديد أدوار إدارة المخاطر الرئيسة في هذه المرحلة، وتحدد استراتيجية إدارة المخاطر البيانات "المهمة" التي تتطلب أنظمة احتياطية واحتياجات معلومات الاسترداد المقابلة، وتحدد أي تكرار لحفظ المعلومات اللّازمة لضمان سلامة الأجهزة وسلامة البيانات لتغذية **سياسة التعافي من الكوارث** مع الإجراءات اللازمة، في هذه المرحلة أيضاً يجب على الهيئة المحلية تحديد مستوى تحمُّل المخاطر الذي يرتبط عادةً ارتباطاً وثيقاً بالميزانية المخصصة، وتحمُّل المخاطر هو مزيج من الأهميّة النّسبية للبيانات في البنية التّحتية والقدرة على التعافي في إطار زمني معقول مع العمليات المطبَّقة.
يجب إدخال هذه المعلومات في استراتيجية إدارة المخاطر ، ويجب توثيق الإجراءات والعمليات لتمكين المراجعة السّنوية.

2.التّصنيف : "تصنيف" تأثير المخاطر على الأنظمة. الهدف هو توثيق خصائص النظام وأمنه ليتم اعتماده من قِبل مسؤول تكنولوجيا المعلومات والاتصالات (انظر أيضا سياسة امن المعلومات).

3. الاختيار: الخطوة الثالثة هي "**تحديد**" الضّوابط اللازمة لحماية النظام في الهيئة المحليّة كنظام خاص أو مختلط أو مشترك.

4. التنفيذ : ينفذ الضوابط كعناصر التّحكم هي الخطوة الرابعة وللتأكد من تحديثها أيضاً وانعكاسها في ملف خُطط الأمان والخصوصية.

5. التقييم : هي لبناء خطّة عمل بناءً على نتائج خطوة التّنفيذ نحو الضّوابط المختارة وما إذا كانت قد نُفذت بشكلٍ صحيح وتعمل على النّحو المنشود لإنتاج نتائج الأمان والخصوصية المخطط لها.

6. والاعتماد : تخويل الصلاحيات من أجل تخصيص التراخيص لضوابط النّظام (التي يحددها مدير دائرة تكنولوجيا المعلومات والاتصالات) للتعامل مع استجابات المخاطر وضوابط النظام.

7. المراقبة: الخطوة الأخيرة، تحتفظ بجدول مراقبة مستمر بناءً على "إستراتيجية مراقبة معتمدة مصممة في خطوة التحضير" وستدعم مخرجاتها قرارات إدارة المخاطر.

3. سياسة التعافي من الكوارث

3.1 المقدمة والأهداف

3.1.1 بيان السياسة

تتطلب هذه السّياسة تحديد كيفيّة الحفاظ على التّحكم الفعّال في استرداد البيانات الإلكترونيّة في حالة وقوع أحداث تؤثر على عمل هذه الأجهزة، مثل فشل برنامج تشغيل قرص النظام أو أخطاء إدخال البيانات أو الكوارث الطبيعية؛ مما يعتبر عنصراً حاسماً في عمليات الهيئة المحليّة الفعّالة وأنظمة تكنولوجيا المعلومات الخاصّة بها ويجب توثيق هذه الإجراءات أثناء تنفيذ النظام وكجزءٍ منه .

3.1.2 نطاق العمل

تنطبق السّياسة بشكلٍ أساسيّ على دائرة تكنولوجيا المعلومات، المسؤول الأول عن حماية أنظمة تكنولوجيا المعلومات والاتصالات في الهيئة المحلية .

3.1.3 الهدف

1. تمكين الهيئة المحليّة من إنشاء وسائل تشغيل بديلة محددة مسبقاً مع الحدِّ الأدنى من الانقطاع.
2. حماية سريّة وسلامة المعلومات الواردة في أنظمة تكنولوجيا المعلومات والاتصالات والحدّ من مدى الأضرار المحتملة.
3. ضمان "استمرارية الأعمال" من خلال الاستخدام الفوري للبيانات الهامّة باستخدام عملية الاستعادة.
4. تقليل المخاطر القانونية.
5. تدريب الموظفين على إجراءات الطوارئ.
6. توفير استعادة سلسة وسريعة للخدمة.

3.1.4 المسؤوليات

1. مسؤول قسم تكنولوجيا المعلومات والاتصالات هو المسؤول عن الإشراف على تنفيذ هذه السّياسة.
2. تقوم اللّجنة التّوجيهية بتعيين فريق للطوارئ مسؤول عن تنفيذ الاسترداد.
3. قسم تكنولوجيا المعلومات والاتصالات هو القسم الوحيد في الهيئة المحليّة المسؤول عن سلامة أنظمة وبيانات تكنولوجيا المعلومات والاتصالات في الهيئة المحليّة.
4. يعتبر مدير الهيئة المحليّة "المالك" لإدارة استمرارية العمل، ويعتبر رؤساء الأقسام مسؤولين عن تحديد هدف وقت الاسترجاع، وهدف نقطة الاسترجاع بالاعتماد على مدى تأثير وحيويّة عمليات العمل.
5. تكون الدّائرة مسؤولة عن ترتيبات وخطط الاسترجاع التي تمكن من تحقيق هدف وقت الاسترجاع وهدف نقطة الاسترجاع للعمل.
6. تكون الدّائرة مسؤولة عن إدارة جميع الاتصالات (الدّاخلية والخارجية) المطلوبة حول استمرارية العمل والاسترداد.

3.2 السياسات والإجراءات

3.2.1 السياسات

1. يجب على الهيئة المحليّة تطوير ضوابط وإجراءات الاسترداد الخاصّة بها.
2. يجب إنشاء وسائل تشغيل بديلة محددة مسبقاً مع تحديد الحدِّ الأدنى من الانقطاع، وتحديد هدف وقت الاسترجاع وهدف نقطة الاسترجاع كما هو موضح أدناه.

تحديد هدف وقت الاسترجاع وهدف نقطة الاسترجاع

يعتبر هدف وقت الاسترجاع "RTO " وهدف نقطة الاسترجاع " RPO" جزءاً من خطّة استمرارية الأعمال (BCP)، والتي تحدد مخاطر الكوارث النّادرة على الهيئة المحليّة واتخاذ التدابير الوقائية منها، وإيجاد الحل لها.

بشكلٍ أساسيّ يقوم هدف وقت الاسترجاع "RTO " بالإجابة عن " متى يمكن استرجاع الخدمة وبشكل سريع بعد وقوع الكارثة؟"، وهي نقطة البداية من أجل تحديد ما هو نوع الانقطاع الذي يمكن للهيئة تحمله وما هي الإجراءات التي يجب اتخاذها من أجل الوصول إلى تحديد هدف وقت الاسترجاع والذي يتم تحديده من قِبل "المالك" للعمليّة من خلال تحليل التأثيرات على سير الأعمال. وستتضمن الخيارات الاستراتيجيّة القابلة للتطبيق أي إجراءات من شأنها أن تمكِّن من استئناف العمليات في الهيئة المحليّة في إطار زمني مقارب أو بالتحديد عند هدف وقت الاسترجاع، ثمّ تُقدم هذه اللوائح إلى الإدارة العليا لقبولها.

وأمّا هدف نقطة الاسترجاع " RPO" فهي تقوم بتحديد نقطة الاسترجاع المناسبة لعمليات النّسخ الاحتياطي للبيانات، وعلى سبيل المثال: إذا قررت إدارة تكنولوجيا المعلومات والاتصالات أنَّ فقدان البيانات أكثر من عدد ساعات معيّن سيتسبب في خسائر غير مقبولة أو أي أثرٍ سلبيّ آخر على العمليات، فإنَّ نقاط الاسترداد الاحتياطية ينبغي ألا تتجاوز هذا العدد من السّاعات، على سبيل المثال: 11 ساعة من البيانات لم يتم تضمينها في أحدث نسخة احتياطية.

3. يجب وضع أنظمة لحماية السريّة وسلامة المعلومات والحدّ من مدى الأضرار المحتملة.
4. يجب ضمان "استمرارية الأعمال" من خلال الاستخدام الفوري للبيانات الهامّة من خلال عمليّة الاستعادة لتقليل المخاطر القانونيّة.
5. الاسترداد بطريقة تُحقق التّوازن بين ضمان ضوابط أفضل الممارسات وكفاءة الخدمة المقدمة وفقاً لمتطلبات النّظام وتوصيات البائع وبتوافقٍ تام مع المنصوص عليه في سياسة النسخ الاحتياطي.
6. يجب تدريب جميع الموظفين على إجراءات الطوارئ لتوفير استعادة سلسة وسريعة للخدمة.

3.2.2 إجراءات الاسترداد

بالنّسبة للأنظمة المدعومة من الموردين، اتبع جميع تعليمات الموردين والموثقة لدى قسم تكنولوجيا المعلومات، أما بالنسبة للأنظمة المطورة داخلياً، اتّبع التعليمات التالية:

1. بالاعتماد على هدف وقت الاسترجاع وهدف نقطة الاسترجاع الموضوعة من دائرة العمل والمقرة من قِبل الإدارة، فتقوم الدائرة بتحديد أولويات الاسترداد.
2. تحديد ترتيب استرداد تكنولوجيا المعلومات. ما الذي سيتم تفعيله أولا – الخوادم ومحطات العمل والبريد الإلكتروني، إلخ – استناداً إلى أهميّة العمليات التي تم تحديدها بالخطة.
3. إذا تمّ اختراق البيانات، فاحذف الملفات واستعد أحدث نسخة احتياطية "نظيفة".
4. إذا تمّ اختراق برنامج التطبيق ، فاحذف جميع ملفات البرنامج وأعد تثبيت البرنامج باستخدام الوسائط الأصلية للمورد.
5. إذا تم اختراق أنظمة التّشغيل أو الأمان أو برامج الاتصالات السلكية واللاسلكية ، وكان التوقيت أمراً بالغِ الأهميّة ، فقم على الفور بتثبيت خادم النسخ الاحتياطي لتوفير الوقت "لتنظيف" النظام وإعادة تثبيت واختبار جميع البرامج على النظام الأصلي.

يجب أن يتضمن توثيق عملية الاستعادة ما يلي :

أ. تحديد البيانات والبرامج الهامّة والاسترشاد بسياسة تحديد المخاطر.
ب. عناصر التوثيق والدعم اللازمة لأداء المهام الأساسية للهيئة أثناء عملية الاسترداد.
ت. إجراءات الاسترداد.
ث. وضع تعليمات خاصّة بالإدارة المسؤولة في حالة تشفير البيانات.

3.2.3 اختبار إجراءات الاستعادة

1. يقوم موظفي الدّائرة تحت إشراف المسؤول (وبمشاركةٍ من فريق الطوارئ) بعمل اختبار برامج النظام والنسخ الاحتياطية للبيانات عن طريق استعادة عينة من النسخ الاحتياطية وفقاً لجدول رسمي في بيئة الاختبار للتأكد من أنها لا تؤثر على بيئة الإنتاج.

2. يكون مدير قسم تكنولوجيا المعلومات مسؤولاً عن التَّحكم في اختبار النسخ الاحتياطي والإشراف عليه كما هو محدد بسياسة النسخ الاحتياطي .
3. يجب فحص إجراءات الاستعادة بانتظام على الأقل على أساس شهري واختبارها للتّأكد من أنّها فعالة، وأنّه يمكن إكمالها في غضون الوقت المخصص في الإجراءات التشغيلية للاسترداد.
4. ضمان إمكانية الوصول: هو الوقت الفعلي لاسترجاع البيانات.
5. يجب الاحتفاظ بالأدلَّة الموثّقة لعمليات الترميم الاحتياطية.
6. وضع خطط التواصل (الدّاخلية والخارجية).

3.3 السياسات ذات الصّلة

1. سياسة إدارة المخاطر.
2. سياسة النسخ الاحتياطي.
3. سياسة شراء أصول تكنولوجيا المعلومات.

4. سياسة إدارة التغيير

4.1 المقدمة والأهداف

4.1.1 بيان السياسة

تمّ وضع هذه السّياسة لضمان التّحكم الفعّال بجميع المتغيرات التي تطرأ على أنظمة المعلومات الرئيسة وتطبيقاتها في البيئة التشغيلية، أو البنية التّحتية لتكنولوجيا المعلومات كي يتسنى الحدّ من احتمالات انقطاع أو توقف خدمات تكنولوجيا المعلومات وتوفير ضمانات معقولة لأنّ التغييرات محددة ومصرَّح بها، وقد تمّ اختبارها واعتمادها وتطبيقها وتوثيقها بشكلٍ صحيح.

4.1.2 نطاق العمل

تنطبق هذه السّياسة على جميع الأجهزة والبنية التّحتية للتكنولوجيا والاتصالات التّابعة للهيئة والتي تديرها دائرة تكنولوجيا المعلومات، أو الخدمات التي تمّ التّعاقد عليها من الباطن من خلال طرفٍ ثالث، أو الدّعم التّقني.

4.1.3 الهدف

1. تقليل المخاطر المرتبطة بالتغيير.
2. وتقليل الأخطاء إلى الحدّ الأدنى عندما يحصل تغيير في أنظمة التكنولوجيا.
3. تنفيذ التغييرات المفيدة بأقل قدر ممكن من تعطيل خدمات تكنولوجيا المعلومات.
4. وضع معايير وإجراءات محددة لضمان التّحكم الفعّال على التغييرات الطارئة أو العادية لأنظمة المعلومات الرئيسة والبنية التّحتية للهيئة بهدف ضمان استمرار تقديم الخدمات للمواطنين والمحافظة على المعلومات.

4.1.4 المسؤوليات

1. يعتبر مسؤول الدائرة أو من ينوب عنه مسؤولاً عن تنفيذ هذه السياسة.
2. يشكّل مسؤول الدّائرة **المجلس الاستشاري للتغييرات** لدراسة طلبات التغييرات تتكون من مديري الدوائر التّابعة له ومدير الدائرة التي تقدمت بطلب التغيير ولديها الصلاحيات الكاملة بإعطاء الموافقات أو الرّفض ضمن الإجراء المنصوص عليها بهذه السياسة.
3. على مسؤول الدّائرة أن يقوم بتشكيل **المجلس الاستشاري للتغييرات** الطّارئة تشمل على الأقل بالإضافة إلى شخصه، المسؤول المباشر عن دائرة الدّعم الفنّي وأي مسؤولين آخرين من الدّوائر الفنيّة الأخرى حسب تقييمه للاحتياجات ، ولديها الصّلاحيات الكاملة بإعطاء الموافقات أو الرفض ضمن الإجراء المنصوص عليها بهذه السياسة.
4. في حال اختلاف المجلس الاستشاري على القرار المُتخذ، يعتبر مسؤول الدائرة أو من ينوب عنه المسؤول النهائي عن إعطاء الموافقات لعمل أي تغييراتٍ بالنّظام سواء كانت طارئة أو عادية، ضمن الإجراء المنصوص عليه بهذه السّياسة.
5. على موظفي الهيئة المحلية التبليغ عن أي خللٍ بعمل الأجهزة أو عطل في تقديم الخدمات.
6. على لجنة التغييرات الاجتماع لمراجعة ودراسة طلبات التغيير، ومدى تأثيرها على الدوائر المختلفة بالهيئة المحليّة وللتأكد من أنَّ الجداول الزّمنية لعمل التغييرات أو أي أمور أخرى مرتبطة وأنه قد تمّ التعاطي معها.
7. أي طلب للتغيير يتعلق بمخطط مبرمج لوقف الأنظمة عن العمل أثناء الدّوام الرّسمي للهيئة ولأي مدة من الزمن، يجب أن يتم بموافقة مدير الهيئة المحليّة بالإضافة إلى الموافقات الأخرى المطلوبة.
8. وجوب الحصول على قرار مدير الهيئة المحلية (الإيجاب أو الرفض)، أو من ينوب عنه لعمل أي تغييرات على النظام تعتبر ذو تأثير **عالي**.
9. تعقد الاجتماعات حسب الاقتضاء.

4.2 السياسات والإجراءات

4.2.1 السياسات

1. يجب أن تتأكد الهيئة المحليّة من القيام بالإدارة والسّيطرة على جميع التّغييرات بشكلٍ رسمي على أنظمة المعلومات، والبنية التّحتية لتكنولوجيا المعلومات التّابعة للهيئة.
2. وجوب تصنيف التغييرات بناءً على الآتي:

أ. **التغيير القياسي**: تغيير قليل الخطورة ومتكرر ومعتمد سابقاً لا يتطلب خطّة فحص للتأثيرات أو تقديم طلبٍ للتغيير، ولكن يجب توثيقه وعلى مدير الوحدة التي تأثرت بالتغيير التوقيع على القرار الإداري المتعلق بالتغيير (بعد حصوله)، مثل: إعادة ضبط كلمة المرور، أو إضافة حاسوب للشبكة.

ب. **التغيير الاعتيادي**: ليس تغيير قياسي أو تغيير طارئ وهي التغييرات (رئيسية أو صغيرة) المخطط لها، وتمّ دراستها واعتمادها قبل التغيير، وتم توثيقها.

ت. **التغيير الطارئ:** تغييرات غير مخطط لها ولم تكن متوقعة، ويوجد أولوية طارئة نظراً لأهميّة إجرائها بشكلٍ مستعجل، مثل: **الرقع الأمنية**، وبدون توثيق، ويجب التّعامل مع هذه الحالة فوراً وبالتالي يعطى الأولوية على التغييرات العادية ولا يخضع لمعاييرها نظراً لضيق الوقت ووجوب إجرائها بأسرع ما يمكن (أرجو مراجعة سياسة الدعم الفني).

3. ينبغي أن يتم تسجيل وتقييم التغييرات واعتمادها قبل تنفيذها ويجب مراجعتها بعد تنفيذها ومقارنتها بالنتائج التي قد تم التخطيط المسبق لها.
4. تقوم الدّائرة بجميع الإجراءات للتغييرات العادية وفقاً لإجراءات إدارة التغيير المقترحة في هذه السّياسة.
5. من المهم أن تنتبه الدّائرة لتأثيرات التغيير على سلامة وأمن المعلومات، وأن تتخذ الإجراءات المناسبة.
6. من الضروري أن تقوم الدائرة بتحديد الأنظمة التي قد تتأثر جراء التغيير ووجوب إشراك المسؤولين عن هذه الأنظمة بالمعلومات لما له تأثير على سير العمليات لديهم.
7. وجوب الحصول على الاعتماد المناسب من مسؤول الدّائرة للبدء بعمل التغييرات.
8. يسمح فقط بإجراء التغييرات المصرح بها على إعدادات أنظمة المعلومات.
9. يفضل اختبار التغييرات العادية في بيئة الفحص أولاً قبل التصريح بتطبيق التغييرات في البيئة التشغيلية.
10. تعطى الأولوية للحالات الطارئة للتغيير، ويمكن لإدارة الدّائرة أن تتجاوز مؤقتاً الإجراءات لإدارة التغيير "العادية" وفقط إلى الحدّ الذي يعتبر ضرورياً لضمان استمرار عمل الهيئة المحلية.
11. تخصيص لجنة طوارئ في الدّائرة تشمل بالإضافة إلى مسؤول الدّائرة، رئيس قسم الدّعم الفنّي مثلاً أو مديري الأقسام.
12. أيّ طلبٍ للتغيير الطارئ يجب أن يتم التعامل المباشر معه من قِبل لجنة الطوارئ لدراسته وإرساله إلى مسؤول الدائرة أو من ينوب عنه لمراجعته وإعطاء الرأي النهائي.
13. يتم إجراء التغييرات الطّارئة بشكلٍ فعّال وبالسّرعة الواجبة وفقاً لإجراءات التغييرات الطارئة.
14. بعد الانتهاء من عمل التغييرات الطارئة، يجب استكمال وإغلاق طلب التغيير الطارئ على غرار الإجراءات المتّبعة في حالة التغييرات العادية.
15. وجوب إبلاغ مسؤولي الدائرة التي تأثرت عملياتها بآخر المستجدات بشأن حالة التغيير في أنظمة المعلومات، (انظر سياسة الدعم الفني)
16. تقوم خدمة الدّعم الفنّي بالمحافظة على سجل خاص لمتابعة وتوثيق التغييرات على أنظمة تكنولوجيا المعلومات والاتصالات والبنية التحتية.

4.2.2 كيفية تحديد الأولويات

تستخدم مكتبة البنية الأساسية لتكنولوجيا المعلومات (ITIL) ثلاث أدوات للقياس لتقرر الترتيب التي يجب التعامل من خلالها مع الحدث (انقطاع غير مخطط له أو توقف بالخدمة) وتحديد وضع التغيير:

1. **التأثير**:
   أ. **المنخفض**: يؤثر على عمل الموظفين بشكل فردي ولكن يمكن تجاوز المشكلة من خلال طرق بديله.
   ب. **العادي**: يؤثر على عمل الموظف بشكل فردي.
   ت. **العالي**: يؤثِّر على عمل الأجهزة الأساسية والحسّاسة.

2. **مدى الضرورة**: إلى أي مدى يمكن تأجيل الحلّ أو المدة الزّمنية المطلوبة لحلّ الحادث:
   أ. 1: إلى 0.5 ساعة .
   ب. 2: إلى 2.0 ساعة .
   ت. 3: إلى 6.0 ساعات.

3. **الأولوية:** ما هي السّرعة الواجبة لمعالجة الحادث، وعلى سبيل المثال يتحدد من خلال الآتي:
   أ. الأولوية : (1: 16)ساعة.
   ب. الأولوية: (2: 8)ساعات.
   ت. الأولية : (3: 4)ساعات.
   ث. حساس : (4: 2)ساعات.

تقترح ايتيل (ITIL) أن تكون الأولوية لنتاج الأثر والضرورة كما تبين الآتي:

	مدى الضرورة 1	مدى الضرورة 2
الأثر 1	الأولوية 1	**الأولوية 2**
الأثر 2	**الأولوية 2**	**الأولوية 3**
الأثر 3	الأولوية 3	**الأولوية 4**

ملاحظة: يجب الانتباه أنَّ تحديد المُدة الزّمنية لتنفيذ الحلول عبارة عن توقعات توضع من قِبل الدّائرة آخذين بعين الاعتبار إمكانية الحاجة لتدخل طرفٍ ثالث.

4.2.3 الإجراءات

4.2.3.1 طلب التغيير الاعتيادي:

يتم تقديم طلب التّغيير من خلال خدمات الدّعم الفنّي (الواجهة الرئيسة والأولى لتقديم الدّعم). يُرسَل طلب التّغيير إلى الأشخاص المحددين للتعامل مع هذه الحالات في الدّائرة ليتم دراسته وتقييمه وتجهيزه إلى المجلس الاستشاري، بحيث يوثّق المعلومات حول التغييرات المطلوبة مع الشّرح الوافي عن أسبابه، والتي من الممكن أن تكون مثل:

1. حادث أدّى إلى تغييرٍ جديد.
2. تغيير نتيجة مشكلة معروفة.
3. المستخدم يطلب تغيير.
4. مسؤول الدّائرة أو مَن ينوب عنه يطلب تغيير كجزء من الصّيانة المستمرة.

لإتاحة المجال للدراسة، يجب تقديم الطلب العادي:

أ. قبل (#) أيام عمل من موعد عرضه على المجلس.
ب. قبل (#) أيام عمل إذا كان بحاجة إلى تقييم المخاطر قبل عرضه على المجلس.

يشمل عملية طلب التغيير الاتي:

1. **التخطيط**: يشمل تحديد الأسباب للتغيير، كالجهات والوظائف التي تتأثر بالتغيير والنتيجة المرجوَّة من التغيير، الخطوات المطلوبة للتنفيذ ويشمل تحديد الأشخاص المسؤولين عن التغيير، المخطط الزّمني وطريقة العمل للتنفيذ، تحديد متطلبات الاختبار (التقدير و \أو خطة الفحص)، وفي حالات معينه خطط لإصلاح التغيير.

2. **التقييم**: تحديد آثار التّغيير والمخاطر المحتملة (انظر سياسة تقييم المخاطر) وتحديد متطلبات الأمن للمعلومات وتحديد التّكاليف المقدّرة لعمل التّغيير، وتقدير الفوائد التي تعود على الهيئة المحليّة وتوثيقها.
3. **المراجعة**: تدارس التغيير مع موظفي القسم و\أو اللجنة الاستشارية.
4. **الموافقة**: يجب أن تحصل جميع طلبات التغيير على الموافقات المناسبة من قِبل مدير الدّائرة التي تطلب التغيير والمجلس الاستشاري وأي موافقات أخرى مطلوبة.
5. في حال تمّ رفض التغيير، يتم إبلاغ مقدِّم الطّلب بالنتائج مع الأسباب، مثل: عدم وجود مصادر أو تضارب بجداول الأوقات.
6. في حال اعتماده من قبل المجلس الاستشاري للتغييرات، يتم البدء:

أ. تحديد أولويات التغيير: طارئ ام عادي
ب. تحديد أولويات الإجراءات في طلب التغيير لتخصيص الموارد الرئيسة.
ت. تحديد جدول زمني للتنفيذ.

7. **التّواصل**: تحديد الإدارات التي من الممكن أن تتأثر بالتغيير من أجل اطلاعهم على المستجدات وتوثيق التغيير وإبلاغ مقدِّم الطّلب.
8. **التنفيذ**: عند إصدار الأمر للفريق المعني ببدء التنفيذ (الذي يُعتبَر المسؤول عن التغيير)، يتم وضع خطّة بإجراءات محددة للتنفيذ، والقيام بتطوير، أو إرسال طلب شراء العناصر التكنولوجية اللّازمة للتنفيذ (انظر سياسة شراء أصول تكنولوجيا المعلومات).

أ. سيقوم الفريق المسؤول عن التنفيذ، بفحص التغييرات المطلوبة في بيئة الفحص مستخدماً الأدوات المناسبة، وبوضع خطّة العلاج، والتي تشمل إما التقويم أو إجراءات إعادة العمل أو استخدام خطط استمرارية الخدمة للتراجع عن التغيير المعتمد كما هو مشار في سياسة أمن المعلومات في حال فشل تنفيذ التغيير.
ب. قبل البدء بالتنفيذ في البيئة التشغيلية، يتم إعلام جميع الدوائر ذات العلاقة والتي قد تتأثر من التغيير.
ت. عند تنفيذ التغييرات في البيئة التشغيلية يجب اختيار أوقات مناسبة لعمل التغييرات بحيث تقلل من فترات انقطاع خدمات تكنولوجيا المعلومات.
ث. تقوم خدمة الدّعم الفنّي بإعلام الجهات ذات العلاقة بوضع التغييرات.

9. **التوثيق**: في حال الانتهاء من التغيير، يقوم المسؤول عن فريق التغيير ومسؤول الدّائرة بعمل مراجعة لجميع التغييرات والقيام بتحديث حالة التغييرات المنفذة بنجاح بأنها أُغلقت، وتوثيق التغييرات بالسجل.
10. **مراجعة ما بعد التغيير:** مراقبة التغييرات بهدف الحصول على تحسينات مستقبلية.
11. تقوم خدمة الدعم الفني بإعلام مقدم الطلب "بإغلاق " طلب التغيير.
12. على جميع طلبات التغيير العادية أن تتبع إجراءات التشغيل القياسية (SOP) ومن ضمنها الحصول على الموافقات المناسبة.
13. يستطيع الشّخص المسؤول تغيير وضع طلب التغيير من عادي الى رئيسي أو طوارئ متجاوزاً بقية الإجراءات.

4.2.3.2 طلب التغيير الطارئ:

1. إذا كان طلب التّغيير "طارئ" فيجب إحالته فوراً إلى المجلس الاستشاري للطوارئ لتتبع الطّلب ولدراسته وتقييمه وبناءً على المعطيات المتوفرة للوصول إلى رأي واضح (الموافقة أو رفض التغيير) وفي حال الموافقة على التغييرات الطارئة يجب تحديد الأولويات.
2. يجب تقديم الطّلب الخاص بالحوادث الرئيسة من أجل المتابعة والرّصد من قِبل خدمة الدّعم الفني، وأي استثناءات بهذا الخصوص يجب أن تكون مُعلّلة وبموافقةِ مدير الوحدة التي تقدمت بالطلب.
3. في حال الوصول إلى قرار بالموافقة للتغيير واعتماده، يمكن التغاضي عن الأنشطة التفصيلية المقررة" للتغييرات العادية" مؤقتاً، والبدء الفوري بتنفيذ الخطة للتغييرات المستعجلة لاحتواء الوضع الطارئ.
4. بعد احتواء الوضع الطارئ يقوم مسؤول الدّائرة أو من ينوب عنه بعمل تقييم للتغييرات الطارئة التي تمت لاتخاذ قرار إما الإبقاء على التغييرات بشكلٍ دائم، أو عمل إجراء تعديلات وتحسينات إضافية عليها مع توثيق التغييرات بالسّجل الخاص بالتغييرات.
5. يجب وضع خطة التّراجع عن الأعمال إذا تقرر بوجوب إضافة تعديلات جديدة.

4.2.3.3 المتابعة بعد عمل التغيير

بعد عمل التغييرات وفحصها يتوجب اتباع الإجراءات التالية:

1. يقوم مسؤول الدّائرة وقائد فريق التّنفيذ بمراجعة جميع التغييرات المنفذة وتوثيق النتيجة بأنّها نُفّذت بنجاح وتمّ إغلاق الملف (في حالة الطلب العادي والطوارئ فقط).
2. تقوم خدمات الدّعم الفنّي بإدخال المعلومات على السجل وإخطار طالب الخدمة \ مالك الخدمة بالنتيجة المقررة وتقييم النتيجة.
3. تقوم خدمات الدّعم الفنّي بتوثيق النّتيجة وحفظ المستندات، وإعلام طالب الخدمة بأنَّ الطّلب قد "أُغلق".
4. تقوم الدائرة بعمل تقييم للجدوى الفنيّة والتأثير الكامل للتغيير من خلال الآتي:

أ. الأداء
ب. القدرة.
ت. الأمن.
ث. قابلية التشغيل.

4.2.3.4 التحقق من التغييرات

تقوم خدمة الدّعم الفنّي بعمل تقييم للتغيرات مع طالب التغيير، أو الوحدة المتأثرة بالتغيير بمراجعة الآتي:

1. برتوكول الإجراءات.
2. الشّخص المسؤول.
3. المجموعة الدّاعمة.
4. وقت وتاريخ التغيير.
5. وصف للنّشاط.
6. توثيق أي إجراءات اتُّخذت لتفادي الحدث واستمرار العمل.
7. توثيق الأسباب التي أدت إلى الحدث وانقطاع الخدمة.
8. تاريخ تطبيق الحلّ.
9. تاريخ إغلاق الملف.
10. تحديد النتائج بعد عملية التغيير.

4.3 خدمة الدعم الفني

1. سيقوم الدّعم الفنّي باتّباع الإجراءات المقرة بسياسة الدّعم الفنّي من أجل توثيق الطّلبات، إبلاغ المتقدّمين بطلب التغيير بالتّطورات، إبلاغ الدّوائر التي تتأثر بالتغيير، ومتابعة حالة طلب التغيير.
2. سيقوم الدّعم الفنّي بتوثيق اجتماعات لجنة التغييرات والقرارات المتخذة.
3. سيقوم الدّعم الفنّي بإدخال طلبات التغيير بسجل متابعة التّغييرات مع إعطاء صفة الوضعية كما حددتها سياسة الدّعم الفنّي، (أرجو مراجعة سياسة الدعم الفني).
4. سيقوم الدّعم الفنّي بتحديث صفة الوضعيّة النهائي في سجل التغييرات وتوثيق الوثائق المتعلقة بالطّلب .

4.4 السياسات ذات الصلة

1. سياسة خدمة الدّعم التّقني.
2. سياسة شراء أصول تكنولوجيا المعلومات.
3. سياسة أمن المعلومات.

5. سياسة إدارة موردي تكنولوجيا المعلومات

5.1 المقدمة والأهداف

5.1.1 بيان السياسة

تمَّ وضع هذه السّياسة لضمان التّحكم الفعّال بتعاقدات الهيئة المحليّة مع جميع الموردين الذين تعتمد الهيئة المحليّة عليهم لتزويدها بأجهزة أو برامج جديدة أو خدمات (طرف ثالث)، وقد تتعاقد الهيئة المحليّة مع مورد لتثبيت البرامج أو إزالة أو نقل أجهزة الكمبيوتر وخدمات الاتصالات وموظفي الدّعم والاستشاريين. يجب أن يتّبع جميع الموردين العملية القياسية في هذه السياسة.

5.1.2 نطاق العمل

تنطبق هذه السّياسة على جميع موظفي الهيئة المحليّة المسؤولين عن التّفاوض أو تنفيذ العقود الخاصّة بالجهات الخارجية "الموردين" نيابة عن الهيئة المحلية .

5.1.3 الهدف

تسعى هذه السّياسة إلى تقليل المخاطر المرتبطة بالتّعاقد مع الجهات الخارجية وتقليل الأخطاء إلى الحدّ الأدنى من خلال التّحكم في التّكاليف، ورفع التّميز في الخدمة سعياً وراء زيادة القيمة المضافة والعائد على الاستثمار من تطوير الخدمات، كما تسعى إلى تحديد الموردين الذين قد يعرضون عمل الهيئة المحليّة للخطر ووضع الضّوابط لتقليل تلك المخاطر.

5.1.4 الإعفاءات

ليست جميع تعاقدات الموردين مهمّة، أو سيكون لها تأثير مالي كبير على الهيئة المحليّة لذلك لن يُطلب من الموردين الذين يستوفون معايير معينة (يجب أن تقررها اللّجنة التّوجيهية لتكنولوجيا المعلومات والاتصالات) الالتزام بجميع مكّونات هذه السّياسة، بالإضافة إلى ذلك يمكن تقديم طلبات الإعفاءات أو الاستثناءات من هذه السياسة رسمياً إلى مجلس الهيئة المحليّة الذي يقدم الموافقات كتابياً.

5.1.5 المسؤوليات

1. يشكّل مسؤول الدّائرة **اللجنة التوجيهية لتكنولوجيا المعلومات والاتصالات** من موظفي الهيئة المحليّة مكونة من مسؤول الدّائرة، مسؤول الخدمة، مسؤول الدائرة التي تطلب الخدمة "مالك الخدمة" ومدير المشتريات.
2. مسؤول الدّائرة هو المسؤول عن الإشراف والحفاظ على هذه السياسة.
3. يجب مراجعة السياسة من قِبل اللّجنة التوجيهية لتكنولوجيا المعلومات والاتصالات على أساس سنوي.
4. على مسؤول الخدمة تنفيذ هذه السياسة وإدارة العلاقة الفنية مع المورد بما في ذلك الإبلاغ الفوري عن أي تغييرات عامّة في المخاطر التي تتعرض لها الهيئة المحليّة.
5. إدارة المشتريات / المالية مسؤولة عن العقود القانونيّة الموقَّعة مع البائع .
6. وجوب الالتزام بجميع القوانين الفلسطينية ذات الصلة وتحديداً قانون الشّراء العام ونظام الشّراء العام.
7. إدارة المشتريات / المالية هي المسؤولة عن إدارة عقود المورّدين بناءً على المدخلات من مسؤول الخدمة.
8. قسم تكنولوجيا المعلومات والاتصالات هو القسم الوحيد في الهيئة المحليّة المسؤول عن سلامة أنظمة وبيانات تكنولوجيا المعلومات والاتصالات في الهيئة المحلية.

5.2 السياسات والإجراءات

5.2.1 يجب تقييم الموردين:

تطوير نظام قائم على محددات واضحة لتقييم الموردين المستقبليين وبشكل سريع من خلال وضع حدٍّ أدنى مقبول لجودة أيّ مورد بمراجعة أمان البيانات والمراجعات المستقلة، ومن ضمنها مراجعة مدى قدرته على تقديم الخدمة المطلوبة، واتفاقية مستوى الخدمة وكيف ستساعد هذه الخدمات الهيئة المحليّة بتقديم خدمة أفضل، كذلك يجب أن نفهم المخاطر المرتبطة باستخدام الموردين تحديدها، وكيف يمكن **للدّائرة** تحديد أي قضايا أو مخاوف أو قيود تتعلق في

دعم إدارة مخاطر الموردين من خلال تنفيذ أنشطة رقابة أخرى تحددها اللجنة لضمان الامتثال للسياسات الداخلية / اللوائح الخارجية .

أفضل الممارسات لإدارة مخاطر الموردين :

1. حدّد جميع الموردين الخارجيين الذين تربطهم علاقات بالهيئة المحليّة.
2. حدّد مخاطر الأمن السيبراني التي يمكن للموردين أن يعرّضوا الهيئة المحلية لها (راجع سياسة تقييم مخاطر تكنولوجيا المعلومات).
3. تقييم الموردين وتصنيفهم حسب المخاطر المحتملة، والقدرة على تخفيف المخاطر التي تفوق قدرة الهيئة المحلية على تحملها، وبالتّالي يجب فهم المخاطر التّالية وتقييمها بدقّة فيما يتعلق بالعمل والعلاقات التعاقدية المبرمة مع الموردين :

أ. **المخاطر الإستراتيجية**: خطر الفشل في تنفيذ أو تحقيق الأهداف المخططة، أو مبادرات العمل المخطط لها، وعدم القدرة على معالجة الأساسيات المطلوبة لتنفيذ الإستراتيجية المتَّفق عليها، كما يتضح من الانحرافات عن خطط العمل.

ب. **مخاطر الامتثال**: المخاطر الناشئة عن انتهاكات القوانين والقواعد والتفويضات التنظيمية المعمول بها جنباً إلى جنب مع القضايا الأخرى، مثل: عدم الامتثال للسياسات والإجراءات والعمليات التشغيلية وأمن المعلومات.

ت. **المخاطر التشغيليّة**: هي المخاطر النّاجمة عن فشل نظام الضّوابط الدّاخلية التشغيلية المتعلقة بالسّياسات والإجراءات والممارسات ذات الصلة، على وجه التحديد حالات الفشل المرتبطة بالعمليات أو الأنظمة أو الأشخاص.

ث. **مخاطرة ماليّة**: هي المخاطر المتعلقة بالوضع المالي للموردين، مثل أن يكون المورد تحت تهديد التّصفية في المستقبل المنظور.

ج. **مخاطر السّمعة:** مخاطر تكوين رأي عام سلبي، ناتجة على سبيل المثال من الممارسات التّجارية غير الأخلاقية، أو انتهاكات البيانات التي تؤدي إلى فقدان معلومات المستهلك الحسّاسة والسّرية.

ح. **مخاطر التكنولوجيا** : المخاطر النّاجمة عن أي عددٍ من قضايا تكنولوجيا المعلومات وإدارة المعلومات والأمن، بما في ذلك عدم كفاية الموارد (الأجهزة أو البرامج أو القوى العاملة) .

خ. **المخاطر المرتبطة بالدّول**: المخاطر الناشئة عن المشهد السّياسي والاقتصادي والاجتماعي والأحداث الأخرى ذات الصّلة داخل بلدٍ أجنبيّ، والتي يمكن أن تؤثر على الخدمات التي يقدمها الموردون ، مما يؤثر في النهاية على عمليات الشركة .

د. **المخاطر البيئية والاجتماعية والحوكمة**: المخاطر المتعلقة بآثار تغير المناخ، والممارسات البيئية وواجب الرّعاية، وظروف العمل والسلامة، واحترام حقوق الإنسان، والامتثال للقوانين واللّوائح.

4. **إنشاء دور "مسؤول الخدمة "** لإدارة العلاقات مع الطرف الثالث وكذلك يعتبر المسؤول عن إدارة مخاطر الموردين وجميع ممارسات إدارة المخاطر الأخرى. يجب على **اللجنة التوجيهية لتكنولوجيا المعلومات والاتصالات** إسناد مسؤولية "مسؤول الخدمة" إلى أحد موظفي تكنولوجيا المعلومات والاتصالات، وبغض النّظر عمن يتولّى دور مسؤول الخدمة، يجب أن يشارك مسؤولي تكنولوجيا المعلومات والاتصالات والمشتريات في مراجعة واختيار الموردين، وسيتم إشراك المسؤول عن الدّائرة، ويُسمى "مالك الخدمة" التي تتلقى الخدمات.
يجب أنْ يكون لهم رأي في تقييم مبررات العمل الضرورية، والمساعدة في الموافقة على البائعين أو رفضهم وفقاً لذلك.

5. تعيين خطوط دفاع:

لضمان الإدارة الفعّالة للمخاطر، حدد ثلاثة خطوط دفاع:

أ. **خط الدّفاع الأول**: يعتبر "مسؤول الخدمة" مسؤولاً عن تحديد وتقييم وتخفيف أنشطة المخاطر، وتنفيذ الضّوابط.

ب. **خط الدفاع الثاني**: يقوم مسؤول الدائرة ومسؤول دائرة المشتريات في دعم إدارة مخاطر الموردين من خلال تنفيذ أنشطة رقابة أخرى تحددها اللجنة لضمان الامتثال للسياسات الداخلية / اللوائح الخارجية .

ت. **خط الدفاع الثالث**: يوفر التدقيق الداخلي للبلدية تأكيدات مستقلة من خلال تزويد مجلس البلدية بتقارير تقييم التصميم والفعالية التشغيلية لأنشطة إدارة المخاطر والضوابط الداخلية لعملية إدارة الموردين.

6. ضع خطط طوارئ في حال أنّ خدمات المورد كانت أقل من الجودة المتوقعة أو عند حصول اختراق للمعلومات حيث يمكنك تقليل تأثير الفشل من خلال وضع خطة تجاوز "الفشل" والتي يمكن أن تتضمن الآتي:

1. تعرّف على ما يتأثر بفشل خدمة المورد، بالإضافة إلى ما يقدمه المورد حالياً:

أ. يجب على مسؤول الخدمة تحت إشراف مدير تكنولوجيا المعلومات والاتصالات إنشاء رسم تخطيطي لجميع البائعين، والخدمات التي يقدمونها، مع تبيان تواجد أي ترابطات بينهم. تأكد من أنّ هذا الرّسم البياني يسرد أيضاً رقم هاتف الدّعم واسم الشّخص المسؤول، حتّى تتمكن من الاتصال بهم فوراً للحصول على أحدث التّطورات.
ب. قم بإنشاء خطّة استجابة داخليّة لكل مورد تحسباً لحالة حدوث فشل ممكن من خلال تحديد ما هي الخطوات اللازمة للاستجابة.
ت. يجب وضع الآليات لتجاوز توقف النظام الرئيسي بشكلٍ تلقائيّ كما هو منصوص عليه في سياسة التعافي من الكوارث وسياسة النسخ الاحتياطي.

2. اكتب استجابة نموذجيّة لإبلاغ المستخدمين النهائيين بالفشل: أثناء التّركيز على استعادة الخدمات، يجب أن يكون التّواصل الواضح حول الوضع الرّاهن للخدمات جاهزاً للنّشر على قنوات التّواصل الاجتماعي التّابعة للهيئة.

5.2.2 كتابة العقود

1. معلومات العقد:
يجب على مسؤول الخدمة تحت إشراف مسؤولي تكنولوجيا المعلومات والاتصالات والمشتريات مراجعة العقد للتّأكد من وجود الآتي:
أ. الشّروط والتّجديدات ومستويات الخدمة المطلوبة ومتطلبات الإنهاء.
ب. يتضمن العقد قائمة الخدمات ويسلّط الضّوء على معايير الجودة التي يجب على المورد اتباعها لضمان رضا عملاء الهيئة المحليّة .
ت. يجب أنْ يُشير العقد متطلبات تقديم التقارير وإلى سبل معالجة الثّغرات والمشاكل المتوقع حدوثها.
ث. العقود التي تتضمن تبادل بيانات حسّاسة (على النحو المحدد في سياسة أمن المعلومات)، يجب أنْ تؤكد على المورد الالتزام بسياسة عدم الإفصاح التّابعة للهيئة والقوانين الفلسطينية (الموجودة بهذه السّياسة) ، مع تحديد وجوب الالتزام بالسّياسات الخاصّة والإجراءات المعمول بها (على وجه الخصوص سياسة الأمن الرقمي، وسياسة النَّسخ الاحتياطي، وسياسة تقييم المخاطر) والتي يخضع لها المورد.
ج. يجب أنْ يتم تحديد متطلبات الإبلاغ عن الحوادث الأمنية والعقوبات المتوقعة لعدم التّسليم.

2. التفتيش والمراجعة:
يجب أنْ تتمتع الهيئة المحليّة بالقدرة على فحص ومراجعة عمليات الموردين بحثاً عن المخاطر المحتملة لعمليات أو بيانات الهيئة المحلية، وقد تتضمن هذه المراجعة فحصاً ماديّاً مخططّاً وغير مخططٍ للموقع، واختبار نقاط الضّعف الفنيّة، وفحص الوثائق، مثل: نتائج اختبار الأمان وخطط التّعافي من الكوارث.

3. تجديد العقد
يجب على الإدارات التي تنوي تجديد العقود الحالية تضمين الإجراءات الخاصّة بهذه السّياسة.

5.2.3 متطلبات تقديم التقارير

1. يجب أنْ تُحدّد العقود بوضوح متطلبات إعداد التّقارير الأمنية التي تنص على أنَّ البائع مسؤول عن الحفاظ على أمان البيانات الحساسة بغضّ النّظر عن المُلكية، ويجب أنْ يرسل تقارير منتظمة تركّز على أربع مجالات رئيسة للمخاطر المحتملة:
أ. الوصول غير المصرَّح به إلى الأنظمة.
ب. البيانات المخترقة.
ت. فقدان سلامة البيانات.

ث. عدم القدرة على نقل البيانات أو معالجتها.

2. في حالة حدوث خرق لأمن البيانات الحسّاسة، يكون المورد مسؤولاً عن إخطار إدارة تكنولوجيا المعلومات والاتصالات / الهيئة المحليّة على الفور والعمل معهم فيما يتعلق بالاسترداد والمعالجة.
3. يجب أنْ تشمل العقود متطلبات الإبلاغ الأمني في حالة حدوث خرقٍ للبيانات الحسّاسة المتبادَلة أو خسارتها في غضون 24 ساعة من الخسارة أو الاختراق المشتبه به.
4. **الاستثناءات**: يجب تدوين أي استثناءات من النّشاط العادي في التقارير، ومراجعتها، وتحديد الرّدود المناسبة.
5. يتعيّن على البائعين الامتثال لجميع سياسات أمن معلومات الهيئة المحليّة المعمول بها.

5.2.4 اتفاقيات عدم الإفصاح

أ. يجب توقيع جميع الموردين الذين سيتمتعون بإمكانية الوصول إلى المعلومات السريّة للهيئة على اتفاقية عدم الإفصاح (NDA) التّابعة للهيئة وأي قوانين فلسطينيّة بهذا الخصوص.
ب. تقع على عاتق مدير قسم تكنولوجيا المعلومات والاتصالات مسؤوليّة التأكد من توقيع الاتفاقية قبل أيّ عمل يتم تنفيذه أو الإفراج عن أي معلوماتٍ سريّة بالهيئة المحليّة .

5.2.5 إنهاء الخدمة

من الممكن أن تحصل تطورات متعددة تؤدي إلى إنهاء الخدمات، مثل: انتهاء العقود، أو شروط التّعاقد قد تمّ تنفيذها، أو نتيجة خلل بالتّنفيذ، أو التغيير بإستراتيجية الهيئة المحليّة، وبالتّالي يجب أن تتضمن العقود:

1. القدرات، التّكاليف، المصادر المطلوبة وتحديد الإطار الزّمني.
2. المخاطر المرتبطة بالاحتفاظ بالبيانات وتدميرها وأيّ ارتباطاتٍ أخرى.
3. كيفيّة التّعامل مع حقوق الملكيّة التي قد تكون قد تطورت أثناء فترة التّعاقد.
4. أيّ مخاطرٍ أخرى مرتبطة بالسمعة نتيجة النّزاع حول التّعاقد أو التّنفيذ.
5. يجب على مديري المشتريات والعقود التّأكد على الفور من إنهاء الوصول إلى أنظمة معلومات الهيئة المحليّة والمرافق التي تضم هذه الأنظمة.

5.2.6 المراقبة

تعتبر المراقبة المستمرة لأداء الموردين بالإنفاق المالي والمخاطر المترتبة على ذلك من المكونات الرئيسة لسياسة إدارة موردي تكنولوجيا المعلومات، وتتم المتابعة من خلال:

1. تحليل أداء الموردين بالإنفاق المالي من خلال (تقرير مستند إلى البيانات).
2. أداء المورد.
3. مُراقبة مستمرة للمخاطر.
4. تحديد أداة المورد تقنيا وفنيا.

5.3 السياسات ذات الصلة

1. سياسة أمن المعلومات.
2. سياسة إدارة المخاطر.
3. سياسة النّسخ الاحتياطي.
4. سياسة الدّعم التّقني.
5. سياسة شراء أصول تكنولوجيا المعلومات.

6. سياسة الاستعانة بمصادر خارجية

6.1 المقدمة والأهداف

6.1.1 بيان السياسة

تعتمد هذه السّياسة على الاستعانة بمصادر خارجيّة، أو ما يسمّى "الطّرف الثالث" لتنفيذ نشاط مملوك للهيئة ضمن اتفاق وعلى أساس مستمر بما يتيح للهيئة القدرة على الاستفادة من مصادر تستطيع تقديم الخدمة المطلوبة، مثل: دعم الأجهزة والبرمجيات وموظفي الصّيانة، مستشارين وبائعين خارجيين مقابل رسوم؛ وبذلك تستفيد الهيئة المحليّة من الحصول على موارد غير متاحة داخلياً مع إدارة أفضل للتكاليف.

تغطّي السّياسة الجوانب التّالية للتّعاملات مع الطّرف الثالث:

- تقييم مخاطر الطّرف الثالث.
- الاتفاقيات والعقود.
- توفير خدمات للشّبكة.
- صلاحيّات الوصول للأنظمة والشّبكات .
- أمن الوصول من قِبل الأطراف الثّالثة.
- امن المعلومات والحفاظ عليها من التلف والضياع.

6.1.2 النطاق

تنطبق هذه السّياسة على الموظفين في الهيئة المحليّة المختصين بتوفير وصول الأطراف الثّالثة إلى شبكة الهيئة المحليّة، أو الأجهزة الملحقة بها، أو الموردين، أو الأطراف الثّالثة (سواء كانوا أفراداً، أو شركات، أو مؤسسات، أو متعاقدين، أو استشاريين، أو متخصصين)، الذين يشاركون في تقديم الخدمات نيابةً عن الهيئة المحليّة.

6.1.3 الهدف

توفر هذه السّياسة إرشاداتٍ في تقييم ما إذا كان من الممكن استخدام مصادرٍ خارجيّة لتقديم خدمة مرتبطة بتكنولوجيا المعلومات، أو الأنشطة ذات الصّلة وكيفية القيام بذلك، ويجب ألّا تقلل ترتيبات التّعاقد مع المصادر الخارجيّة من قُدرة الهيئة المحليّة على الوفاء بالتزاماتها تجاه المواطنين، ولا تُعيق الإشراف الفعّال من قِبل الموظفين المُعيَّنين.

6.1.4 المسؤوليات والأدوار

1. "مالك" الخدمة هو مدير القسم الذي يستعين بمصادر خارجيّة؛ لتنفيذ مهمةٍ أو وظيفة معينه.
2. يدير "مسؤول الخدمة" العلاقة مع المورد وسيتابع تنفيذ خدمات الاستعانة بمصادر خارجيّة.
3. يحق للجنة الاستشارية التي تتكون من مسؤول الخدمة، ومسؤول الدّائرة، ومدير المشتريات، و "المالك" الاستعانة بمزوّد خارجي أو "الموردين"؛ لتأدية وظيفة / عمليّة تابعة للهيئة كما تنص عليه سياسة إدارة الموردين.
4. سيقوم مسؤول الدّائرة بتنفيذ هذه السّياسة.

6.2 السياسات والإجراءات

6.2.1 مبادئ الاستعانة بمصادر خارجية

1. التّحديد والتّوثيق بإنشاء استراتيجيّة رسميّة .
2. تخضع الخدمات التي تمَّ تعهيدها لنفس الضّوابط الإدارية كما لو أنّها لم يتم تعهيدها.
3. يجب على قسم تكنولوجيا المعلومات والاتصالات التّأكد من أنَّ خدمات التّعهيد ستظهر بوضوح في المخطط التّنظيمي للهيئة.
4. من الممكن عمل لكلّ خدمة خارجيّة وصف وظيفي يتم إنشاؤه لها بنفس الطّريقة كما لو كان التّنفيذ يتم داخلياً، ويتم توثيق هذا الوصف الوظيفي مع الوثائق الأخرى المتعلقة بمقدِّم الخدمة.

5. من النّاحية المثالية يجب أن تكون الخدمات التي تم تعهيدها ضمن اتفاقيات موثّقة تتضمن: اتفاقية مستوى الخدمة، وعمليات المراجعة، وفترة الخدمة، وتفاصيل الخدمة، والقيود المفروضة على أنشطة التّعهيد، ومتطلبات إدارة المخاطر، والقضايا الماليّة المتعلقة بالقدرات، وإلغاء العقد، والتأمين، وعمليات النّزاع.
6. من الناحية الفنية، يجب تطبيق قانون سرية وامن المعلومات المتعلق بالهيئات المحلية.

6.2.2 العناية الواجبة

يجب استخدام العناية الواجبة المناسبة على النّحو المبيَّن في هذه السّياسة عند الاستعانة بطرفٍ ثالث لتنفيذ نشاطٍ ما ولديها القدرة على التّنفيذ، وخاصّةً أنَّ إدارة المخاطر المرتبطة تنتقل إلى الطّرف الثّالث التي قد تفشل في تقديم الخدمات المطلوبة، بالتالي ستكون الهيئة المحليّة مسؤولة. يجب اتباع عمليّة تقييم صارمة للمخاطر لتقييم مقدّمي الخدمات الخارجيّة مقابل المعايير التالية:

6.2.2.1 معايير اختيار المصادر الخارجية "الطرف الثالث"

يجب تحديد وتوثيق معايير اختيار الطّرف الثّالث، مع مراعاة ما يلي :

1. طول الخبرة : سمعة الشّركة وتاريخها.
2. جودة الخدمات المقدمة للعملاء الآخرين: مراجعة أي أعمال سابقة للتّأكد من مستوى الخدمات مثلاً.
3. عدد وكفاءة الموظّفين والمديرين.
4. الاستقرار المالي للشّركة.
5. أداء حلّ النّزاع.
6. أداء التّعافي من الكوارث.
7. معايير الاستجابة والتّواصل.
8. احتمالات النّزاع.
9. معايير ضمان الجودة وإدارة الأمن التي تتبعها الشّركة حالياً ،على سبيل المثال: الامتثال(ISO 9000وISO / IEC 27001).
10. الالتزام بمعايير الأمان الإضافيّة التّي تمّ تعريفها نتيجة لعمليّة تقييم المخاطر.
11. اتّباع التّعليمات والإرشادات المتعلقة بالإدارة الفعّالة للمخاطر المحدّدة **بسياسة إدارة الموردين**.

6.2.3 الإستراتيجية وتقييم المخاطر

1. يجب تحديد مسؤول الخدمة و المالك.
2. يجب على المالك تقييم المخاطر قبل الاستعانة بمصادر خارجيّة.
3. يجب على المالك تقييم الأثر المتوقع إذا ما تمَّ الاستعانة بالمصادر الخارجيّة.
4. يجب على مسؤول الخدمة و المالك دراسة المعطيات حول تقييم المخاطر والآثار المتوقعة قبل الاستعانة بمصادر خارجيّة للوظيفة / العملية ، باستخدام عمليّة الاختيار الموضّحة أعلاه.
5. يجب على مسؤول الخدمة و المالك مراعاة التأثير على الأنظمة الحاليّة والمخاطر المرتبطة بها لاتخاذ قرار بشأن طبيعة الوصول المنطقي والمادي إلى أصول معلومات الهيئة المحليّة والمرافق المطلوبة من قِبل الطّرف الثّالث للوفاء بالعقد (**انظر سياسة أمن المعلومات سياسة إدارة موردي تكنولوجيا المعلومات**):

أ. **إنشاء الاتصال:** يجب أن يستند كلّ اتصالٍ قائم على مبدأ "أقل صلاحيات الوصول" وفقاً لمتطلبات العمل والمراجعة الأمنية المعتمدة .
ب. **تعديل أو تغيير الاتصال والوصول:** يجب أنْ تتم التّغييرات في الاتصال أو الوصول بناءً على ما تقتضيه مصلحة العمل وأنْ تخضع للمراجعة الأمنية، كما يجب تنفيذ التغييرات من خلال عمليّة إدارة التغيير بـ الهيئة المحلية .
ت. **وصول الطّرف الثّالث المسموح به :** يسمح للطّرف الثّالث الوصول إلى أنظمة أو شبكة الهيئة المحليّة للأغراض المتفق عليها في العقد، ويشمل ذلك شركاء الهيئة المحليّة غير الموظفين مباشرة ولديهم وصول مباشر، أو عن بعد إلى أنظمة وشبكة الهيئة المحلية.
ث. يجب السّماح للطّرف الثّالث بالوصول إلى المرافق والخدمات والبيانات التي تكون مطلوبة لتنفيذ المهام المحددة في العقد فقط، وعلى النّحو الذي تم توضيحه للمسؤولين على هذه المرافق والبيانات ضمن طلب الوصول الأصلي.
ج. حساسيّة وحجم وقيمة أي أصول معلومات ذات صلة.

ح. المخاطر المترتِّبة عن احتمال فشل عمل الطّرف الثّالث تماماً، أو الفشل في تلبية مستويات الخدمة المُتفق عليها.
خ. يجب تقديم جميع مقترحات عقود الاستعانة بمصادر خارجيّة بغضّ النّظر عن التكاليف الإجماليّة إلى مجلس الهيئة المحليّة للموافقة عليها قبل الدّخول في أي التزامات / عقود مع المورد.
د. سيقوم المجلس بدراسة العقد للتّأكد من أنّه يتماشى مع الأهداف الإستراتيجية للهيئة ويقرر ما إذا كانت الهيئة المحليّة ستستفيد من الاستعانة بمصادر خارجيّة للوظيفة، مع مراعاة جوانب أمن المعلومات. إذا كانت المخاطر التي ينطوي عليها الأمر عالية وكانت فوائد الهيئة المحليّة هامشيّة، على سبيل المثال: إذا كانت الضّوابط اللّازمة لإدارة المخاطر مكلفة للغاية، فلن يتمّ الاستعانة بمصادر خارجيّة للوظيفة.
ذ. يجب تسجيل معلومات المخاطر ذات الصّلة على النّحو المنصوص عليه في سياسة تقييم المخاطر.
ر. إذا كان الطّرف الثّالث لديه حق الوصول إلى "البيانات الحساسة"، فيجب إجراء مراجعة دورية له للحصول على تأكيد معقول بشأن الضّوابط والفعاليّة التشغيلية.

6.2.4 السرية والعقود المكتوبة

يجب أنْ تحكم علاقات الاستعانة بمصادر خارجيّة عقود مكتوبة تصف بوضوح جميع الجوانب الماديّة لترتيب الاستعانة بالطّرف الثّالث، بما في ذلك حقوق ومسؤوليات وتوقعات جميع الأطراف.

1. يجب أنْ يحدَّد العقد الرسمي بين الهيئة المحليّة والمتعاقد الخارجي بوضوح أطراف العقد، والتاريخ الفعلي، والوظائف أو الخدمات المقدَّمة (مثل مستويات الخدمة)، والمسؤوليات، والقيود المفروضة على استخدام المقاولين من الباطن والمسائل التجارية / القانونية الأخرى العادية لأي اتفاقية.
2. يجب أنْ يُحدِّد العقد بوضوح أنواع المعلومات التي يتم تبادلها والغرض من ذلك. إذا كانت المعلومات التي يتم تبادلها حساسة (سرية)، يجب أن تكون هناك اتفاقية سريّة ملزِمة بين الهيئة المحليّة والمتعاقد الخارجي، سواء كجزء من عقد الاستعانة بمصادر خارجية أو اتفاقية منفصلة لعدم إفشاء السّر.
3. يجب أن تتخذ الهيئة المحليّة خطوات لضمان قيام مقدمي الخدمات بحماية المعلومات السريّة من الكشف المتعمد، أو غير المقصود للأشخاص غير المصرَّح لهم. يتم تناول هذا في السّياسة الرّقمية لتكنولوجيا المعلومات، و سياسة إدارة بائعي تكنولوجيا المعلومات والإجراءات.
4. اعتماداً على نتائج تقييم المخاطر، يجب تضمين العديد من الضّوابط الإضافيّة أو الإشارة إليها في العقد لمراقبة جميع عمليات الوصول إليه، واستخدام مرافق الهيئة المحليّة وشبكاتها وأنظمتها وما إلى ذلك، وللسماح بمراجعة امتثال المتعاقد الخارجي للعقد.
5. بعد المراجعة من قِبل خدمات المشتريات والتّأكد من ذكر امتيازات الهيئة المحلية بوضوح، يجب تقديم جميع العقود إلى الشؤون القانونية للبلديات للحصول على الموافقة النهائية.

6.2.5 إدارة النزاعات

من المتوقع في أي علاقة مع طرفٍ ثالث أنْ يكون هناك تضارب في المصالح من حينٍ لآخر وانتهاكات محتملة تنشأ نتيجة الخروج عن المصالح المشتركة. إنَّه يمثل خطراً يجب على الهيئة المحلية مراعاته، سواء كانت النزاعات فعلية أو محتملة، فيجب على الهيئة المحلية اعتماد نموذج لحل النزاعات المتوقعة بناءً على العمليات التّالية المقترحة:
حيث ينشأ نزاع أو خرق للعقد، سينهي "مسؤول الخدمة" و "المالك" الخلاف فوراً من خلال ما يلي:

أ. **السيطرة على النزاع:**

1. تحديد الخلاف (الحالي أو المستقبلي).
2. تقييم خطورة الخلاف وتقييم الآثار.
3. تحديد الرد وكيفية تنفيذه.
4. التأكد من عدم تأثر الخدمات بشكلٍ كبير.

ب. **الكشف عن النزاع**

يتعيَّن على الطّرف الثّالث إبلاغ "مسؤول الخدمة" عن أي تضارب في المصالح قد ينشأ فيما يتعلق بتقديم الخدمات من أجل السيطرة عليه.

ج. **تجنب النزاعات**

1. إذا كان النّزاع له تأثير كبير على الهيئة المحليّة، فيجب تجنبه بأيّ ثمنٍ حتّى تؤدي عمليات السيطرة على الخلافات أو الكشف عن الخلافات الى حلّ الإشكال.
2. في هذه الحالة سيطلب "مسؤول الخدمة " من مسؤول الدائرة التّدخل لتجنب الخلاف.
3. يجب على مسؤول الدائرة حل النزاع في غضون 14 يوماً، واعتماداً على خطورة الأمر، يمكن اعتماد التدابير البديلة التّالية إذا لم يتم تصحيح الخلاف :
   أ. قبول الفشل، أو خرق الطّرف الثّالث للعقد.
   ب. إحالة الأمر إلى محكمين لحلّ المنازعات.
   ت. إحالة الأمر إلى المستشارين القانونيين للهيئة.
   ث. التوصية بإنهاء عقد التوريد أو الاتفاقية إلى المجلس البلدي للنظر فيها.
   ج. التوصية لمجلس الهيئة المحلية بخدمات بديلة من مورد بديل.

6.2.6 المراقبة والتقييم (انظر سياسة إدارة موردي تكنولوجيا المعلومات)

1. يجب على مسؤول الخدمة (خط الدّفاع الأول) تقديم تقارير الأداء بما في ذلك تقارير المخاطر، والامتثال، والتقييم على أساسٍ شهريّ.
2. سيقدم مسؤول الدّائرة (خط الدفاع الثاني) تقريراً سنوياً عن ترتيبات الاستعانة بمصادر خارجية.
3. يجب على إدارة التّدقيق الدّاخلي في الهيئة المحليّة (خط الدّفاع الثّالث) المراجعة بانتظام أي تعهيد مقترح لنشاط وظيفي\ عملي وتقديم تقرير إلى المجلس بشأن الامتثال لسياسة الاستعانة بالمصادر الخارجيّة التّابعة للهيئة.
4. سيقوم المجلس البلدي بتقييم خدمات المصادر الخارجية واعتماد / تغيير أنشطة التعهيد رسمياً.

6.2.7 الملكية الفكرية

الهيئة المحلية هي المالك الوحيد لجميع الوثائق والملفات وقواعد البيانات والبرمجيات والرسومات أو أي محتوىً آخر تم إنشاؤه أو تصميمه أو تطويره أو شراؤه من قبل "المورد" للهيئة ويعتبر ملكاً للهيئة ويجب أن يظلّ كذلك بعد إنهاء الاتفاقية مع المورد.

6.2.8 خطط الطوارئ

يجب أنْ تَتبع إدارة تكنولوجيا المعلومات والاتصالات سياسة التعافي من الكوارث، وسياسة النسخ الاحتياطي لوضع خطط الطوارئ والحفاظ عليها.

6.3 السياسات ذات الصلة

- سياسة الأمن الرقمي.
- سياسة إدارة مخاطر تكنولوجيا المعلومات.
- سياسة إدارة بائعي تكنولوجيا المعلومات.
- سياسة إدارة موردي تكنولوجيا المعلومات.

7. سياسة النسخ الاحتياطي لتكنولوجيا المعلومات والاتصالات

7.1 المقدمة والأهداف

7.1.1 بيان السياسة

تعمل هذه السّياسة بشكلٍ أساسي على توفير حمايةٍ شاملةٍ لبيانات الهيئة المحلية، كما تسعى إلى تحديد ضوابط النسخ الاحتياطي للبيانات واستعادتها لموظفي الهيئة المحلية؛ وذلك لضمان نسخ البيانات احتياطيّاً بشكلٍ صحيحٍ وفعّالٍ واستعادتها بما يتماشى مع أفضل الممارسات، كما تستهدف السّياسة أيضاً توحيد منهجيّات النَّسخ الاحتياطيّ المستخدمة لتحسين تكامل الأنظمة التي يتمّ استضافتها وحفظ البيانات بشكلٍ آمن.

7.1.2 نطاق العمل

تنطبق السّياسة على كلّ فردٍ يستخدم أو يتفاعل مع البنية التّحتية لدائرة تكنولوجيا المعلومات والاتصالات في الهيئة المحلية، بما في ذلك الجهات الخارجيّة، ومقدمي الخدمات، والاستشاريين، كما تشمل أيضاً جميع بيئات أنظمة المعلومات التي يتم تشغيلها من خلال الهيئة المحليّة، أو عن طريق أيَّ جهةٍ خارجيةٍ تتعاقد معها الهيئة المحلية، وتُعد الهيئة المحلية المالك الوحيد لجميع المعلومات الإلكترونية الموجودة على أيّ نظام كمبيوتر تابع للدوائر، ووفقاً لسياسة البريد الإلكتروني، يجوز لإدارة الهيئة المحلية الاطلاع على أي معلوماتٍ أو اتصالاتٍ يتم إجراؤها أو تلقيها أو استلامها باستخدام أيٍّ من الأنظمة المذكورة أعلاه، وكذلك مراقبتها وأخذ نسخٍ منها.

7.1.3 الهدف

وُضعت سياسة النَّسخ الاحتياطي للبيانات لتوجيه الهيئة المحليّة ومساعدتها على مواكبة أفضل الممارسات المُعترف بها دولياً؛ لدعم التَّحكم الفعّال في النَّسخ الاحتياطي للبيانات الإلكترونيّة وتعزيزه، ولتمكين استعادة البيانات في حالة وقوع أحداثٍ كفشل برنامج تشغيل قرص النّظام، أو أخطاء إدخال البيانات، أو الكوارث الطّبيعية، و تعدُّ هذه السّياسة عنصراً حاسماً في الحماية الفعالة لبيانات الهيئة المحليّة وأنظمة دائرة تكنولوجيا المعلومات والاتصالات الخاصة بها.

يساعد تنفيذ هذه السّياسة على:

1. معالجة مخاطر فقدان البيانات.
2. الحفاظ على سريّة وسلامة المعلومات الموجودة في أنظمة تكنولوجيا المعلومات والاتصالات.
3. ضمان "استمرارية الأعمال" عن طريق الاستخدام الفوري للبيانات الهامة من خلال عملية الاستعادة.
4. تحديد ضوابط فرض أنشطة الدّعم وعمليات النسخ الاحتياطي المُنتظمة بما يحد من تأثير أي مخاطر مرتبطة بإدارة عمليات النسخ الاحتياطي للبيانات واستعادتها.

7.1.4 المسؤوليات

1. دائرة تكنولوجيا المعلومات والاتصالات هي الجهة الرئيسة المسؤولة عن سلامة البيانات الإلكترونية.
2. مسؤول دائرة تكنولوجيا المعلومات والاتصالات بالهيئة المحليّة هو المسؤول عن الإشراف على تنفيذ هذه السياسة.
3. يجب على مسؤول دائرة تكنولوجيا المعلومات والاتصالات تفويض موظفين (أحدهما أساسي، والآخر احتياطي)؛ من أجل الالتزام والتقيد بكل جدولٍ زمنيٍ للنسخ الاحتياطي.
4. يُصرّح مسؤول الدائرة لعدد محدود من الموظفين بالوصول إلى النَّسخ الاحتياطية.
5. يتحمل مجلس الهيئةِ المحليّةِ (أو لجنة فرعية متخصصة) مسؤولية مراجعة أي تغييراتٍ وتدقيقها واعتمادها (على أساسٍ سنويّ).

6. يتحمَّل كلُّ مسؤولٍ، ورئيس وحدة، والموظفين مسؤولية التأكد من أنَّ استخدام بيانات الهيئة المحليّة يتوافق مع الإرشادات المُوضحة في هذه السّياسة.
7. يتحمَّل كلُّ موظفٍ مسؤولية الالتزام الدّقيق ببروتوكولات هذه السّياسة لضمان السّلامة الكاملة لمعلومات الهيئة المحلية .
8. من واجب المُستخدِم (بمساعدة الدّعم الفنّي) ضمان استعادة جميع المستندات المتعلقة بالعمل على خادم الملفات ضمن الدّليل المُخصص له.
9. يجب أنْ يتأكد مسؤول تكنولوجيا المعلومات من اكتمال جميع النّسخ الاحتياطية بنجاح، بالإضافة إلى النسخ الاحتياطي للبيانات الخاصّة بالدّوائر، فيجب على دائرة تكنولوجيا المعلومات إجراء إدارة منتظمة لسعة القرص على جميع خوادم البيانات، ويحقُّ لها حذف جميع البيانات غير الخاصّة بالدّوائر ذاتِ الصّلة بعد التّشاور مع الموظفين المعنيين.
10. يجب على مسؤول تكنولوجيا المعلومات مراقبة حالة جميع عمليات النّسخ الاحتياطي التي يتم إجراؤها، ويجب تصحيح أيَّ أخطاءٍ يتم تحديدها.
11. يجب على مسؤول تكنولوجيا المعلومات وموظفي تكنولوجيا المعلومات التّأكد من عمل نسخة احتياطية من قِبل كلّ موظف قبل تثبيت الدُفعات أو الترقيات وبعده، أو إجراء أي تغييرات في التّكوين على النّظام. ويمكن تحقيق ذلك باستخدام مجموعة من نُسخ الصّور أو النُسخ الاحتياطية المتزايدة أو النُسخ الاحتياطية الجزئية أو سجلّات المعاملات أو أي تكنولوجيا أخرى.

7.2 السياسات والإجراءات

7.2.1 تحديد البيانات الهامة:

يجب أن تُحدِّد الهيئة المحليّة "البيانات الهامّة" الضروريّة لاستمرارية العمل للهيئة من أجل الحفاظ عليها عن طريق عمليات النسخ الاحتياطي الكاملة والدورية ونقلها خارج الموقع إلى موقعٍ آمن لتمكين آليات الاستعادة (حسبما هو منصوصٌ عليه في سياسة التعافي من الكوارث).

تتضمن البيانات التي يتعين نسخها احتياطياً ما يلي:

1. بيانات المستخدمين المُخزَّنة على خادم الملفات في الدّليل المخصص لكلّ مستخدم.
2. جميع البيانات والبرامج المتعلقة بالتّشغيل المستمر للهيئة والتّطبيقات والمعلومات والتّكوين بشكلٍ منتظم، ويشمل ذلك:
   أ. خادم Exchange Server، وجميع رسائل البريد الإلكتروني.
   ب. صندوق البريد.
   ت. حالة النّظام لجميع الخوادم بما في ذلك وحدة تحكم المجال الأساسية (PDC)، ووحدة تحكم مجال النسخ الاحتياطي (BDC)، وخادم WSUS، وخادم البريد.

7.2.2 التعامل مع البيانات المحذوفة

يجوز لدائرة تكنولوجيا المعلومات والاتصالات أن تقرر حذف امتدادات ملفاتٍ معينة من النُسخ الاحتياطية، مثل امتداد AVI لملفات تداخل الصوت والفيديو، أو امتداد Mpeg لنوع ملفات الأفلام والفيديو الرقمية، أو ملفات من نوع MP4 أو غير ذلك حسب الضرورة.

7.2.3 تشفير النسخ الاحتياطي

يجب تشفير النُسخ الاحتياطيّة من أجل الحفاظ على بيانات الهيئة المحليّة السريّة وغير العلنية والمحافظة على سلامتها ولمنع استخدامها من الأشخاص غير المخولين لذلك.

7.2.4 مرافق النسخ الاحتياطي

1. يجب أن يكون للهيئة مرافق تخزين نُسخ احتياطية خاصة بها في مقراتها.
2. يجب تخزين وسائط النسخ الاحتياطي خارج الموقع، في موقعٍ محميٍّ بيئيّاً يمكن التحكم في الوصول إليه، ويقع على مسافةٍ كافيةٍ (يُقترح 6 كيلومترات)؛ وذلك لتجنب أي ضررٍ ناتجٍ عن كارثةٍ في الموقع الرئيسي أو للتّخزين طويل الأجل، إلى جانب سجلاتٍ دقيقةٍ وكاملةٍ للنُسخ الاحتياطية وإجراءات الاستعادة المُوثقة.
3. يُنصح باستخدام وسيطِ تخزينٍ مناسبٍ، مثل: النسخ الاحتياطي المستند إلى السحابة لتأمين البيانات الهامة وأرشفتها بشكلٍ صحيح. قد يتضمن وسيط النّسخ الاحتياطيّ نسخاً متماثلاً للبيانات أو خادماً متطابقاً في موقعٍ بعيد (مع اتصالٍ مباشر بالخادم الرئيسي إن أمكن).
4. يمكن إجراء النّسخ الاحتياطي يدويّاً من خلال قرصٍ، أو قرصٍ مضغوط (CD)، أو شريطٍ، أو محرك أقراصٍ ثابتٍ خارجيّ، أو أي وسيطٍ آخرٍ معروف.
5. يجب توفير مرافق نسخٍ احتياطيٍّ كافية لضمان إمكانية استعادة جميع معلومات الأعمال والبرامج الأساسية بعد وقوع كارثةٍ أو فشل الوسائط. سيساعد الفحص الكامل لأصول الهيئة المحلية في اكتشاف الثغرات، ويجب تضمينه في خطة تكنولوجيا المعلومات والاتصالات (# سنوات) على النحو المنصوص عليه في سياسة شراء أصول تكنولوجيا المعلومات.
6. يجب تسجيل وسائط النّسخ الاحتياطي التي يمكن نقلها من غرفة الخادم إلى موقع التخزين خارج الموقع.
7. يجب أن يحتوي سجل وسائط النسخ الاحتياطي في الموقع على المعلومات التالية:

أ. تاريخ أخذ النّسخة الاحتياطيّة.
ب. تاريخ نقل الوسائط إلى موقع التخزين خارج الموقع.
ت. محتويات الوسائط، مثل: (النّسخ الاحتياطي للمعاملات، والنسخ الاحتياطي للتطبيق، والنسخ الاحتياطي للنظام بالكامل)
ث. طبيعة النّسخ الاحتياطي (مثل نسخ الملفات أو نسخ الصور الكامل).
ج. اسم الناقل.
ح. اسم موقع التخزين خارج الموقع
خ. اسم الشخص المسؤول في المكان داخل الموقع وتوقيعه.
د. أيّ معلومات تسميةٍ أخرى.

8. يجب عمل نسختين على الأقل من الإصدارات القابلة للاسترداد بالكامل لجميع البيانات المهمة. ويجب تخزين نسخة واحدة في غرفة الخادم، وتخزين النسخة الأخرى في موقع تخزينٍ خارج الموقع.
9. يجب إعطاء النسخ الاحتياطي للبيانات مستوى مناسب للحماية البيئية متوافقة مع المقاييس التي تمّ اتخاذها لحماية الخادم.
10. يجب اتباع سياسة الوصول إلى النسخ الاحتياطية بناءً على تصنيف البيانات ودور المستخدم ووظيفته.

7.2.5 تكرار النسخ الاحتياطي

يجب نسخ جميع البيانات والبرامج احتياطيّاً بانتظامٍ وفقاً لجدولٍ زمنيٍّ مُعتمد للنسخ الاحتياطي (يدويًا أو آليًا) استناداً إلى الأسلوبين المتزايد وإلغاء التكرار. يُرجى الرجوع إلى الملحق المرفق للحصول على مثالٍ على جدولٍ زمنيٍّ للنّسخ الاحتياطيّ.

7.2.6 الجدول الزمني للنسخ الاحتياطي:

1. يجب تشغيل نسخ احتياطي كامل كل أسبوعٍ، ويجب تخزينه خارج الموقع.
2. يجب إجراء النسخ الاحتياطي الجزئي/المتزايد يومياً.

3. يجب اختبار ترتيبات النّسخ الاحتياطيّ للأنظمة الفرديّة والبيانات ذات الصّلة وفقاً لجدولٍ زمنيٍّ رسميٍّ للتّأكد من أنها تُلبّي متطلبات خطة الاستعادة من الكوارث الخاصة بالهيئة المحلية.
4. تستطيع الدّائرة أن تقرر أخذ صورٍ كاملة للخوادم كنسخةٍ احتياطيةٍ لضمان إمكانيّة استرداد النّظام بأقلّ قدرٍ من المعرفة بتكوين النظام، علاوةً على ذلك يمكن بسهولةٍ توحيد حلّ النّسخ الاحتياطيّ ووسيط النّسخ الاحتياطي لهذا الخيار عبر جميع المواقع.

فيما يلي سياسةٌ مقترحةٌ يمكن لدائرة تكنولوجيا المعلومات والاتصالات اتباعها (والتي يمكن تعديلها لإنشاء نموذجٍ يناسب بشكلٍ أفضل أنواع النسخ الاحتياطية التي يستخدمونها حاليّاً، أو يرغبون في استخدامها):

	شهريّاً	أسبوعيّاً	متزايد	عدد مرات التحقق		
الخوادم	**جميع الأقراص الصّلبة (نسخ احتياطي كامل)**		**عدد المرات اليوميّة**	**أسبوعيّاً (الجمعة)**	**التحقق الثاني - السبت**	**التحقق الثالث - الأحد**
وحدة تحكم المجال الأساسية (PDC)	D ، C					
وحدة تحكم مجال النسخ الاحتياطي (BDC)	C					
خادم - MIS	C					
نظام إدارة المستندات الإلكتروني (EDMS)	C					
Exchange	C					

7.2.7 إجراءات النسخ الاحتياطي الآلي واليدوي

يجب أن يفاضل مسؤول/ فريق تكنولوجيا المعلومات والاتصالات بين إجراءات النّسخ الاحتياطيّ الآلي و إجراءات النّسخ الاحتياطيّ اليدوي بناءً على المتطلبات والقيود الخاصّة بهم. يتماشى كلا الإجراءين مع أفضل الممارسات، غير أنَّ النّسخ الاحتياطيّ اليدويّ يعتمد بشكلٍ كبير على الموارد البشرية المُعرَّضةً للأخطاء البشرية، على عكس النّسخ الاحتياطيّ الآلي الذي يمكن جدولته وهذا ما تنصح به هذه السّياسة.

7.2.8 استعادة اختبارات البيانات

1) وفقاً لما هو منصوصٌ عليه في سياسة التعافي من الكوارث، يجب على طاقم التّشغيل اختبار أشرطة النّسخ الاحتياطيّ/الأرشيف بانتظام للتأكد من إمكانية قراءة الأشرطة والاعتماد عليها للاستخدام في حالات الطوارئ عند الضرورة. إذا كانت الإجراءات العاديّة لا تستخدم أشرطة النسخ الاحتياطي لإجراء عمليات الاستعادة بشكل منتظمٍ تماماً، فيجب إجراء الاختبارات العشوائيّة الرّوتينيّة أسبوعيّاً على الأقل.
2) يجب اختبار استعادة النّسخ الاحتياطيّ عند إجراء أيّ تغيير قد يؤثر على نظام النّسخ الاحتياطيّ. سيتم مراجعة معلومات سجل الأحداث النّاتجة من كلّ مهمة نسخ احتياطي يومياً للأغراض التالية:
   أ. للتحقق من الأخطاء وتصحيحها.

ب. لمراقبة مدة عملية النسخ الاحتياطي.
ت. لتحسين أداء النسخ الاحتياطي حيثما أمكن ذلك.

7.2.9 الاحتفاظ بالنُسخ الاحتياطية

1) يجب الاحتفاظ بنسخ احتياطيّة لجميع البيانات بحيث يمكن استعادة جميع الأنظمة بالكامل، وكحدٍّ أدنى يجب الاحتفاظ بنسخةٍ احتياطيّةٍ سنويّةٍ لمدة 5 سنوات على الأقل (حسب إمكانات الهيئة المحلية).
2) يجب أنْ تظهر جميع بيانات النّسخ الاحتياطيّ الأرشيفيّة المُخزَّنة خارج الموقع في دليلٍ محدّثٍ يعرض تاريخ آخر تعديلٍ للمعلومات بالإضافة إلى طبيعة المعلومات.
3) يجب ألا تتعرض جميع الوسائط المخزنة لفتراتٍ تزيد عن ستة (6) أشهر لانخفاض الأداء السّريع.

7.2.9.1 وثائق النسخ الاحتياطي

1) يجب أنْ تتضمن وثائق النّسخ الاحتياطيّ تحديداً لجميع البيانات والبرامج والوثائق وعناصر الدّعم المهمّة التي قد تكون ضروريةً لأداء المهام الأساسية خلال فترة الاستعادة.
2) يجب تسميّة كلَّ وسيطِ نسخٍ احتياطيٍّ بشكلٍ مناسب مع تفاصيل تحدد معايير النسخ الاحتياطي وتاريخه وطبيعته، مثل: (النسخ المتزايد، أو نسخ الصورة الكامل)، بالإضافة إلى ذلك يجب وضع بطاقة تصنيف للوسيط؛ وذلك على النّحو الذي تحدده الهيئة المحليّة . فيما يلي الحد الأدنى من معايير تحديد وسائط النسخ الاحتياطي:
   أ. اسم الخادم.
   ب. وصف المحتويات.
   ت. تاريخ الإنشاء.
   ث. تصنيف الحساسيّة (بناءً على لوائح الاحتفاظ بالسّجلات الإلكترونيّة المعمول بها).
   ج. معلومات الاتصال بالهيئة المحليّة.
3) يجب مراجعة وثائق النّسخ الاحتياطيّ والاستعادة وتحديثها بانتظامٍ لمواكبة التكنولوجيا الجديدة وتغييرات الأعمال وترحيل التّطبيقات إلى الأنظمة الأساسيّة البديلة.
4) يجب التّخلص بشكلٍ آمن من وسائط النّسخ الاحتياطيّ التي لم تعد قيد الاستخدام، ممّا يجعل البيانات الموجودة عليها غير قابلةٍ للقراءة.
5) يجب مراعاة إمكانيّة الوصول إلى الوسائط في المستقبل في وقتٍ تتغير فيه التكنولوجيا، فضلاً عن احتمال تلف الوسائط المُستخدمة لتخزين السجّلات.
6) يجب إعطاء البيانات المخزنة الاحتياطيّة مستوى مناسباً من الحماية الماديّة والبيئيّة بما يتوافق مع المعايير المُطبَّقة في غرفة الخادم.

7.3 مقاييس أساسية

1) يجب تحديث خطّة البيانات للأنظمة والعمليات.
2) يجب تشفير جميع البيانات الحسّاسة.
3) يجب أن تستخدم البنية الأساسيّة للتخزين آليات الحماية من جميع التهديدات المحتملة مثل:
   أ. التلف والتّعديل غير المصرَّح به بشكلٍ عرضيٍّ أو متعمد.
   ب. تدمير البيانات أو تلف أو فقد أجهزة الكمبيوتر ومحركات الأقراص الثّابتة.
   ت. الحذف العرضي للملفات أو محركات أقراص التّنسيق.
4) ينبغي أن يكون بمقدور الطّرف الثّالث – في حال التّعاقد معهم لتوفير حلول سحابية على سبيل المثال - توفير خدمات دعم على مدار 24 ساعة طوال أيام الأسبوع؛ للاستجابة في حالة وقوع حوادث خارج أوقات العمل العادية.

5) ينبغي استخدام ضوابط الوصول المناسبة لمنع الوصول غير المصرَّح به إلى البيانات الحسّاسة المخزنة في بيئة سحابية للطّرف الثّالث، بما في ذلك موظفي موفر خدمة السّحابة (انظر خطط الوصول التفصيلية في سياسة إدارة المورد وسياسة أمن تكنولوجيا المعلومات).
6) يجب اتباع سياسة الوصول إلى النّسخ الاحتياطية بناءً على تصنيف البيانات ودور المستخدم ووظيفته.

7.4 سياسات ذات علاقة

1. سياسة شراء الأصول.
2. سياسة التّعافي من الكوارث.
3. سياسة إدارة المخاطر.

8. سياسة امن المعلومات

8.1 المقدمة والأهداف

8.1.1 مقدمة

يجب أنْ تكون التّدابير الأمنية مُصممةً بشكلٍ يتناسب مع جميع الخدمات المقدَّمة للمواطنين من قِبل الهيئة المحليّة، ومن الأهمية بمكان أنْ ينظر المجلس البلدي إلى هذه التّدابير الأمنيّة من زاويةٍ استراتيجيةٍ، وكجزءٍ مهمّ يساعد في تطوير أداء الهيئة المحليّة وتحسين الخدمات وكمركز ربحٍ وليس فقط كعبءٍ ماليّ أو مركز تكلفه. في هذه السّياسة ننصح بشدّة عدم النّظر إلى مستوى الأمان المنشود باعتباره نموذجاً واحداً يناسب الجميع؛ وذلك لاعتباراتٍ تتعلق بقدرة الهيئة المحلية على التّطوير ومدى الاحتياجات المطلوبة من الهيئة المحلية والقدرات الإدارية، ولكننا نؤكد أنَّه بغضِّ النّظر عن حجم القدرات في الهيئة المحلية إلّا أنَّه من الضروري التّعامل مع الأمن الرّقميّ بشكلٍ شامل كمجال سياسة واحدة على النّحو المنصوص عليه في هذه السّياسة وكذلك في السّياسات التّالية ذات الصّلة: **سياسة إدارة التغيير**، **سياسة شراء أصول تكنولوجيا المعلومات** ، **سياسة كلمة المرور** ، **سياسة النّسخ الاحتياطيّ** ، **سياسة تقييم المخاطر**.

8.1.2 بيان السياسة

تعتبر موارد نظام الكمبيوتر والبيانات المرتبطة بها من الأصول (الممتلكات) الهيئة المحلية المهمّة والضرورية لتنفيذ أعمالها. ينبغي اتخاذ تدابير كافية لضمان أنَّ جميع معلومات الهيئة المحليّة بأمانٍ تامّ بجميع الأوقات، وبالتالي تمَّ وضع السّياسات والمعايير والإجراءات والمبادئ التّوجيهية لمعالجة الضّمانات الإدارية والفنيّة والماديّة من أجل:

1. ضمان أمن وسريّة سجلات ومعلومات المواطنين / الأشخاص.
2. الحماية من أي تهديدات أو مخاطر متوَّقعة على أمن أو سلامة هذه السجلات.
3. الحماية من الوصول غير المصرَّح به إلى هذه السّجلات أو المعلومات أو استخدامها مما قد يؤدي إلى ضررٍ كبيرٍ أو إزعاجٍ لأيّ مواطن.

8.1.3 المجال

تنطبق هذه السّياسة على جميع موظفي الهيئةِ المحليّةِ ومقدمي الخدمات والبائعين والوكلاء سواءً الذين لديهم جهاز كمبيوتر مملوك للهيئة أو مملوك بشكلٍ شخصيّ أو محطة عمل مستخدمة للاتصال بشبكة الهيئة المحليّة، وكذلك اتصالات الوصول عن بعد المستخدمة للقيام بالعمل نيابةً عن الهيئة المحليّة بما في ذلك قراءة أو إرسال رسالة بالبريد الإلكتروني وعرض مواد على مواقع التواصل الاجتماعي أو الويب وبالتالي **تغطي هذه السياسة:**

1. موظفي الهيئة المحليّة بدوامٍ كامل وبدوام جزئيّ.
2. المتطوعين المرخص لهم باستخدام موارد الهيئة المحلية للوصول إلى الإنترنت.
3. متعاقدي الهيئةِ المحليّةِ المرخص لهم باستخدام المعدات والمرافق التّابعة للهيئة.

8.1.4 الهدف

ضمان سريّة وسلامة وتوافر جميع المعلومات "الرقمية" التي تم إنشاءها واستلامها ونقلها وتخزينها من قبل مرافق الاتصالات وتكنولوجيا المعلومات الإلكترونية التابعة للهيئة بشكل أفضل من خلال دمج حوكمة الأمن الرقمي ضمن ممارسات إدارة المخاطر العامة بالهيئة المحلية على النحو المنصوص عليه في **سياسة تقييم المخاطر وسياسة النسخ الاحتياطي**.

8.1.5 المسؤوليات

تهدف الإرشادات الواردة أدناه إلى مساعدة المستخدمين على تحقيق أقصى استفادة من موارد دائرة تكنولوجيا المعلومات المتاحة لهم ضمن الإجراءات التالية:

1) يقوم مسؤول الدّائرة بتعيين شخص\ أشخاص بتولي مسؤولية الأمن ومتابعة شؤونها والحوادث المرتبطة.
2) يتّحمل المستخدمون المسؤولية الفردية عن حماية البيانات والمعلومات التي يتعاملون معها.
3) عندما يكون الموظفون غير متأكدين من حساسية المعلومات، يجب الاتصال برئيس القسم للحصول على المساعدة.
4) يجب على المستخدمين الإبلاغ فوراً عن أيّ شيءٍ غير معتاد بشأن البيانات أو المعلومات الموجودة على أجهزة الكمبيوتر الخاصة بهم إلى رئيس القسم.
5) التّصدي لأيّ شخصٍ يبدو أنّه غريب ومتواجد في منطقة العمل لتحديد الغرض من وجودهم، أو إبلاغ فوراً مسؤول المكان أو الأمن للتعامل مع الحالة.
6) يجب حماية المعدّات من السّرقة والاحتفاظ بها بعيداً عن الأطعمة والمشروبات.
7) من الأفضل تخزين البيانات على محرك أقراص الشّبكة (وليس محرك الأقراص المحلي)؛ لضمان نسخ البيانات احتياطيّاً بانتظامٍ كما هو منصوصٌ عليه في **سياسة النّسخ الاحتياطيّ**. في حالة قيام الهيئة المحليّة باختيار حلّ "سحابي" خارجي، فيجب مراجعة **سياسة إدارة موردي خدمات تكنولوجيا المعلومات** و **سياسة خدمات الاستعانة بمصادر خارجية لتكنولوجيا المعلومات** .
8) يقوم مسؤولي الأقسام فورا باعلام دائرة تكنولوجيا المعلومات بإلغاء حق الوصول للمعلومات في حال ترك الموظف وظيفته، او في حال انتهاء التعاقد مع الجهة الخارجية او في حالة حصل تغيير لا يتطلب الوصول الى البيانات او لاي سبب أخر مشروع.

8.1.6 ملكية المعلومات

جميع المعلومات التي يتمّ الحصول عليها من قِبل الموظفين أو الاستشاريين في أيّ مشروعٍ تابعٍ للهيئة هي ملك للهيئة ويجب أنْ تكون محميّة من قِبل الهيئة المحليّة وفقاً للتصنيف الخاصّ بالبيانات .

8.2 السياسات والإجراءات

8.2.1 السياسات

من أجل تجنُّب سيناريوهات الخسارة العَرَضية للمعلومات وتخفيف المخاطر المعلنة (بناءً على سياسة تحديد المخاطر) يعتبر رفع وعي المستخدمين بالهيئة المحلية (أي كان موقعهم الوظيفي) أمرٌ أساسي لإنفاذ هذه السّياسة المتعلقة بأمن المعلومات، و تستند المكونات الأساسيّة على:

8.2.1.1 تصنيف البيانات

لا تتطلب جميع المعلومات المتوفرة لدى الهيئة المحليّة نفس مستوى الحماية وبالتّالي يجب أنْ يكون مستوى الحماية المطَّبق على المعلومات مناسباً لتصنيفها لضمان التّعامل والكشف المناسبين. بعد تحديد جميع المعلومات، ومدى احتياج المعرفة لأداء العمل يتم تصنيفها إلى **العامة أو للاستخدام الدّاخلي فقط أو سرية**.

أ. التصنيف العام

المعلومات متاحة للجمهور ومن المحتمل أن تكون موجودة على الإنترنت. أمثلة على المعلومات العامة هي البيانات الصحفية، ومن الجدير بالذّكر أنّه لا تتطلب المعلومات العامة أي معالجة خاصة أو تحديدها بعلامات.

ب. التصنيف الداخلي

المعلومات التي تكون مخصصة للتوزيع الدّاخلي بالهيئة المحليّة بسبب حساسية الأعمال أو محتواها التّقني تأخذ التصنيف "الدّاخلي"، ومن الأمثلة على المعلومات الدّاخلية هي كتيبات الموظفين، والإدارة الرّوتينيّة لمعلومات المكتب، والمخططات التنظيمية ، والسّياسة والمعايير. يجب وضع علامة على جميع المعلومات "الدّاخلية" التي تتم مشاركتها مع الآخرين "للاستخدام الدّاخلي للهيئة فقط" ويتم التّعامل مع المعلومات التي لم يتم تصنيفها على أنّها "استخدام داخليّ فقط".

ت. وسم مستندات الاستخدام الداخلي

يجب وضع علامة التّصنيف المناسب على أيّ مستندٍ أو تقرير تم إنشاؤه بواسطة موظف، أو جهاتٍ خارجية يحتوي على معلومات غير عامّة. يجب تحديد التّصنيف بوضوح باستخدام التمييز، أو الكتابة بالخط العريض، أو العلامات لزيادة الرؤية على سبيل المثال:

() اسم الهيئة المحليّة - الاستخدام الدّاخلي فقط.
() اسم الهيئة المحليّة – سرّي.

ت. التصنيف السري

تعتبر المعلومات التي قد يكون لإفشائها أو إتلافها أو "إتلافها غير المصرَّح به" تأثير سلبي على عمل الهيئة المحليّة أو سمعتها أو المواطنين أو موظفيها، أو تعرض الهيئة المحليّة لخسارة ماليّة **معلومات سرية**. أمثلة على المعلومات السّريّة هي أرقام حسابات المواطنين أو قوائم ومتطلبات المواطنين، وبيانات الكمبيوتر، ومعلومات الموظفين أو خطط الهيئة المحلية ، والميزانيات المُخطط لها، وسجلّات الموظفين، وتكوينات النّظام، وعناوين الشبكة. إنَّ عدم تعيين معلومات معينة على أنَّها سريّة و / أو خاصّة بالهيئة المحليّة لا يمنع أي مطالبة لاحقة من قِبل الهيئة المحليّة بأنّ هذه المعلومات سريّة ومملوكة لها. يتضمن ذلك المعلومات التي تم إنشاؤها خارج مباني الهيئة المحليّة إذا كانت المعلومات جزءاً من أنشطة الهيئة المحليّة . يجب حماية المعلومات السريّة ونسخها احتياطيّاً على النّحو المنصوص عليه في **نهج النسخ الاحتياطي**، وبالتالي يتطلب معالجة خاصّة ووسمها بالعلامات على النّحو الموضح أدناه.

ث. وسم المستندات والوسائط السرية

يجب وسم جميع المستندات التي تعتبر " **سريّة**" بإضافة بيانات الرّقابة المناسبة المتمثلة ببيانات التّحكم إلى كل صفحة (رأس أو تذييل) جنباً إلى جنب مع فئة التّصنيف (على سبيل المثال: سرّي).
يجب تمييز البيانات بوضوح باستخدام الكتابة بالخط العريض أو العلامات لزيادة وضوحها. أمثلة على بيانات التحكم هي:

1. (.....) سري للهيئة - يحظر التعديل أو الاستنساخ.
2. (.....) سري للهيئة - ليس للتوزيع.

يجب تصنيف جميع الوسائط الإلكترونيّة (أقراص DVD ، والأقراص المدمجة، والأشرطة، والأقراص المرنة، وما إلى ذلك) على خارج الجاهز لتحديد المحتويات وتجنُّب سوء التّعامل معها، أما الوسائط التي تحوي معلومات سريّة فيجب وضع ملصق خارجي عليها يوضح تصنيف المعلومات ويجب تخزينها في مكانٍ آمن ماديّاً مقاوم للحريق (معتمد للوسائط) عندما لا تكون قيد الاستخدام.

8.2.1.2 إعطاء أقل الصلاحيات -بناءً على مدى الحاجة إلى المعرفة

يجب تحديد الوصول إلى البيانات على أساس مدى الحاجة إلى المعرفة، مع مراعاة تصنيف البيانات والمخاطر المحددة **(بالرجوع إلى سياسة تقييم المخاطر)**، وبالتّالي يجب منح امتيازات للموظف للوصول إلى الأنظمة المتعلقة بتكنولوجيا المعلومات والاتصالات بناءً على أقل عدد من الامتيازات المطلوبة؛ لأداء الوظيفة وما لم يكن هناك مخاطر مرتبطة بالوصول، وبالتالي تحدد هذه السّياسة متطلبات منع أيّ تسريب للبيانات بشكل عرضي وعن طريق الخطأ منْ قِبل الموظفين أو المستخدمين من خلال استعراض الضّوابط الأمنيّة التّالية:

1. التحكم بالوصول التقديري:

توصي هذه السّياسة باستخدام أسلوب التّحكم في الوصول التّقديري، وهو أحد أشكال التفويض السّائدة التي تتحكم بالوصول الأمني إلى المعلومات أو الأجهزة باستخدام قوائم التّحكم في الوصول الذي يمنح أو يقيد الوصول، بحيث يتم تحديد المستخدمين جنباً إلى جنب مع الأذونات أو الامتيازات الممنوحة لهم أو المرفوضة.

أ. يقوم "مالك" النّظام بعمل إجراءاتِ السّيطرة الخاصّة بالأجهزة تحت سيطرته ومن ضمنها الأشخاص المصرَّح لهم بالوصول.
ب. يجب أنْ تشمل قائمة التّحكم في الوصول فقط موظفي الهيئة المحليّة، وموظفي قسم تكنولوجيا المعلومات والاتصالات الذين يقومون بصيانة وإدارة قاعدة البيانات أو طرفٍ ثالث متعاقد معتمَد بشكلٍ رسميّ.
ت. يجب أنْ يكون لدى الأشخاص المصرَّح لهم فقط حقَّ الوصول إلى قواعد البيانات في الهيئة المحليّة. وسيقوم الدّعم التّقني بعمل الإجراءات التي تنزع الصّلاحيّات للوصول أو تغيرها سواء للموظفين أو للطّرفِ الثّالث.
ث. بشكلٍ عام يجب تطبيق الوصول الأكثر تقييداً على قاعدة البيانات، والسّماح بالوصول فقط على أساس الحاجة إلى المعرفة.
ج. يجب مراجعة قائمة الوصول إلى قاعدة البيانات كلّ ثلاثة أشهر للتأكد من أنّ المستخدمين المصرَّح لهم فقط قادرون على الاتصال بقاعدة البيانات أو أداء المهام المحليّة.

2. فرض قيود على الوصول من خلال:

أ. توفير الحماية الماديّة: إجراء أمني لتأمين الموقع المادي لأصول (المعدات) تكنولوجيا المعلومات والاتصالات:

1. يجب على قسم تكنولوجيا المعلومات والاتصالات، كجزءٍ من إدارة الأصول إجراء جرد مادي لمعدات الحوسَبة المكتبية على أساس سنوي مع مراعاة تحديد مواقع الأصول الحاسوبية، ووضعها في سجل خاص مع معلومات الأشخاص المصرَّح لهم بالوصول سواء الموظفين أو الطّرف الثّالث الذي يملك حقّ الوصول بشكلٍ مؤقت.
2. يجب أن تحتوي جميع المعدات الحاسوبية على أرقام تسلسلية وعلامات الملكية ومسجلة في نظام أصول الهيئة المحليّة لأغراض تحديد الهوية، أو في حالة تلف هذه المعدات أو سرقتها على النّحو المنصوص عليه في **سياسة شراء أصول تكنولوجيا المعلومات**.
3. من المتوقع أنْ يكون الموظفين على دراية بالمعدات الموجودة داخل مكاتبهم المباشرة وأن يبلِّغوا المشرفين فوراً عن المعدات المفقودة.
4. يجب على أي موظف يشتبه في أيّ شكلٍ من أشكال الخرق الأمني إبلاغ مسؤول الدّائرة بذلك، وهذا يشمل على سبيل المثال لا الحصر الدّخول غير المصرَّح به، والأبواب التي تُركت غير مغلقة، والأقفال التي لا تعمل، والأبواب التي لا تُغلق بشكلٍ صحيح أو تُركت غير مغلقة، والرّموز الأمنية التي تم الكشف عنها للأفراد غير المصرّح لهم، وفقدان مفاتيح غرفة تكنولوجيا المعلومات التي تحوي الأجهزة الأساسيّة.
5. يجب على أي شخص يلاحظ وجود أفراد مشتبه بهم أو غير معروفين في غرفة تكنولوجيا المعلومات إما أن يواجه الفرد مباشرة، أو أن يبّلغ المسؤول بالحادث.
6. يجب تفعيل خاصيّة الحماية التلقائيّة (كلمة سر شاشة التوقف المحمية، وقفل لوحة المفاتيح) في الخوادم ومحطات الحاسوب، ومحطات العمل أو الحواسيب الصّغيرة إذا لم يكن هناك أي نشاط لمدة محددة مسبقاً لمنع الوصول إلى النّظام بطريقة غير مشروعة.
7. يجب إبلاغ إدارة دائرة تكنولوجيا المعلومات والاتصالات من قِبل إدارة الموارد البشريّة عن إنهاء أو انتهاء عقود الموظفين، أو عندما لم يعد المستخدم المعين بحاجة إلى الوصول إلى النّظام من أجل الإلغاء الفوري لحساباتهم، أو صلاحياتهم.
8. أيّ حالات تؤدي إلى انتهاكات أمنية ناتجة عن عدم اتباع الموظفين للإرشادات المذكورة أعلاه يمكن اعتبارها مسألة تأديبية.

ب. التحكم بالوصول الداخلي:

1. يجب أن تستخدم الهيئة المحليّة أنظمة التّحكم في الوصول لجميع الأماكن التي تقوم بالعمليات أو تحتوي على أصول / معدات تكنولوجيا حرجة أو تحوي بيانات حسّاسة، مثل: مراكز البيانات، وغرف الكمبيوتر، وما شابه.
2. يجب أن تقوم الدّائرة بعمل قائمةٍ بالأماكن التي تقوم بالعمليات أو تحتوي على أصول / معدات تكنولوجيا وأسماء الموظفين المعتمدين للوصول إلى هذه الأماكن، بما في ذلك الموظفين والمقاولين الذين مُنحوا تصاريح مؤقتة ويجب الاحتفاظ بها في سجل.

3. سيقوم مسؤولي الخدمة بإعلام الموظفين الذين يملكون حقَّ الوصول لهذه الأماكن عن المخاطر المحتملة والإجراءات المتخذة للسّيطرة.

ج. التحكم بالوصول عن بعد:

يجب أنْ تتم الموافقة على أيّ اتصال بشبكة الهيئة المحليّة مع أي طرفٍ خارجيٍّ من قِبل قسم تكنولوجيا المعلومات والاتصالات بالهيئة المحليّة وباطلاع الإدارة العليا للهيئة. يجب التّحكم في الوصول الآمن عن بُعد بشكلٍ صارم وفقاً للمتطلبات التّالية:

1. يمنع الوصول عن بعد لشبكة الهيئة المحليّة باستخدام إجراءات تسجيل المستخدمين.
2. يجب تقديم مذكرة توضح اسم الشّخص، واسم الشركة، ومدة التّعاقد مع الهيئة المحليّة، والأسباب لطلب الوصول إلى النظام، على أن يوافق المسؤول عن الدائرة أو من ينيبه على الطلب.
3. يُمنح الوصول عن بعد على أساس مدى الحاجة للوصول ولأغراض العمل فقط ولمدة مؤقتة، وفي حال الاحتياج إلى تمديد المدة، يجب تقديم طلب جديد موضحاً الأسباب المتعلقة بالتمديد.
4. سيتم فرض التّحكم عبر مصادقة استخدام كلمة المرور لمرة واحدة. يمكنك الحصول على معلومات حول إنشاء عبارة مرور قوية بمراجعة سياسة تغيير كلمة المرور وفي هذه السّياسة.
5. يتم التّحكم بجميع حالات الوصول عن بعد عبر عدد محدود من نقاط الوصول لشبكة الهيئة المحليّة.
6. يجب تسجيل كافّة اتصالات الدّخول عن بعد، بما في ذلك عنوان برتوكول الإنترنت واسم المستخدم الخاص بالدّخول.
7. يجب على الموظفين ومقدمي الخدمات الذين يتمتعون بامتيازات الوصول عن بعد التّأكد من أنَّ أجهزة الكمبيوتر أو محطة العمل المملوكة للهيئة أو الشخصيّة والتي تكون متصلة عن بعد بشبكة الهيئة المحلية غير متصلةٍ بأيّ شبكةٍ أخرى في نفس وقت.
8. يجب توعية جميع المستخدمين بالمعايير الدّاعمة والإجراءات الأمنية ذات الصّلة.

د. التحكم بالوصول عن بعد لموردي المصادر الخارجية أو "الطرف الثالث":

بالإضافة إلى الإجراءات المنصوص عليها بخصوص الوصول عن بعد، سيتم التّحكم بالسّماح بوصول المصادر الخارجية "الطّرف الثّالث" من خلال الآتي:

1. يجب أنْ تشمل الاتفاقيات الموقعة على اتفاقية مستوى الخدمة وتُتَابع منْ قِبل مسؤول الخدمة (انظر الى سياسة إدارة موردي تكنولوجيا المعلومات).
2. سيلتزم أيّ طرفٍ ثالثٍ من مزودي الخدمات بسياسة أمن المعلومات التّابعة للهيئة ويتحمل المسؤولية عن أي تبعات ناتجة عن إساءةِ استخدام الوصول.
3. بشكلٍ عامّ لا يجب إعطاء الطّرف الثّالث إمكانية الوصول عن بعد.
4. يجب تقديم مذكرة توضح اسم الشخص، واسم الشركة، ومدة التعاقد مع الهيئة المحلية ، والأسباب لطلب الوصول إلى النظام، على أن يوافق المسؤول عن الدائرة أو من ينيبه على الطلب.
5. سيتم إصدار اسم المستخدم على أساس مؤقت وبناءً على مدى الحاجة للوصول ولأغراض العمل فقط ولمدة مؤقتة، وفي حال الاحتياج إلى تمديد المدة، يجب تقديم طلب جديد موضحاً الأسباب المتعلقة بالتمديد وإلّا سيتم تجميد الحساب فوراً.
6. سيقوم مسؤول الخدمة – من خلال الدّعم التّقني - بإعلام الدّائرة فوراً وأي أقسام أخرى بالهيئة المحليّة عند عدم احتياج الطّرف الثّالث للوصول.
7. يتأكد مسؤول الخدمة أنَّ الطّرف الثّالث مطلِّع وملتزم بسياسات الأمن التّابعة للهيئة وأنّه قد تمّ توقيعه على اتفاقيات عدم إفشاء الأسرار.

ذ. توفير الأمن المادي في بيئة العمل:

تطلب الهيئة المحليّة العمل المشترَك بين الموظفين والإدارة من أجل توفير حماية أمنية فعّالة لأصول دائرة تكنولوجيا المعلومات والاتصالات في مكان العمل، وتعتبره مسؤولية مشتركة. يتطلب سياسة الأمن كذلك التّحكم بالوصول "الشخصي أو المادي" إلى أماكن تواجد الأجهزة والبيانات "الأصول" وبالتّالي يجب ملاحظة الآتي:

1. يجب على جميع الإدارات التّأكد من توفير أجهزة إطفاء حريق كافية في منطقة المكاتب، ويجب صيانة هذه المعدات ومراجعتها على أساس سنوي من قِبل الإدارة المسؤولة.
2. يُفضَّل أنْ يكون لدى الأقسام التي تحتوي على معدات حاسوبية في الطّوابق المرتفعة أجهزة مناسبة للكشف عن الحرائق والمياه الموجودة أسفل الأرضيّة ويجب صيانة هذه الأجهزة واختبارها على أساسٍ سنويّ.
3. يجب توصيل أجهزة كمبيوتر سطح المكتب وأجهزة الكمبيوتر المحمولة ومحطات الإرساء وخوادم الملفات بأجهزة مزود الطاقة غير المنقطع "المقابس الحمراء" لمنع ارتفاعات الطّاقة وانقطاع التّيار الكهربائي والأضرار اللاحقة بالبيانات والأجهزة.
4. يجب عدم توصيل أيَّ معداتٍ أخرى غير أجهزة الكمبيوتر بمزود الطاقة ("المقابس الحمراء"). يستثنى من ذلك طابعات الليزر التي قد لا يتم توصيلها مطلقاً بمنافذ الطّاقة.
5. يجب إيقاف تشغيل جميع أجهزة الكمبيوتر غير الأساسية خارج ساعات العمل (أي ليالي الأسبوع وعطلات نهاية الأسبوع والإجازات والعطلات)، وهذا يشمل وحدات المعالجة المركزية والشّاشات والطابعات وأجهزة المودم.
6. يجب تشغيل تكييف الهواء المناسب في بيئات المكاتب التي تضم أجهزة الكمبيوتر المكتبية وموارد التكنولوجيا (الأساسية) للحيلولة دون تلفها نتيجة الحرارة على المدى الطويل وتعطّلها.
7. يجب على جميع الموظفين عدم تحميل المنافذ الكهربائية بحمل زائد بربطها بأجهزة كثيرة. كذلك يجب مراجعة الاستخدام الصحيح والعملي لأسلاك التمديد سنويّاً في بيئة المكتب.
8. يجب أنْ تظل جميع الأماكن التي تحتوي على أجهزة الكمبيوتر الشخصيّة وأجهزة سطح المكتب مغلقة عندما لا يتواجد الموظفين فيها من أجل تقليل حدوث الدّخول والوصول غير المصرَّح به.
9. يجب تأمين معدات الكمبيوتر المكتبي التي توجد في منطقة وصول عامة بقطعة أثاث أو سطح عمل باستخدام جهاز لمنع السّرقة / الأمان. يجب أيضاً تأمين أجهزة الكمبيوتر المحمولة بأجهزة منع السّرقة.
10. يتحمل مسؤول إدارة تكنولوجيا المعلومات والاتصالات أو من ينوب عنه مسؤولية ضمان متابعة حماية جميع المعدات من السّرقة أو سوء الاستخدام.
11. يجب تسجيل خروج المستخدم لجهاز الكمبيوتر بشكلٍ تلقائيّ بعد 5 دقائق من التوقف عن العمل عند التعامل مع معلومات مصنفة سرية.

8.2.1.3 استخدام إدارة التغيير

1. إنَّ سياسة إدارة التغيير يجب أن تطبق لتنفيذ أيّ طلبٍ للتغيير على أنظمة الهيئة المحليّة ومن ضمنها الرّقع الأمنية المُوصَّى بها من مزودي منتجات أنظمة المعلومات.
2. يجب فحص أيّ تحديثات لتصحيح البرامج قبل التنفيذ، ويجب تنفيذها من قِبل مزودي منتجات أنظمة المعلومات "الطّرف الثّالث" المعين وفقاً للعقود الموقعة.
3. في حال الحاجة إلى استخدام وسيلة الوصول عن بعد للتنفيذ، تطبق الإجراءات آنفة الذّكر.

8.2.1.4 فصل المهمات

لا ينبغي لفردٍ واحدٍ أنْ يتحكم في العمليات الحرجة و\ أو التشغيليّة المتعلقة بتكنولوجيا المعلومات بأكملها، بالتّالي يجب على إدارة تكنولوجيا المعلومات والاتصالات تحديد أدواروظيفيّة لأنظمة تكنولوجيا المعلومات ذات الصّلة الخاصّة بهم. وبمجرد تحديد هذه الوظائف يجب تنفيذ فصل الواجبات المتعلقة بوظائف تكنولوجيا المعلومات الحرجة / التشغيلية إلى وظائف متميزة لتنفيذها منْ قِبل أكثر من شخص وبالتّالي منع شخص واحد من إلحاق الضرر بنظام التّطوير أو التّشغيل أو الخدمات التي يقدمها، سواء كان ذلك بفعل عرضي أو إهمال أو فعل متعمد . يجب إدراج الأدوار المحددة (وتنفيذ فصل الواجبات) في خطّة الأمان الخاصّة بنظام المعلومات المعين.

8.2.1.5 التدقيق الأمني

1. يجب اختبار أنظمة تكنولوجيا المعلومات التي تستضيفها وتصونها الهيئة المحليّة بشكلٍ دوريّ لمعرفة نقاط الضّعف والعيوب الأمنية المعروفة.
2. يجب اختبار التّطبيقات التي تستضيفها وتحتفظ بها جهات خارجية، مثل أنظمة "برامج الشبكات(SAAs) "، مرة واحدة على الأقل سنوياً .
3. يجب على الموردين تقديم دليل إثبات على إجراء الاختبار قبل تحميل بيانات الهيئة المحليّة أو إدخالها في التّطبيق.

8.2.2 اتفاقية عدم الإفشاء عن الأسرار

1. يجب على جميع الأطراف الخارجيّة التي ستتمتع بإمكانية الوصول إلى البيانات السريّة التّوقيع على اتفاقية عدم إفشاء السريّة الخاصّة التّابعة لقسم تكنولوجيا المعلومات والاتصالات بالهيئة المحليّة وبالقوانين الفلسطينيّة ذات الشأن، كذلك يجب على الموظفين التّابعين للطّرف الثّالث الذين سيصلون إلى البيانات السريّة التّوقيع على الاتفاقية أيضاً.
2. تقع على عاتق المشرف الإداري مسؤولية ضمان توقيع الاتفاقية قبلَ أيّ عمل يتم تنفيذه أو الإفراج عن أيّ **معلومات سريّة** خاصّة بالهيئة المحليّة.

8.2.3 التّخلص الآمن من البيانات

عند إتلاف المستندات الورقية "السريّة"، يجب أن يتم إتلافها إما عن طريق تمزيق المستند بشكلٍ آليّ أو وضعه في سلة قمامة مغلقة لحين الإتلاف النهائي. يجب أن تكون جميع مراكز خدمة الهيئة المحليّة التي تتلقى نماذج مكتوبة مجهزة بهذا النّوع من الآلات.

8.2.4 أمن الوسائط القابلة للإزالة

يجب تخزين جميع أشرطة النّسخ الاحتياطيّ للبيانات في مكانٍ آمن ذو قدرة على تخزين الوسائط المغناطيسية والاستخدام التشغيلي لمعدات الكمبيوتر على النّحو المنصوص عليه في **نهج النسخ الاحتياطي**. إذا لم يكن ذلك ممكناً، فيجب إتاحة الوقت لوسائط النّسخ الاحتياطيّ لإعادة التّكيُّف مع ظروف التّشغيل قبل الاستخدام.

8.2.5 التخزين خارج الموقع

حُددت "**سياسة النسخ الاحتياطي**" بوجوب تسجيل الدّخول والخروج لجميع وسائط النسخ الاحتياطي المأخوذة إلى خارج الموقع لضمان إمكانية تحديد موقع جميع نسخ البيانات إذا لزم الأمر، وإمكانية تدقيق المستودعات خارج الموقع.

8.2.6 وسائط نقل

يمكن أنْ تكون وسائط الكمبيوتر عُرضةً للوصول غير المصرَّح به، أو سوء الاستخدام، أو الفساد أثناء نقلها، وبالتالي يجب تطبيق الضّوابط التّالية على الوسائط التي تنتقل بين المواقع:

1. يجب تشفير المعلومات والمحتويات الموجودة بالوسائط مع وجوب الاحتفاظ بمفتاح التشفير في مكان آمن تحت سيطرة مدير الهيئة المحليّة.
2. يجب استخدام وسائل نقل أو سُعاة موثوق بهم كموظف بالهيئة المحلية مصرح له.
3. يجب أن تكون الحاويات التي يتم النَّقل بها كافية لحماية المحتويات من أي ضرر مادي يُحتمل أن ينشأ أثناء النقل ووفقاً لمواصفات الشّركات المُصنّعة.
4. يجب الاحتفاظ بالوسائط في حاويات آمنة وعبوات مانعة للعبث تكشف عن أي محاولة للاختراق.

8.2.7 التخلص من الوسائط الإلكترونية

1. يجب تدمير الأقراص المرنة، والأقراص المضغوطة، ومحركات الأقراص القابلة للإزالة، ومحركات الأقراص الثابتة، وجميع أشكال وسائط الأشرطة من خلال عملية تضمن عدم إمكانية استعادة البيانات في نهاية عملية التّدمير وقبل التّخلص منها للتأكد من أنَّ المعلومات ليست كذلك مقروءة، بالإضافة إلى ذلك يجب التّخلص من جميع الوسائط وأجهزة التّخزين التي يتَّعذر محوها بشكلٍ آمن في حاوية تمزيق وسائط متخصصة.
2. يجب محو الأقراص الصّلبة في الخوادم وأجهزة الكمبيوتر التي يتعين إزالتها سواء للاستبدال أو الصّيانة بواسطة الدّائرة أو من خلال" طرفٍ ثالث" مع التّأكد بالتزام الطرف الثّالث ببنود السّريّة الصّارمة في عقودهم.

3. يجب الاحتفاظ بسجلٍ للتخلص من معدات تكنولوجيا المعلومات والوسائط، بحيث يشير السّجل إلى الخطوات التي تم اتخاذها لضمان الالتزام بالإرشادات الواردة في هذه السيّاسة بما في ذلك إزالة جميع البرامج المرخصة والتّفويض بهذا التّخلص.

8.2.8 تخزين المعلومات على المجلدات الشخصية

يستطيع الموظف حفظ المعلومات المصنّفة "سريّة" بمجلداتٍ مخصصةٍ له أو على مجلدات أخرى محددة على خادم قسم تكنولوجيا المعلومات بالهيئة المحليّة الموجود في غرفة آمنة، ويُمنع تخزين المعلومات السريّة على محرك الأقراص المحلي للجهاز المستخدم، وبالنّسبة لأجهزة الكمبيوتر المحمولة يجب تشفير المعلومات "السريّة" المخزنة على محرك الأقراص المحلي باستخدام البرامج التي تم تهيئتها وإدارتها بواسطة قسم تكنولوجيا المعلومات في الهيئة المحلية، ومع ذلك لا ينبغي تخزين البيانات "السريّة" على جهاز كمبيوتر محمول إلا في الحالات الاستثنائية الضروريّة المقرة من إدارة الهيئة المحليّة .

8.2.9 خطة إلغاء تعديلات العمليات

يتوجب وضع خطة "التراجع عن التّعديلات" كجزء من أي خطة طوارئ يتم وضعها لحماية البيانات بحيث يتمّ الالتزام بقائمة بالإجراءات التي تمّ إنشاؤها قبل عملية تكامل البرامج أو النظام وتتضمن هذه القائمة خطوات وأساليب تفصيليّة لإلغاء تثبيت نظام جديد أو إلغاء تكامله، بالإضافة إلى عكس تغييرات العملية. أرجو التحقق من **سياسة إدارة التغيير** للمزيد من المعلومات.

8.3 أمن كلمة المرور

تعد كلمات المرور جانباً مهماً من جوانب أمان الكمبيوتر والخط الأمامي لحماية حسابات المستخدمين. قد تؤدي كلمة المرور المختارة بشكلٍ سيء إلى تعريض الشّبكة التّابعة للهيئة للخطر، على هذا النّحو فإنَّ جميع الموظفين (بما في ذلك مزودي الخدمة والبائعين الذين لديهم إمكانية الوصول إلى أنظمة الهيئة المحلية) مسؤولون عن اتخاذ الخطوات المناسبة لاختيار وتأمين كلمات المرور الخاصّة بهم كما هو موضح أدناه (يرجى مراجعة **سياسة تغيير كلمة المرور)**

أ. فرض كلمة مرور قوية:

1. يجب التّعامل مع جميع كلمات المرور على أنّها بيانات سريّة.
2. يجب اختيار كلمة المرور التي يصعب التكهُّن بها.
3. يجب أن تتكون كل كلمة مرور من ثمان (8) خانات على الأقل.
4. يجب أن تكون كلمات المرور أبجدية رقمية، أي يجب أن تشتمل على أحرف وأرقام.
5. يجب أن تستخدم كلمات المرور توليفة من الأحرف الكبيرة والصغيرة، مع وجود أرقام وعلامات ترقيم متناثرة في كل مكان قدر الإمكان. ولا يكفي استخدام رقم في بداية كلمة المرور أو نهايتها.
6. يجب عدم استخدام الأسماء أو الكلمات: كلمات المرور القوية هي مزيج عشوائي من الأرقام، والحروف، وعلامات الترقيم.
7. لا يجب استخدام اسم المستخدم في كلمة السر.
8. لا يجوز استخدام أرقاماً أو حروف متكررة مثل (333 أو AAA) ، أو أرقام أو حروف متتابعة مثل (1124) أو (d c b a).
9. يجب على المستخدمين تغيير كلمات المرور للشّبكة بحدٍّ أقصى تسعون (90) يوماً (منذ آخر تغيير لكلمة المرور).
10. يجب تغيير كلمات مرور مسؤول الشّبكة (Root/Administrator) كل ثلاثين (30) يوماً، ويجب تغيير كلمة المرورللأجهزة المحليّة كل مائة وثمانون (180) يوماً.
11. يجب إعادة تعيين كلمات مرور حساب الخدمة مرة واحدة سنويّاً أثناء الصّيانة.
12. يجب الاحتفاظ بتاريخ كلمة المرور: يجب أن تكون كلمات المرور المنشأة حديثاً مختلفة عن كلمات المرور العشر السّابقة المستخدمة.
13. يجب تغيير جميع كلمات المرور الأولية لأي نظام من نظم المعلومات التّابعة للهيئة عند تشغيله واستخدامه لأول مرة بشكلٍ رسمي ويجب فرض مدة انتهاء لصلاحيتها ثلاثة (3) أيام لإجبار المستخدم على تغييرها.

14. استخدم المصادقة متعددة العوامل لإعادة تعيين كلمات المرور إذا كان ذلك ممكناً، مثل إرسال رسالة نصية إلى مستخدم الهاتف المحمول المرتبط بالحساب.
15. يجب تغيير كلمات المرور فوراً إذا حصل اشتباه بأنّها اختُرقت، أو كإجراء احتياطي عند الكشف عنها لفنيين يقومون بأعمال الصّيانة والدّعم.
16. يجب منع الولوج للأنظمة الدّاخلية والخاصّة بعد 3 محاولات خاطئة خلال مدة زمنية لا تتجاوز 14 دقيقة ويستمر المنع لمدة أقلها 30 دقيقة وأكثرها 3 ساعات.
17. سيتم حذف الحسابات المعطلة التي تزيد مدتها عن ستين (60) يوماً.
18. لا يجب السّماح للتطبيقات بإعطاء تذكير أو لمحه عن كلمة المرور السّرية.
19. يجب إعطاء كلمات المرور المؤقتة للمستخدمين بطريقة آمنه بحيث يجب تجنب نقلها على ورقة مكشوفة أو عن طريق أطراف ثالثة أو عن طريق البريد الإلكتروني غير المحميّة (النص الواضح).
20. وضع إجراءات للتّحقق من هوية المستخدم قبل تقديم كلمة مرور جديدة، أو بديلة، أو مؤقتة.

ب. تخزين كلمة المرور:

1. لحماية كلمات مرور المستخدمين عند تخزينها يتم حفظ كلمات السرّ على شكل نص مشفر لا يمكن فكه أو استخدامه إلا من الشخص المخول.
2. كلمات المرور للأنظمة (جذر النظام/مسؤول النظام Root/Administrator) يجب أن تخزن باستعمال برمجيات حفظ كلمات المرور بطريقة مشفرة.
3. يجب ضمان عدم تفعيل خاصيّة حفظ كلمة المرور في المتصفح وإدخال البيانات في كل مرة من جديد.

يحظر الأفعال التالية :

1. الكشف عن كلمة المرور عبر الهاتف لأيّ شخص.
2. الكشف عن كلمة المرور في رسالة بريد إلكتروني.
3. التحدث عن كلمة المرور أمام الآخرين.
4. أي تلميح حول تنسيق كلمة المرور (على سبيل المثال ، "اسم عائلتي").
5. الكشف عن كلمة المرور في الاستبيانات أو نماذج الأمان.
6. مشاركة كلمة المرور مع أفراد الأسرة.
7. الكشف عن كلمة السر لزملاء العمل أثناء الإجازة.

ج. يجب أن يُطلب من المستخدمين التّوقيع على بيان للحفاظ على سريّة كلمات المرور الشخصيّة، ويمكن تضمين هذا البيان في شروط التوظيف.

8.4 جدار الحماية

يتوجب على إدارة تكنولوجيا المعلومات والاتصالات استخدام جدار حماية لمنع وحظر الوصول غير المصرَّح به إلى أنظمة الهيئة المحليّة، وينبغي بهذه الحالة الإبقاء على جميع التّراخيص المرتبطة فعّالة وصالحة طوال الوقت.

8.5 تدابير مكافحة الفيروسات

1. يجب أنْ تحتوي جميع خوادم الهيئة المحلية وأجهزة الكمبيوتر المحمولة وغير المحمولة على تطبيق مضاد للفيروسات مثبَّت لفحص أجهزة الكمبيوتر والوسائط بحثاً عن البرامج الضّارة.
2. يجب أنْ تعمل برامج مكافحة الفيروسات في جميع الأوقات عندما يستخدم الكمبيوتر أي موارد موجودة على شبكة تابعة للهيئة.
3. يجب تهيئة البرنامج لعمل تحديثات يومية تلقائيّاً.
4. يجب فحص جميع رسائل البريد الإلكتروني بحثاً عن المرفقات الضّارة.
5. يجب فحص جميع الملفات الموجودة على الوسائط الإلكترونية ذات الأصل غير المؤكد أو الملفات المستلمة عبر شبكات غير موثوق بها بحثاً عن الفيروسات قبل استخدامها.

6. يجب فحص جميع محركات الأقراص بحثاً عن الفيروسات وأيّ نوع من التعليمات البرمجيّة الضّارة، مرة واحدة على الأقل في الأسبوع.
7. يجب أنْ يكون برنامج مكافحة الفيروسات قادراً على مراقبة الأنظمة وتنبيه موظفي دعم الهيئة المحليّة واتخاذ الإجراءات التّصحيحيّة في حالة اكتشاف الفيروسات.

8.6 السياسات ذات الصّلة

1. سياسة التّعافي من الكوارث.
2. سياسة تقييم المخاطر.
3. سياسة النّسخ الاحتياطيّ .
4. سياسة تغيير كلمة المرور.

9. سياسة خدمات الدعم التقني

9.1 المقدمة والأهداف

9.1.1 المقدمة

دائرة الدّعم الفنّي و تعرف باللغة الإنجليزية " HelpDesk " هي مزيج من العمليّات الإداريّة، ومهمَّات الدَّعم بالإضافة إلى استخدام النّظم و البرمجيات لترتبط معاً وتشكِّل وحدة جديدة كجزء من قسم تكنولوجيا المعلومات والاتصالات، بالتالي تعتبر دائرة الدّعم الفنّي نظاماً شاملاً يستخدمه موظفو الدّعم لتوفير الحلول الأوليّة، وإدارة ومتابعة الدّعم أو الخدمة، والطلبات الناشئة عن المواطنين/المستخدمين، وضمان تسجيل المشكلات وتعقبها بشكل منظم.

9.1.2 بيان السياسة

تقوم دائرة الدّعم الفنّي بعمل محوري في آليات تقديم الخدمات التكنولوجيا حيث إنّها الجهة الرئيسة الأولى وواجهة الاتصال مع المستخدم النّهائي لتقديم حلول لجميع أنواع الإشكاليّات التي تحصل نتيجة استخدام الأجهزة الإلكترونيّة التّابعة للهيئة. يتمحور عمل دائرة الدّعم الفنّي على إدارة وتنظيم خدمات الدّورة المتكاملة لتكنولوجيا المعلومات المُقدمة لموظفي الهيئة المحليّة والتي تتضمن التّالي:

1. إدارة عمليّة الدّعم الفنّي والتّقني.
2. إدارة عمليّة طلبات الخدمة.
3. إدارة عملية تقديم الخدمة.
4. الإبلاغ عن الحوادث.
5. إدارة عمليّة الجودة في تقديم الخدمة (SLA).
6. تقديم التّقارير بالحوادث التي تعيق العمل في المؤسسة.
7. توثيق التغييرات والتحسينات الرئيسة على نظم تكنولوجيا المعلومات المستخدمة في الهيئة المحلية ضمن الإجراءات المتّبعة.
8. إدارة بوابة المعرفة.

9.1.3 نطاق العمل

تنطبق هذه السّياسة على جميع أنواع الخدمات المرتبطة بتكنولوجيا المعلومات والاتصالات.

9.1.4 الهدف

تهدف هذه السّياسة إلى تأسيس الإجراءات للتحكم بجميع أدوات وطرق تقديم خدمات الدّعم الفنّي بما ذلك الحصول على الأجهزة والبرمجيات أو الخدمات من خلال طرفٍ ثالث. يهدف الدّعم الفنّي لدى الهيئة المحليّة بتوفير الخدمات التالية:

1. تبسيط وتحسين عمليات الدّورة المتكاملة لخدمات تكنولوجيا المعلومات.
2. تحسين وقت الاستجابة لطلبات الخدمة وتقليل الوقت المستغرق في تتبع الطلبات.
3. توفير خدمات دعم فعّالة لموظفي الهيئة المحليّة.
4. تقديم حلول فعّالة للحوادث المتعلقة بتكنولوجيا المعلومات.
5. تحسين الاتصالات بين تكنولوجيا المعلومات وإدارات البلديات الأخرى.
6. تحسين تحرك الموظفين للاستجابة عند حدوث حادث.
7. زيادة إنتاجية الهيئة المحليّة بالاعتماد على شفافيّة إجراءات خدمات الدّعم.
8. استخدام دائرة الدّعم الفنّي لإدارة ومراقبة وتحسين الأداء في عمليّة الدّعم المقدَّمة للموظفين وإصدار تقارير دوريَة تساعد الإدارة على اتّخاذ قرارات مدروسة بخصوص الخطط المستقبلية.

9.1.5 المسؤوليات والأدوار

1. يعتبر الدّعم الفنّي الواجهة الأولى للاتصال والمستوى الأول لتقديم الدّعم للمستخدم النّهائي.
2. يعتبر موظفو الدائرة المستوى الثاني لتقديم خدمات الدعم التقني.
3. سيقوم الدّعم الفني باتباع الإجراءات المقرة بهذه السياسة.
4. ستقوم الدّائرة بإيجاد الضّوابط اللازمة لتنفيذ هذا الإجراء.
5. ستقوم الدائربتلبية جميع طلبات المساعدة المتعلقة بالطّلبات المدعومة في إطار اتفاقية مستوى الخدمة المتفق عليه
6. سيقوم الدّعم الفني باتّباع الإجراءات المقرة من أجل توثيق الطلبات، وإبلاغ المتقدمين بطلب التغيير بالتّطورات، وإبلاغ الدّوائر التي تتأثر بالتغيير، ومتابعة حالة طلب التغيير.
7. سيقوم الدّعم الفنّي بتوثيق اجتماعات المجلس الاستشاري للتغييرات العاديّة والطّارئة والقرارات المُتخذة.
8. سيقوم الدّعم الفنّي بإدخال طلبات التغيير بسجل متابعة التغييرات مع إعطاء صفة الوضعيّة كما حددتها سياسة الدّعم.
9. على موظفي الهيئة المحليّة التبليغ عن أي خلل بعمل الأجهزة أو عطل في تقديم الخدمات.
10. يعتبر مسؤول الدّائرة أو من ينوب عنه مسؤولاً عن تنفيذ هذه السّياسة.

9.2 السياسات والإجراءات

9.2.1 أهداف دائرة الدّعم الفنّي

1. تيسير الحلّ السّريع لمشاكل العملاء من خلال نقطة اتصال واحدة.
2. الاحتفاظ بسجل يوثق الدّعم المقدَّم لكلِّ عميل.
3. تحديد مواقع المستخدمين التي تواجه صعوبة مع تطبيق معين.
4. تعقب نوع المشاكل التي تتم مواجهتها لكلِّ تطبيق.
5. الكشف عن المشاكل المتكررة والمساعدة في تخطيط مسار تصحيحي للعمل.

إنشاء إحصائيات، مثل عدد المكالمات ونوعها حسب التطبيق.

9.2.2 خدمة الدّعم الفنّي

يستلم الدّعم الفنّي جميع الطّلبات المختصة بخدمات تكنولوجيا المعلومات والاتصالات الحاليّة والجديدة، ويمكن أخذ لمحه عن عمل الدّعم الفنّي بملاحظة العيّنة التّالية من الخدمات:

أ. **الأحداث:**

1. إنشاء وتحديث وحذف المستخدمين في أنظمة تطبيقات.
2. إنشاء وتحديث وحذف المستخدمين في النّطاق(Domain).
3. إنشاء وتحديث وحذف مجلدات المستخدم المشترك.
4. إنشاء وتحديث وحذف المستخدمين في نظام إدارة الهاتف.
5. تكوين وتركيب أجهزة الهاتف.
6. إضافة وإزالة الأجهزة.
7. تثبيت وتكوين وتحديث البرامج الموصَى بها أو المعتمدة ؛
8. تركيب وإعداد أجهزة الكمبيوتر والعناصر الطرفية.
9. صيانة برامج التّطبيقات ودعم جميع طلبات التّغيير.
10. إدارة تسجيل الطّلبات وتتبعها وتوفير الدّعم الفنّي بهدف تقليل عدد المشكلات من الوصول إلى دعم المستوى الثّاني والثّالث من خلال استهداف حل المكالمة الأولى.

ب. **الدّعم العام**

1. المستوى الأول للدّعم الفنّي.

2. نصائح عامّة حول الحوسبة: يشمل الدّعم الفنّي دعم المستخدمين الذين يستخدمون أجهزة الكمبيوتر الشّخصيّة، وتطبيقات العمل مثل مايكروسوفت اوفس، وتطبيقات البريد الإلكتروني أو التطبيقات المحددة مثل iMAL،
3. خدمات دعم الشبكة
4. خدمات النّسخ الاحتياطيّ واستعادة الملفات.
5. تسجيل ومراقبة وتتبع وتحديث الطّلبات.
6. إدارة مستوى الخدمة.
7. مساعدة إدارة التغيير وتسهيل إخطارات طلب التغيير.
8. تقارير الاستخدام والأداء.
9. عمل استبيانات مع المستخدمين النهائيين (الموظفون مثلاً).
10. تزويد المستخدمين النهائيين بالمعلومات عن انقطاع الخدمة أو إخطارات تكنولوجيا.
11. تقديم تحديثات عن الحوادث الرئيسة باستخدام "نموذج الحوادث الرئيسة".
12. قاعدة معرفة الخدمات.

9.2.2.1 تحديد الأولويات

تستخدم *مكتبة البنية الأساسية لتكنولوجيا المعلومات (ITIL)* (ITIL) ثلاث أدوات للقياس لتقرر التّرتيبات التي يجب التّعامل من خلالها مع الحدث (انقطاع غير مخطط له، أو توقف بالخدمة)، وتحديد وضع التغيير:

1. التأثير:
أ. المنخفض: يؤثر على عمل الموظفين بشكلٍ فرديّ، ولكن يمكن تجاوز المشكلة من خلال طرق بديلة.
ب. العادي: يؤثر على عمل الموظف بشكلٍ فرديّ.
ت. العالي: يؤثر على عمل الأجهزة الأساسيّة والحسّاسة.

2. مدى الضّرورة: إلى أيّ مدى يمكن تأجيل الحلّ أو المدة الزمنية المطلوبة لحلّ الحادث:

أ. 1: إلى 0.5 ساعة.
ب. 2: إلى 2.0 ساعة.
ت. 3: إلى 6.0 ساعات.

3. الأولوية: ما هي السّرعة الواجبة لمعالجة الحادث (وعلى سبيل المثال) يتحدد من خلال الاتي:
أ. الأولوية (1: 16) ساعة.
ب. الأولوية (2: 8)ساعات.
ت. الأولية (3: 4)ساعات.
ث. حساس (4: 2)ساعات.

تقترح ايتيل أن تكون الأولوية نتاج الأثر والضرورة كما تبين الاتي:

	مدى الضرورة 1	مدى الضرورة 2
الأثر 1	الأولوية 1	**الأولوية 2**
الأثر 2	**الأولوية 2**	**الأولوية 3**
الأثر 3	الأولوية 3	**الأولوية 4**

يجب الانتباه أنَّ تحديد المدّة الزّمنية لتنفيذ الحلول عبارة عن توقعات توضع منْ قِبل الدّائرة، آخذين بعين الاعتبار إمكانيّة الحاجة لتّدخل طرفٍ ثالث.

9.2.3 إذن تفويض

1. وجوب الحصول على الموافقات المناسبة والتواقيع المعتمدة من مسؤول وحدة الأعمال التي تطلب التغيير قبل تقديمه إلى الدعم الفني.

2. من المقبول لوحدة أعمال ليست تابعة لقسم تكنولوجيا المعلومات أن ترسل "نموذج طلب تغيير النظام" مع توقيع المسؤول عن الدائرة فقط.
3. سيقوم الدعم الفني بتوجيه طلب التغيير إلى موظفي تكنولوجيا المعلومات المناسبين وللحصول على مزيد من الموافقات بناءً على سياسة **إدارة التغيير**.
4. المدير العام للهيئة أو من ينوب عنه مسؤول عن إعطاء الموافقة أو الرفض على طلبات تغيير النّظام ذات التأثير العالي.

9.2.4 مسؤوليات المستخدم النهائي

يُطلب من موظفي الهيئة المحليّة تقديم معلومات مفصَّلة عند طلب الخدمة باستخدام النّموذج الصّحيح .

9.2.4.1 نماذج طلبات الخدمة

يجب تطوير نماذج المستخدمة بالدّعم التّقني بهدف جمع المعلومات الصحيحة لحل مشكلة قائمة في البيئة التكنولوجيا أو إدخال خدمة جديدة. انظر الملحق للحصول على عينة من النّماذج المختلفة المقترحة:

1. **طلب دعم**: الطّلبات التي تغطّي الأجهزة أو البرامج أو الخدمة المثبّتة والفشل في الأداء أو تعتبر غير صالحة مثل لوحة المفاتيح المعطلة أو عدم القدرة على الطّباعة أو الوصول إلى مورد الشبكة.
2. **طلب خدمة:** الطّلبات التي تغطي احتياجات المستخدم النّهائي للأجهزة أو البرامج أو الخدمات الجديدة.
3. **طلب لتقديم مقترحات جديدة:** طلب لخدمة تعتبر مشروع تطويري، مثل: تقديم تكنولوجيا جديدة، أو حزمة برامج، أو حلول.
4. **تقرير حادث رئيسي**: الإبلاغ عن الحوادث بهدف توفير تحكُّم مزدوج وتقليل تكرار وقوع الحادث.
5. **الإبلاغ عن حوادث أمن المعلومات**

9.2.5 إجراءات الدعم الفني

1. يمكن إرسال جميع طلبات الخدمة إلى الدّعم الفنّي بعدّة طرق ومنها: التّسليم الشّخصي للطلب، مكالمة هاتفية، بريد إلكتروني إلى helpdesk@municipal.ps أو إرسالها عبر مذكّرة داخليّة.
2. سيتم إرسال إيصال التّأكيد خلال ساعات العمل العاديّة إلى مقدِّم الطّلب في غضون # ساعة. سيتلقى المستخدمون النهائيون ردّاً برقم تتبع الحالة.
3. **تسجيل الطلب:** سيتم تسجيل جميع الطّلبات والتّحقق منها في نظام الدّعم الفنّي والتّأكد من كتابة جميع المعلومات المطلوبة. إذا كان النّموذج غير مكتمل، فسيتم إرجاع الطّلب إلى مقدم الطلب لاستكماله.
4. **فتح طلب:** سيتم فتح طلب في النّظام مع اسم طالب الخدمة ورقم الهاتف ووصف الحادث وتحديد مستوى الخدمة (SLA) الصّحيحة (يرجى الاطلاع على تحديدات مستوى الخدمة في القسم أدناه). إذا كان من الممكن إيجاد حل فوري للحادث ، مثل إعادة تعيين كلمة المرور على سبيل المثال فسيقوم الموظف في الدّعم الفنّي بالاهتمام بالحادث على الفور، وتحديث نظام التّسجيل وفقاً لذلك، مع تعيين وضع "الحالة" المناسب في السّجل (انظر سجل الحالة أدناه).
5. **حل المشكلة**: ستحاول الدّائرة حل جميع المشكلات والطلبات الخاصّة بالأنظمة والتّطبيقات المدعومة بشكلٍ فوري ولكن إذا ظلّت المشكلة دون حل، فمن الممكن تصعيدها إلى المستوى الثّاني من الدّعم وإذا كانت تتطلب مشاركة الموردين الخارجيين أو مقدمي الخدمات (دعم المستوى الثالث)، فسيتم إبلاغ مقدم الطّلب بهذه التّرتيبات والتّأخيرات المحتملة في حلّ الحادث .
6. **إغلاق الحوادث:** سيتم إغلاق جميع الحوادث عندما يتم تنفيذ المهمة بنجاح ويكون الطلب "مغلقاً"، أمّا في حالة كون الحادث معقداً ولا يمكن حله خلال فترات زمنية معقولة، أو أنَّ حل الحادث قد يكون باهظ التّكلفة، فسيتم إبلاغ مقدم الطلب بالخيارات المتاحة.
7. **رضا المستخدمين النهائيين:** سيتم إجراء استطلاعات للرأي لضمان رضا المستخدمين النهائيين. قبل إغلاق أي طلب يجب أنْ يتأكد موظف الدّعم الفنّي من مقدم الطلب ما إذا كان قد تم حلّ الإشكال بشكلٍ مُرضٍ. بمجرد حلّ الحادث، سيتم تحديث نظام التّسجيل مع وضع الحالة المناسبة بالسّجل.

8. **يقدم الدعم الفني الدعم الكامل** خلال ساعات عمل الهيئة المحلية. في حالة الطوارئ أو لأي مشكلة مِلّحة لا يمكن أن تنتظر حتى يوم العمل التالي، يجب على المستخدمين النهائيين الاتصال بالمهندس أو الفنّي المعين بالاتصال على رقم: XXXX.

أ. سجل الحالة

حالة	تعريف
أ - معتمد	وافق المسؤولين المحددين (مسؤول طالب الخدمة ، مسؤول الدائرة المتأثرة) على نموذج طلب تغيير النظام ووقع عليه.
ن - نفذت	أكمل المنفذ طلب التغيير. قد لا يزال الاختبار / التحقق من صحة التغيير مطلوباً.
نجاح - "مغلق"	أكد المنفذ و / أو مقدم الطلب الانتهاء بنجاح من اختبار ما بعد التنفيذ (إذا لزم الأمر) والتحقق من صحة التغيير.
غ-غير ناجح	قرر المنفذ و / أو مقدم الطلب أن التغيير، أثناء الاختبار والتحقق من الصحة ، لم يفي وظيفياً بمتطلبات العمل. إذا لزم الأمر سيتبع المنفذ خطة التراجع.
ح - عقد	طالب مقدم الطلب و / أو المنفذ بتعليق طلب التغيير. قد يطلب مسؤول وحدة الأعمال أيضاً تعليقاً بسبب متطلبات المعلومات الإضافية أو تضارب المواعيد.
ج - ملغاة	تم إلغاء طلب التغيير.
د- مرفوض	تم رفض طلب التغيير لسبب محدد (مثل متعارضات الجدولة ومشكلات الموارد وما إلى ذلك).

ب. اتفاقية مستوى الخدمة "SLA"

يتم تسجيل الطّلبات التي يتم إنشاؤها من خلال الدّعم الفنّي في النّظام وإعطاء صفة محددة بناءً على اتفاقية مستوى الخدمة (SLA). التالي (كمثال):

مستوى الخطورة / أولوية	وصف تأثير الأعمال	أمثلة	زمن الاستجابة
معلوماتية (5)	طلب للحصول على المعلومات فقط	كيف يمكنني تغيير الخط الافتراضي الخاص بي؟ كيف أضيف طابعة أو أغيرها	# أيام العمل (ثلاثة أيام عمل)
منخفض (4)	تأثير طفيف المشكلة هي التي تؤدي إلى خسارة طفيفة في الخدمة ولكنها لا تؤثر على الإنتاجية. الموظف يحتاج إلى معلومات و التركيب و إعدادات أو الصيانة المؤجلة. يواجه الموظف مشاكل ملحوظة ولكن لا يزال بإمكانه أداء معظم العمليات.	جهازي بطيء في التمهيد. التطبيق بطيء في التشغيل.	# أيام العمل (يومي عملٍ مثلاً)
وسط (3)	مشاكل تؤدي إلى تدهور إنتاجيه الهيئة المحلية على المدى البعيد، مشاكل تكون مُلاحَظة من قبل الزبون. إنها قضية حساسة للوقت ومهمة	جهاز كمبيوتر واحد لا يعمل.	# من الساعات (يوم عمل مثلاً)

	للإنتاجية على المدى الطويل، ولكن لا يتسبب في توقف فوري للعمل أو قلق كبير للعملاء.	لا يستطيع شخص واحد الطباعة. يحتاج المستخدمون تحميل مايكروسوفت اوفس.	
عالي (2)	تأثيرها شديد ومتعدد وقد يمتد لأكثر من موظف أو لعدة مستخدمين ولا يوجد حل متاح. يعاني العديد من الموظفين من مشاكل ملحوظة تؤثر على العمليات وعدم القدرة على إنجاز الأعمال.	لا أحد يستطيع الطباعة. الكمبيوتر الوحيد الذي يحتوي على تطبيق مهم للأعمال معطل.	مباشر (2-4 ساعات) مثلاً
طارئة وحرجة (1)	قاتلة – مهلك، يؤثر على المكونات الحاسمة لبيئة الإنتاج الخاصة بالعميل. أكثر من مستخدم واحد غير قادر على الوصول إلى أجهزتهم أو موارد الشبكة بسبب مشكلة واحدة ذات صلة. تشير الإشارة الأولية إلى أنّ المكونات الحرجة ربما تتعطل لمدة تزيد عن 30 دقيقة. تسبب حالات الانقطاع على مستوى النظام في إحداث تأثير كبير على العمليات والتعليمات التجارية الهامة.	توقف الجهاز الرئيسي عن العمل أو الخادم معطل ولا أحد يمكنه الوصول إلى نظام البريد الإلكتروني على المستوى الخارجي.	فوري وبفترة لا تتجاوز الربع ساعة + يخطر الإدارة فوراً

الاستجابة والإقرار بالاستلام ضمن اتفاقية مستوى الخدمة *

مستوى الخطورة	الإقرار بالاستلام	الاستجابة	التعديل على الحالة (عندما يتطلب الحل وقت أكثر من أكبر من # ساعة)
طارئة والحرجة (1)	مباشر	=< 14 دقيقة	لا ينطبق
مرتفع (2)	=< 30 دقيقة	2 ساعات	لا ينطبق
وسط (3)	=< 60 دقيقة	2-4 ساعات	مرة كل 8 ساعات
منخفض (4)	=< 4 ساعات	يوم عمل واحد	مرة كل 16 ساعة
استعلام (5)	=< 4 ساعات	يوم عمل واحد	مرة كل 16 ساعة

*** تحتاج دائرة تكنولوجيا المعلومات والاتصالات والإدارة إلى تحديد الأطر الزمنية للعمليات المذكورة أعلاه**

ج. إجراءات العميل

من المتَّوقع أن يطور العميل خبرة وعمل إجراءات داخليّة من أجل إيجاد حلول للمشاكل والتصعيد. قبل الاتصال مع الدّعم الفنّي، يجب على الخبير الدّاخلي بذل قصارى جهده لحلّ المشكلة من خلال الرّجوع إلى وثائق ودليل النّظام أو اتباع الإجراءات الخاصّة بالموقع. إنَّ الخبرة الدّاخلية وإجراءات حلّ المشاكل مهمة من أجل:

1. حلّ المشاكل الإجرائيّة والفريدة التي تواجه العميل بواسطة السّلطة الملائمة بالعميل.
2. يمكن حلّ المشاكل البسيطة دون أي تأخير.
3. تحديد المسائل المتعلقة بالموظفين الذين بحاجة إلى تدريب إضافي، وبالتالي يمكن اتخاذ إجراءات تصحيحية في الوقت المناسب.

د. تصعيد طالب الخدمة

يتمركز مجمل عمل موظفي دائرة الدّعم الفنّي على توفير خدمة الدّعم لطلبات المستخدمين النّهائيين في أسرع وقت ممكن، ولكن يتوقف هذا على مدى تعقيد و نطاق الخدمة المطلوبة، فبعض الحوادث تُحل في غضون فترة زمنية بسيطة و بعضها قد يستغرق عدة ساعات أو عدة أيام، ومع ذلك هناك أوقات يحدث بها تأخير بالاستجابة للخدمة المطلوبة و يصبح من الضّروري التّصعيد إلى مستويات أعلى من الإدارة لإسراع عملية الرّد على الطّلب المنشود، و قد يكون ذلك التّصعيد من قِبل الشّخص طالب الخدمة أو موظف الدّعم الفنّي. يجوز لطالب الخدمة الاتصال بالمستوى التالي من الإدارة لتسريع الحل.

مستويات التصعيد:

المستوى 1- عادي : طاقم الدعم التقني.
المستوى 2 - التصعيد: مسؤول الدعم التقني.

ذ. سجل طلب تغيير على النظام

يقوم الدّعم التّقني بالمحافظة على سجل خاص لطلبات التغيير على النظام، ويحتوي هذا السّجل على قائمة موحدة لجميع نماذج طلبات تغيير النّظام وحالة كل طلب. يقوم الدّعم التّقني طوال مرحلتي الموافقة والتنفيذ بعملية المتابعة المستمرة للتغيير من أجل تحديث الحالة باستمرار. ستكون القائمة الموحدة لجميع نماذج طلب تغيير النّظام موجودة في موقع محدد معروف لمسؤول الدّائرة والمدير العام للهيئة.

ر. متابعة ما بعد الخدمة

بعد تنفيذ دعم الخدمة واختباره ، يتم تطبيق ما يلي:

1. سيؤكد الدّعم التّقني استكمال تقديم الخدمة وانتهائها.
2. سيقوم الدّعم التّقني بتحديث السّجل وتوثيق جميع المستندات.

ز. قائمة التحقق

يتم التّحقق من الإدخالات التّالية لسجل تقديم الخدمة بهدف التأكد من مصداقيتها وأنّها متكاملة أثناء إغلاق طلب دعم الخدمة:

1. بروتوكول الإجراءات.
2. الشّخص المسؤول.
3. مجموعة الدّعم.
4. الوقت و التّاريخ.
5. وصف النّشاط.
6. توثيق الحلول التطبيقية.
7. توثيق السبب الجذري لانقطاع الخدمة.
8. تاريخ قرار الحادث.
9. تاريخ إغلاق الحادث.

س. جدولة تنفيذ التغيير والأخطار

1. سيقوم الدّعم التّقني بإدخال جميع طلبات الخدمة في السّجل لتتبع أحداث التغيير المجدولة والإبلاغ عنها لوحدات العمل والدّائرة والأطراف المعنيّة.
2. سيرسل إشعاراً بالبريد الإلكتروني إلى الإدارات المتأثرة و\أو المكاتب الخارجية مكتوبة من قِبل مقدّم الطّلب (بمساعدة الجهة المنفذة حسب الحاجة).
3. يجب جدولة تغييرات النّظام في أوقات مختارة لتقليل التأثير على المستخدم / العميل. بمجرد جدولة أي نوع من التغيير والموافقة عليه، لا يمكن تعديل التاريخ و\أو الوقت.
4. يجب أن يحصل التغيير المُعاد جدولته على موافقة من الأفراد الذين وقّعوا على طلب التغيير الأصلي.
5. يتم إرسال الإخطارات العامة من قِبل الدّعم التّقني على أساس الحاجة، مثل خطة انقطاع الخدمة بعد الموافقة عليها.

ش. التقارير والأداء

تقديم التقارير للإدارة هي من أهم أعمال دائرة الدّعم الفنّي، حيث تستخدم هذه التّقارير كوسيلة إداريّة لقياس حجم الأنشطة التي تقوم بها دائرة تكنولوجيا المعلومات والاتصالات، وتبين مراحل عملية التّنفيذ وتنظيم الإنتاجية لدى الدّائرة، ومن المزايا الإضافية لكتابة التّقارير:

1. تبين المشاكل والطّلبات المتكررة.
2. توضح مراحل عمليات التنفيذ للإدارة العليا.
3. التحديث المستمر على حالة الطلبات والمشاكل الموجهة للدّائرة.
4. تعمل على تقديم خدمة موحدة ومنظمة لجميع الدوائر بالهيئة المحليّة .
5. تقدم الإحصائيات حول عدد المشاكل بناءً على الموضوع أو التّاريخ أو أيّ تصنيفٍ آخر.
6. تعمل على تحسين الخدمة المقدمة وتوثيق عمليّة التّنفيذ فتحسن الإنتاجيّة، توضح الطلبات المفتوحة والمغلقة، والطلبات التي خرجت عن اتفاقية مستوى تقديم الخدمة .
7. تُستخدم لتحدد نقاط الضعف في الأنظمة أو المستخدمين.
8. تُستخدم كأداة للمساءلة.

ص. أنواع التقارير

تحتوي التّقارير على بيانات إحصائيّة حول عدد الطّلبات المفتوحة والمغلقة، وتاريخ الطّلب، والدّائرة المرسلة للطلب، والأهمية، والحالة، والشّخص المسؤول عن الطلب، وعدد الطلبات حسب مستوى الخدمة المطلوبة، وعدد الطلبات حسب الأهمية والأولوية، وعدد الطلبات المرسلة لكلّ شخصٍ مسؤول عن حلها.

ض. الإبلاغ عن الحوادث الرئيسة والكوارث

1. الكوارث هي الأمور غير المخطط لها التي تعترض العمل وتسبب أضرار فادحة للهيئة كتوقف النّظام الإلكتروني أو خلل في شبكة الاتصالات في الهيئة المحليّة. الإبلاغ عن الكوارث هي إحدى مهمات موظفي الدّعم الفّني.
2. يتولى الدّعم التّقني الإبلاغ عن الحوادث بعد أو أثناء إدارة الحادث.
3. عند وقوع الكارثة، على الدّائرة أو الموظف الذي يتتبع هذه المشكلة الإبلاغ عن الحدث ضمن إجراءات العمل وتقديمه إلى دائرة الدّعم الفنّي. دائرة الدّعم الفنّي تقوم بدورها بإعلام الشّخص المناسب من الإدارة العليا طبقاً لما هو متفق عليه في السّياسة العامة للإبلاغ عن الكوارث.
4. إذا تعطلت خدمة رئيسية (كتوقف جهاز الكمبيوتر الرئيسي) لمدة معينه من الوقت (مثل 60 دقيقة)، أو تكررت أكثر من مرة خلال 3 أشهر حتى لو لوقت أقل من 60 دقيقة ، يتطلب إعلام رئيس الهيئة المحلية أو المدير العام.
5. إذا حدث فشل في النّظام ولكنه لم يؤثر على العملية الأساسيّة مثل خادم الملفات أو الطّابعة، فلا داعي لإخطار الإدارة، ومع ذلك سيتم إنشاء تقارير عن الحوادث وإرسالها إلى مديري أقسام دائرة تكنولوجيا المعلومات.

ط. سياسة الإعلام عن الكوارث

المستوى	النظم والخدمات المتأثرة	مدة التوقف	الجهة المبلغة
عالي (2)		=< 30 دقيقة	لا يتم الإبلاغ
طارئة وحرجة (1)	توقف جهاز كمبيوتر رئيسي مثل : سيرفر النظام وقاعدة البيانات، عدم وجود مركزية بين الإدارة والفروع	=< 60 دقيقة، أو تكررت أكثر من مرة خلال 3 أشهر حتى لو لوقت أقل من 60 دقيقة	رئيس الهيئة المحلية والمدير العام للهيئة

توثيق التغييرات والتحسينات الرئيسية على نظم تكنولوجيا المعلومات المستخدمة في الهيئة المحلية .

يقوم موظف دوائر نظم المعلومات إبلاغ دائرة الدّعم الفنّي عن أية تغييرات أو تحسينات رئيسة على نظم تكنولوجيا المعلومات كانت مخططة أو طارئة عن طريق تقديم نموذج تغييرات أو تحسينات رئيسة لتقوم دائرة الدّعم الفنّي بتوثيقه.

فترات التّقرير (أو حسبما تراه الإدارة مناسباً)

- تقارير يومية أو أسبوعية لأقسام تكنولوجيا المعلومات.
- تقارير شهرية لمدير عام الهيئة المحلية.
- تقارير ربع سنوية لرئيس الهيئة المحلية والمجلس.

9.3 بوابة المعرفة

تخدم هذه البوابة موظفي الهيئة المحلية بلا استثناء، حيث يقوم طالب الخدمة بالبحث عن الحلول في المشاكل الأساسية في أقسام بوابة المعرفة، مثل: كيفية الاتصال بطابعة معينة، فيتم تغذية بوابة المعرفة عن طريق إضافة موظفي الدعم الفني الحلول للقضايا الأساسية على شكل مقالات.

من محاسن وجود بوابة المعرفة :

1. إيجاد حلول سريعة و مكتوبة للقضايا التي تتكرر باستمرار.
2. تقليل عدد الطلبات الموجهة إلى دائرة الدّعم الفنّي مما يؤدي إلى تقليل الوقت و الجهد .
3. يسمح لطالب الخدمة في البحث عن الحلول قبل إرسال طلب الخدمة لموظفي الدّعم الفنّي مما يؤدي إلى زيادة معرفة الموظفين بتطبيقات الحاسوب.

9.4 مواصفات الأجهزة والبرامج

يجب أن تحدد دائرة تكنولوجيا المعلومات والاتصالات أنواع الأنظمة الموجودة لديها ووفقاً لسياسة شراء تكنولوجيا المعلومات، يجب أنْ يكون لكل وحدة رقم بطاقة تعريف أو رقم تعريف.

9.5 السياسات ذات الصلة

1. سياسة إدارة التّغيير.
2. سياسة التّعافي من الكوارث.
3. سياسة تقييم المخاطر.
4. سياسة النَّسخ الاحتياطيّ.
5. سياسة كلمة المرور.
6. سياسة إدارة موردي خدمات تكنولوجيا المعلومات.
7. سياسة خدمات الاستعانة بمصادر خارجيّة لتكنولوجيا المعلومات.

10. سياسة تغيير كلمة المرور

10.1 المقدمة والأهداف

10.1.1 بيان السياسة

وُضعت هذه السّياسة لتتناول آليات الوصول إلى أنظمة الهيئة المحليّة الإلكترونيّة من خلال معلومات تسجيل دخولٍ مُكونةً من اسم مستخدمٍ وكلمة مرورٍ بهدف حماية معلومات الهيئة المحليّة السّرية والمُقيدة من جميع التّهديدات المحتملة وكجزءٍ من الخطواتِ المناسبة لتمكين الأمان العام للهيئة. كما تحدد الضّوابط ضد تهديدات الوصول غير المُصرَّح به وسرقة المعلومات وتعطيل للخدمات نتيجة الفيروسات، والكشف عن رسائل الاتصال الإلكترونيّة الدّاخلية والخارجيّة (البريد الإلكتروني) التي يتم إنشاؤها أو إرسالها أو تخزينها عبر الإنترنت، أو عبر شبكة الإنترنت الخاصّة بالهيئة المحليّة من خلال موظفيها ومديريها ورؤساء دوائرها والزّوار والمتعاقدين الذين يستخدمون أنظمة البريد الإلكتروني الخاصّة بالهيئة المحليّة .

تؤكد السّياسة على:

1. الضّمان المعقول بأنْ يقتصر استخدام أنظمة الهيئة المحليّة على الأفراد المُصرَّح لهم.
2. الضّمان المعقول بأنْ يقتصر الوصول إلى أيٍّ من برامج الهيئة المحليّة على الأفراد المُصرَّح لهم وعلى النّحو المناسب.
3. الضّمان المعقول بأنْ تكون الأنظمة الحسّاسة المُحددة معزولةً بشكلٍ مناسب.
4. توفير الإرشادات الكافية حول مسؤولية المُستخدم النّهائي عن كلمات المرور وحمايتها.

10.1.2 الهدف

تهدف هذه السّياسة إلى حماية سرّية وأمان وسلامة وتوافر جميع المعلومات المُقيدة التي تم إنشاؤها واستلامها وإرسالها وتخزينها بواسطة النظم الإلكترونيّة التّابعة للهيئة.

10.1.3 نطاق العمل

تسري هذه السّياسة على جميع مستخدمي الأجهزة الإلكترونيّة التّابعة للهيئة بما في ذلك الموظفين (بدوامٍ كاملٍ وجزئي) والموردين وشركاء الأعمال وموظفي المتعاقدين والوحدات الوظيفية، بغضّ النّظر عن الموقع الجغرافي. كما تشمل أيضاً جميع بيئات أنظمة المعلومات التي يتم تشغيلها من خلال جهةٍ خارجيةٍ أو عن طريق التّعاقد معها، بما في ذلك:

1. جميع موظفي الهيئةِ المحليّة الذين يستخدمون مرافق البريد الإلكتروني أو أنظمة البريد الإلكتروني أو وظائف المراسلة الخاصّة بالهيئة المحليّة لتخزين المعلومات أو إرسالها، بما في ذلك المعلومات العامّة والسّريّة والمُقيدة.
2. جميع مرافق الاتصالات الإلكترونيّة الخاصّة بالهيئة المحليّة .
3. جميع وظائف المراسلات بما في ذلك المراسلة الفورية.

10.1.4 المسؤولية

تسري هذه السّياسة على جميع الموظّفين في **الهيئةِ المحليّة**، وبالتالي يتحملوا مسؤوليّة التّأكد من أنّ استخدام المرافق الإلكترونية الخاصّة بالهيئة المحليّة يتوافق مع الإرشادات الموضّحة في هذه السّياسة.

10.2 السياسات والإجراءات

10.2.1 إدارة كلمات المرور

يجب التّحكم بالوصول إلى شبكة أنظمة المعلومات (Network Domain) أو استخدام الأجهزة الإلكترونيّة التّابعة للهيئة باستخدام إجراءات تسجيل دخول المستخدمين بحيث تتوافق مع بروتوكولات إدارة كلمات المرور التّالية:

ا. وجوب استخدام كلمة مرور قوية:

1. يجب التّعامل مع جميع كلمات المرور كمعلومات مصنَّفة "سريّة".
2. يجب أن يبلغ طول كلمة المرور ثماني خاناتٍ على الأقل.
3. يجب أن تكون كلمات المرور أبجدية رقمية، أي يجب أن تشتمل على أحرفٍ وأرقام.
4. يجب أن تستخدم كلمات المرور مزيجاً عشوائيّاً من الأحرف (الكبيرة والصغيرة)، مع وجود أرقام وعلامات ترقيم متناثرة في كلّ مكان ولا يكفي استخدام رقم في بداية كلمة المرور أو نهايتها.
5. لا يجب استخدام اسم المستخدم في كلمة السّر.
6. لا يجوز استخدام أرقامٍ أو حروفٍ متكررةٍ، مثل (333 أو AAA) ، أو أرقام أو حروف متتابعة مثل (1124) أو (abcd).
7. يجب عدم استخدام الأسماء أو الكلمات الموجودة بالقاموس مثلاً.
8. يجب تغيير كلمات المرور للشّبكة بحدٍّ أقصى تسعون (90) يوماً (منذ آخر تغيير لكلمة المرور).
9. يجب تغيير كلمات مرور مسؤول الشّبكة (Root/Administrator) كل ثلاثين (30) يوماً، ويجب تغيير كلمة المرورللأجهزة المحليّة كل مائة وثمانون (180) يوماً، ويجب إعادة تعيين كلمات مرور حساب الخدمة مرة واحدة سنوياً أثناء الصّيانة.
10. يجب أن تكون هناك قائمة بكلمات المرور "التافهة" المحظورة، والتي يتم فرضها تلقائيّاً.
11. يتم تطبيق متطلبات تغيير كلمة المرور بالوسائل التكنولوجيّة كلما كان ذلك ممكناً.
12. يجب الاحتفاظ بتاريخ كلمة المرور، ويجب أن تكون كلمات المرور المنشأة حديثاً مختلفة عن كلمات المرور العشر (10) السّابقة المستخدمة.
13. يجب تمكين كشف التّسلل لمنع محاولات الاختراق بمنع الوصول بعد 3 محاولات إدخالٍ فاشلة. يجب أن تكون مدة المهلة قبل إعادة المحاولة لتسجيل الدّخول 30 دقيقة كحدٍّ أدنى وثلاثِ (3) ساعاتٍ كحدٍّ اقصى.
14. لا يجب السّماح للتّطبيقات بإعطاء تذكير أو لمحه عن كلمة المرور السّريّة.
15. يجب حذف الحسابات المعطّلة التي تزيد مدتها عن ستين (60) يوماً.
16. يجب انشاء نظام للتعرف والتحقق من المستخدمين قبل تسليم كلمات المرور سواء كانت جديدة، مؤقته، او بديلة وعند استحداث حساب لمستخدم يجب إصدار كلمة مرور مؤقتة لاستخدامها في تسجيل الدّخول لأولّ مرة فقط ويجوز إبلاغ المستخدم بها شفوياً.
17. يجب تغيير جميع كلمات المرور الأولية لأي نظامٍ من نظم المعلومات التّابعة للهيئة عند تشغيله واستخدامه لأول مرّةٍ بشكلٍ رسمي ويجب فرض مدة انتهاء لصلاحيتها ثلاثة (3) أيام لإجبار المستخدم على تغييرها.
18. استخدم المصادقة متعددة العوامل لإعادة تعيين كلمات المرور إذا كان ذلك ممكناً، مثل إرسال رسالة نصيّة إلى مستخدم الهاتف المحمول المرتبط بالحساب يجوز إرسال كلمات المرور الأولية، وإعادة تعيينها عبر الهاتف أو عبر البريد الإلكتروني لدائرة تكنولوجيا المعلومات التّابعة للهيئة (بعد تشفيرها).
19. يجب تغيير كلمات المرور فوراً إذا حصل اشتباه بأنّها اختُرقت، أو كإجراءٍ احتياطي عند الكشف عنها لفنيين يقومون بأعمال الصّيانة والدّعم.
20. يجب على المستخدمين الإقرار باستلام كلمات المرور المؤقت ويجب أن يُطلب من المستخدمين التّوقيع على بيان للحفاظ على سريّة كلمات المرور الشّخصيّة، ويمكن تضمين هذا البيان في شروط التّوظيف.

يحظر الأفعال التّالية :

1. الكشف عن كلمة المرور عبر الهاتف لأي شخص.
2. الكشف عن كلمة المرور في رسالة بريد إلكتروني.
3. التحدث عن كلمة المرور أمام الآخرين.
4. أي تلميح حول تنسيق كلمة المرور (على سبيل المثال ، "اسم عائلتي").
5. الكشف عن كلمة المرور في الاستبيانات أو نماذج الأمان.
6. مشاركة كلمة المرور مع أفراد الأسرة.
7. الكشف عن كلمة السر لزملاء العمل أثناء الإجازة.
8. يجب أن يكون لكل مستخدم من مستخدمي أي نظام معلوماتي اسم مستخدم فريد وكلمة مرور خاصة به.
9. يجب عدم استخدام أسماء المستخدمين العامة مثل حساب (Admin).

ب. يجب أن تتضمن عملية إدارة كلمات المرور الإجراءات التالية:

1. تسليم آمن لكلمة المرور الأوليّة والمؤقتة.
2. إجبار التّغيير الفوري لكلمة المرور.
3. تحديد آليات التّعرُّف على هويّة المستخدم في حالات الطّوارئ.
4. الإقرار باستلام كلمة المرور.

10.2.2 كلمات المرور لمستخدمي الوصول عن بُعد

يجب التّحكم في الوصول إلى شبكات الهيئة المحليّة عن بُعد باستخدام إمّا مصادقة كلمة المرور التي تصلح لمرة واحدة، أومن خلال استخدام نظام مفتاحٍ عام/خاص مع عبارة مرورٍ قويّة والتي يُنصح باستخدامها للمُصادقة. يحدد نظام المفتاح العام/الخاص علاقة رياضية بين المفتاح العام الذي يعرفه الجميع والمفتاح الخاصّ الذي يعرفه المُستخدِم فقط. وبدون عبارة المرور لا يمكن "إلغاء قفل" المفتاح الخاصّ وبالتّالي لا يمكن للمستخدم الولوج. جميع القواعد المذكورة أعلاه والتي تنطبق على كلمات المرور تنطبق أيضاً على عبارات المرور.

10.2.3 كلمات المرور هي سلطة للتصرف

يُمنح كل مستخدمٍ لنظام الكمبيوتر اسم مستخدم وكلمة مرور تسمح له بأداء وظائفه المُصرَّح بها. وتعتبر الهيئة المحليّة أنَّ أيّ إجراءٍ يتم اتخاذه بموجب اسم المستخدم وكلمة المرور هو إجراءٌ حصريٌ للشّخص الذي تم تعيين اسم المستخدم وكلمة المرور له، ويتحمّل هذا الشّخص المسؤولية الكاملة عن هذا الإجراء. وبناءً على ذلك، يتم إصدار كلمات المرور على أساسٍ فرديّ ويجب عدم مشاركتها، ولحماية الهيئة المحليّة ومعلومات دائرة تكنولوجيا المعلومات والموظف، يُحظر مشاركة أسماء المستخدمين وكلمات المرور.

حالات خاصة:

1. إذا كانت هنالك حاجة عملٍ ماسّة ولم يكن هنالك بديلٌ آخر سوى مشاركة اسم المستخدم وكلمة المرور، فيجب تقديم "نموذج طلب استثناء أمان المعلومات" إلى مسؤول أمان المعلومات للموافقةِ عليه. (أرجو ملاحظة اقتراح لهذا النموذج في نهاية هذا الكتيب؛ ملحق رقم.7).
2. كلمات المرور هي ملكٌ للهيئة ويجب تسليمها منْ قِبل الموظّف عند طلب مسؤوله، وقد يكون عدم القيام بذلك سبباً للفصل الفوري من العمل.

10.2.4 تخزين كلمات المرور

يجب توثيق جميع كلمات مرور النّظام بما في ذلك، على سبيل المثال لا الحصر، كلمات مرور الخدمات وكلمات المرور الرئيسة وكلمات مرور التّطبيقات، وكلمات مرور قواعد البيانات، وكلمات مرور المسؤولين، وكلمات مرور مسؤولي المجال (إلكترونيّاً وماديّاً) وحفظها في مكانٍ آمنٍ لا يمكن الوصول إليه إلا من قِبل المدير العام للهيئة. يُنصح، ولكن ليس مطلوباً بالاحتفاظ بقائمة كلمات المرور في مكانٍ ما خارج الموقع أو خارج المكتب الرّئيسي.

10.2.5 الإبلاغ عن اختراقات كلمات المرور

إذا توفر لأي موظفٍ ما يدعو للشّك في أنَّ كلمة المرور الخاصّة به أصبحت معروفةً لشخصٍ آخر أو تعرضت للاختراق، يجب تغيير كلمات المرور على الفور وإخطار مسؤول أمان المعلومات عبر خدمة الدّعم الفنّي.

10.2.6 منح حق الوصول والامتيازات

1. لا يمنح حقّ الوصول أو امتيازاتٍ أخرى لاستخدام أيّ من الأنظمة التّابعة للهيئة ما لم يتم الحصول أولاً على موافقةٍ كتابيّةٍ مسبقةٍ من المسؤول المناسب.
2. يجب أن تتناسب امتيازات الوصول مع المسؤوليات الوظيفيّة للموظف.

3. تُمنح امتيازات الوصول للمستخدمين الذين ليسوا من موظفي الهيئة المحليّة حسب ما تقتضيه الحاجة لأداء الأعمال المطلوبة وفقط عند الحصول على تصريح مناسب من المسؤول **(انظر إلى سياسة خدمة الدّعم الفنّي).**
4. يجب تكوين حسابات المستخدمين الذين ليسوا من موظفي الهيئة المحليّة بحيث تنتهي صلاحيتها تلقائياً عند انتهاء المدة المصرَّح بها .

10.2.7 ألغي حق الوصول والامتيازات أو تغييرها

1. يجب إيقاف ومنع جميع عمليّات الوصول إلى مرافق الهيئة المحليّة وأنظمتها فور انتهاء خدمة الموظف من الهيئة المحليّة .
2. يجب على مسؤولي الدّوائر الإبلاغ فوراً عن جميع التّغييرات المهمّة في مهام الموظف أو حالة التّوظيف إلى إدارة الموارد البشرية وخدمة الدّعم الفنّي، بما في ذلك التّغييرات الحاصلة مع الجهات الخارجيّة (الطّرف الثّالث).
3. بمجرد الموافقة على هذه التّغييرات أو التّحقق من صحّتها، يجب على خدمة الدّعم الفني و/أو الموارد البشريّة إخطار كل مسؤولي التّطبيقات والأنظمة لإجراء هذه التّغييرات.
4. فور الإخطار بانتهاء خدمة الموظّف، سيقوم مسؤولو التّطبيقات والأنظمة بتعطيل و/أو إزالة حقّ وصول المستخدم من جميع الأنظمة المعنيّة، واستعادة جميع معدات أنظمة المعلومات التّابعة للهيئة.
5. يجب تغيير جميع كلمات المرور للأنظمة الحسّاسة والمهمّة بالهيئة المحليّة فوراً في حال استقالة أو انتهاء عقد الموظف المسؤول عن هذه الأجهزة ولديه اطّلاع على كلمات المرور.
6. لا يتم الإخطار بإنهاء الخدمة سوى للموظف فحسب. وينبغي ألّا يتم تضمين غير الموظّفين في إخطارات الانهاء، كما يجب إزالة حقّ الوصول استناداً إلى آخر يوم للمستخدم في مقارّ الهيئة المحليّة، والذي قد يحدث قبل آخر يوم عمل.
7. بالنسبة للموظّفين الذين ينتقلون إلى منصبٍ مختلف، يجب على المسؤولين و/أو إدارة الموارد البشريّة تقديم طلباتٍ على الفور لخدمة الدّعم الفنّي للتّأكد من قيام مسؤولي التّطبيقات والأنظمة بإزالة حقّ الوصول إلى أنظمة المعلومات المختلفة عند الاقتضاء.
8. يجب أيضاً أنْ تكون طلبات تغييرات الامتيازات مكتوبةً وأنْ يوافق عليها مسؤول الموظّف قبل أنْ يقوم مسؤول الأنظمة بتنفيذ هذه الطّلبات.
9. ستتم إحالة أيّ نزاعاتٍ تتعلق بامتيازات الوصول إلى مسؤول أمان المعلومات للفصل فيها.
10. يجب على الإدارة إعادة تقييم النّظام و/أو امتيازات التّطبيقات الممنوحة للمستخدمين كلّ 11 شهراً على الأقل.
11. يجب على مسؤولي الأنظمة إلغاء جميع الامتيازات التي لم يعد المستخدمون بحاجةٍ إليها.
12. اعتماداً على مدى أهمية التّطبيق أو النّظام، قد يكون من المحبّذ تكرار مثل هذه المراجعات بشكلٍ أكثر تواتراً.

10.2.8 ضوابط موقع العمل

وفقاً لسياسة أمن المعلومات، يجب على جميع المستخدمين تأمين محطّة عمل الكمبيوتر الخاصّة بهم عند مغادرة منطقة عملهم المباشرة. يجب استخدام شاشات التّوقف باستخدام ميّزة الحماية بكلمة مرور إذا لم يتم استخدام لوحة المفاتيح أو الماوس لفترةٍ من الوقت. في نهاية كل يوم عمل يجب على المستخدمين تسجيل الخروج من جميع التّطبيقات والأنظمة.

10.3 السياسات ذات الصلة

1) سياسة الدّعم التّقني
2) سياسة أمن المعلومات.
3) سياسة إدارة المخاطر.

11. سياسة البريد الإلكتروني

11.1 المقدمة والأهداف

11.1.1 بيان السياسة

تتناول هذه السّياسة قضايا الوصول والكشف عن رسائل الاتّصال الإلكترونيّة الدّاخلية والخارجيّة (البريد الإلكتروني) التي يتم إنشاؤها أو إرسالها أو تخزينها عبر الإنترنت أو عبر شبكة الإنترنت الخاصّة بالهيئةِ المحليّة عن طريق موظّفيها ومديريها ورؤساء دوائرها والزّوار والمتعاقدين الذين يستخدمون أنظمة البريد الإلكتروني الخاصّة بالهيئة المحليّة. يتّحمل كل مسؤول ورئيس وحدة والموظفون مسؤوليّة التّأكد من أنّ استخدام نظام البريد الإلكترونيّ للهيئة يتوافق مع الإرشادات الموضّحة في هذه السّياسة، ومن هذا المنطلق ستتخذ الهيئة المحليّة إجراءاتٍ مناسبة لحماية المعلومات السريّة والمُقيدة التي يتم إنشاؤها، واستلامها، وإرسالها، وتخزينها بواسطة أنظمة البريد الإلكتروني ووظائف المّراسلة الخاصّة الهيئة المحليّة. نظام البريد الإلكتروني هو ملكٌ للهيئة؛ ولذا فإنّ جميع نُسخ الرّسائل التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها على النّظام تكون ملكاً للهيئة وتظّل كذلك.

11.1.2 نطاق العمل

تشمل هذه السّياسة:

1. جميع مرافق الاتّصالات الإلكترونيّة الخاصّة بالهيئةِ المحليّة .
2. جميع وظائف المراسلة بما في ذلك المراسلة الفوريّة.
3. جميع موظّفي الهيئة المحليّة الذين يستخدمون مرافق البريد الإلكتروني، أو أنظمة البريد الإلكتروني، أو وظائف المراسلة الخاصّة بالهيئة المحليّة لتخزين المعلومات أو إرسالها، بما في ذلك المعلومات العامّة والسريّة والمُقيّدة.

11.1.3 الهدف

حماية السريّة والسّلامة والتّوفر للمعلومات السّريّة والمُقيّدة التي يتم إنشاؤها، واستلامها، وإرسالها، وتخزينها عن طريق مرافق الاتّصالات الإلكترونيّة أو أنظمة البريد الإلكتروني، ووظائف المراسلة التّابعة للهيئة.

11.1.4 المسؤوليات

1) دائرة تكنولوجيا المعلومات والاتّصالات هي الجهة الرّئيسة المسؤولة عن سلامة رسائل الاتّصالات الإلكترونيّة.
2) يتّحمل كلّ مديرٍ، ورئيسِ دائرةٍ، والموظفين مسؤوليّة التّأكد منْ أنّ استخدام نظام البريد الإلكترونيّ للهيئة يتوافق مع الإرشادات الموضّحة في هذه السّياسة.
3) يتّحمل كلّ موظفٍ مسؤوليّة الالتزام الدّقيق ببروتوكولات هذه السّياسة لضمان السّلامة الكاملة لمعلومات الهيئة المحليّة.

11.2 السياسات والإجراءات

11.2.1 حسابات البريد الإلكتروني

1. لا يُمنح حقّ الوصول إلى شبكاتِ الهيئة المحليّة، أو أنظمتها إلا للموظفين الذين لديهم حاجة مشروعة.
2. كلما أمكن يقتصر الوصول إلى نظام البريد الإلكترونيّ الخاصّ بالبلديّات على الوظائف والبيانات الضّرورية للموظفين للوفاء بمسؤولياتهم الوظيفيّة وفقاً **لسياسة أمن المعلومات**.
3. يحق لجميع المستخدمين استخدام حساب مجالٍ واحدٍ، أو تسجيل دخول مجالٍ واحد، بالإضافةِ إلى ذلك قد يتم منح المستخدمين حقّ استخدام حسابات التّطبيقات الأخرى على أساس الحاجة.
4. يجب عدم مشاركة الوصول إلى هذه الحسابات مع أيّ مستخدمين آخرين.

5. يجب أنْ يكون كلّ حسابٍ فريدٍ للمستخدم الفردي.
6. وفقاً **لسياسة تغيير كلمة المرور**، يجب أنْ تكون الحسابات مُطابقة للاسم الأول والأخير كلّما كان ذلك ممكناً.
7. وفقاً **لسياسة تغيير كلمة المرور** يجب تعطيل حسابات المستخدم على الفور حال تركه وظيفته في الهيئة المحليّة.
8. يتطلب من مسؤول دائرة تكنولوجيا المعلومات والاتصالات إجراء مراجعاتٍ ربعِ سنويّةٍ لمعرّفات المستخدمين والامتيازات المرتبطة بحسابٍ ما، ولا سيما حسابات مستخدمي iMAL أو ما شابهه من الأنظمة.
9. يتعيّن على مسؤولي الدّوائر تزويد مسؤولي النّظام بقائمة منْ الحسابات النَّشطة والامتيازات المرتبطة بها كلّ ثلاثةِ أشهرٍ.
10. حيثما أمكن يجب دمج التّطبيقات في الدّليل النَّشط "Active Directory" لأغراض إدارة الهويّة وتوفير كلمة المرور.

11.2.2 الاستخدام المقبول لنظام البريد الإلكتروني الخاص بالهيئة المحلية

يُتاح استخدام حسابات البريد الإلكترونيّ "Email" الصّادرة عن الهيئة المحليّة لتسهيل أعمال الهيئة المحليّة وبناءً على ذلك، فإنّ أنظمة البريد الإلكترونيّ الخاصّة بالهيئة المحليّة مخصّصةً للاستخدام الحصري للهيئة، وليس للتّواصل الشّخصي أو لأي أنشطةٍ أخرى غير ملائمة، ويُسمح بالاستخدام الشّخصي العَرَضي المتقطّع طالما:

1. لا يستهلك إلا قدراً ضئيلاً من موارد النّظام كما يحدده مسؤول الدّائرة ومدير عام الهيئة.
2. لا يؤثر على إنتاجيّة الفرد (المرسل والمستقبل كليهما).

11.2.3 إشعار البريد الإلكتروني

يجب أنْ يكون إشعار التّحذير جزءاً من توقيع البريد الإلكترونيّ لجميع رسائل البريد الإلكترونيّ الصّادرة والموجّهة إلى المستلمين الخارجيين، ويجب أنْ يتضمن إشعاراً بالسّرية بقصد التّأكيد على الحفاظ على سريّة أيّ معلوماتٍ غير عامّةٍ أو خاصّة قد يحتوي عليها البريد الإلكترونيّ، وكذلك إبلاغ أيّ مستلمٍ يتلقّى رسالة بالخطأ بالإجراءات التي يجب اتخاذها، ويتم تكوين الإشعار على خادم البريد الإلكترونيّ بشكلٍ تلقائيّ، متى كان ذلك ممكناً، بحيث لا يضطر المستخدمون إلى تضمين الرسالة كجزءٍ من توقيعات البريد الإلكترونيّ الشّخصيّة الخاصّة بهم.

11.2.4 إشعار المتعاقد "المصادر الخارجية"

في حال استخدام طرفٍ ثالثٍ، أو وجهةٍ خارجيّةٍ حساب بريد إلكترونيّ خاصّ بالهيئة المحليّة (بناءً على اتفاق مع الهيئة المحليّة)، يجب تضمين إشعار تحذير في توقيع البريد الإلكترونيّ لجميع الرسائل الصّادرة للإشارة إلى أنّها مرسلة عن موظفٍ غير تابعٍ للهيئة.

11.2.5 إعادة توجيه الرسائل

إدراكاً بأنَّ بعض المعلومات تكون مخصصةً لأفرادٍ محدّدين وقد لا تكون مناسبةً للتّوزيع العام، يجب على مستخدمي الاتصالات الإلكترونيّة توخّي الحذر عند إعادة توجيه الرّسائل. يُحظر إعادة توجيه المعلومات السّريّة الخاصّة بالهيئةِ المحليّة إلى أيّ جهةٍ خارج الهيئة المحليّة دون موافقة مسؤول الدّائرة، كما يُحظر إعادة التّوجيه الجماعي أو التّلقائي للرّسائل إلى أطرافٍ أو بريدٍ خارج الهيئة المحليّة، ويشمل ذلك إعادة التّوجيه التّلقائي للرّسائل من حسابٍ إلى آخر، ومن البريد الإلكترونيّ لدائرة تكنولوجيا المعلومات بالهيئة المحليّة إلى عناوين البريد الإلكترونيّ الشّخصيّة وغير التّابعة للهيئة.

يجب مراعاة ما يلي عند إعادة توجيه الرسائل:

1. يُحظر إعادة التّوجيه التّلقائي لرسائل البريد الإلكترونيّ منْ قِبل موظّفي الهيئة المحليّة إلى عناوين بريدهم الإلكتروني الشّخصيّة.
2. يُحظر إعادة توجيه رسائل البريد الإلكتروني الفردية التي تحتوي على معلوماتٍ سريّة ومُقيدة، أو الكشف عنها لموظف الهيئةِ المحليّة دون الحاجة إلى معرفتها، أو إلى أطرافٍ خارج الهيئةِ المحليّة، أو إلى مناطق الهيئةِ

المحليّة الأخرى ما لم تكن هناك حاجةٌ واضحة يقتضيها العمل للقيام بذلك، وحسبما يكون مسموحاً به أو لازماً بموجب القانون.

11.2.6 إرسال رسائل البريد الإلكتروني الآمن خارج الهيئة المحلية

1. يجب ألّا يتم إرسال رسائل البريد الإلكترونيّ التي تحتوي على معلوماتٍ سريّة أو مُقيدة "غير عامة" مُرسلة إلى أفرادٍ أو جهاتٍ خارج الهيئة المحليّة إلّا إلى عناوين البريد الإلكترونيّ الفردية أو الشّخصيّة التي يمكن التّحقق منها باستخدام إجراءاتٍ مناسبة كما هو موضّح **بسياسة تغيير كلمة المرور**.
2. ستقوم الهيئة المحليّة بتشفير عملياتِ إرسالِ رسائلِ البريد الإلكترونيّ التي تحتوي على معلوماتٍ إلكترونيّة أو غيرها من المعلومات غير العامّة الخاصّة بالهيئةِ المحليّة ، متى تمّ الاتفاق على ذلك منْ قِبل الهيئةِ المحليّة والمستلم، وحيثما كان ذلك ممكناً.
3. يجب اعتماد جميع حلول وأدوات التّشفير لتخزين أو إرسال رسائل البريد الإلكترونيّ التي تحتوي على معلوماتٍ إلكترونيّةٍ أو سريّةٍ ومُقيّدةٍ خاصّة بالهيئة المحليّة منْ قِبل دائرة تكنولوجيا المعلومات والاتصالات.
4. إذا لم يكن حلّ التّشفير متاحاً، فسيتم تأمين رسائل البريد الإلكتروني التي تحتوي على معلوماتٍ غير عامّةٍ مرسلةٍ خارج الهيئة المحليّة بوسائلٍ أخرى (مثل الحماية بكلمة مرور، وينبغي حينها تزويد مستلم البريد الإلكتروني بكلمة المرور عبر الهاتف).
5. يجب بذل الجهود لإزالة كميّة المعلومات غير العامّة، أو تقليلها في أيّ بريدٍ إلكترونيّ، ومن أمثلة ذلك إدراج رقم حساب جزئي فقط عوضاً عن رقم الحساب الكامل حتّى لا يتم تصنيف البريد الإلكترونيّ على أنّه "سريّ".
6. يجب على الموظف توخّي الحذر المعقول في معالجةِ رسائلِ البريدِ الإلكترونيّ والرّسائل الفوريّة بشكلٍ مناسبٍ حتّى لا يتم إرسالها عن غير قصدٍ إلى عناوين غير صحيحة.

11.2.7 استخدام أنظمة البريد الإلكتروني غير التابعة للهيئة

يُنصح الموظفون بشدّة بألا يستخدموا أيَّ أنظمةِ اتصالاتٍ غير تابعةٍ للهيئة. قد يؤدي استخدام أنظمة البريد الإلكترونيّ المستندة إلى الإنترنت، وكذلك تنزيل المرفقات من هذه الأنظمة إلى أنظمة الهيئةِ المحليّةِ إلى تعريض الهيئة المحليّة لمخاطر متزايدة ومواقف ضارّة، مثل تفشي الفيروسات أو الفيروسات المُتنقلة بما يسمح بتثبيت فيروس حصان طروادة كما هو موضّح **بسياسة إدارة المخاطر**، بالإضافة إلى ذلك فإنّ المعلومات المُخزّنة على أنظمة البريد الإلكتروني المستندة إلى الإنترنت ليست آمنة ويتم فحصها أحياناً بحثاً عن محتوى وكلماتٍ رئيسةٍ تُعرّض الهيئة المحلية لتهديداتٍ حقيقية.

11.2.8 محظورات أنظمة البريد الإلكتروني

1) يُحظر الاستخدام غير المصرَّح به أو غير الملائم أو الكشف عن "المعلومات السريّة" المُحدَّدة أو تعديلها أو إتلافها التي قد تؤثر سلباً على الهيئةِ المحليّة أو لا تؤثر سلباً عليها.
2) يُحظر انتحال شخصيّة موظفٍ آخر للوصول إلى صاحب حساب البريد الإلكتروني أو حسابات وظائف المراسلة.
3) لا يحق للموظفين استرداد أيّ رسائلِ بريدٍ إلكترونيّ غير موجهةٍ إليهم أو قراءتها.
4) لا يحقّ للموظفين استخدام أيّ كلمة مرورٍ، أو رمزٍ، أو الوصول إلى ملف، أو استرداد أي معلوماتٍ مخزنة، ما لم يُصرّح المشرف المناسب لهم بذلك.
5) يُحظر تزوير مصدر الرّسالة عن طريق تغيير أي معلوماتٍ تشير إلى المصدر الحقيقي للرسالة.
6) يُحظر استخدام أنظمة البريد الإلكترونيّ الخاصّة بالهيئة المحليّة أو وظائف المراسلة بطريقةٍ تنتهك أحكام **سياسة امن المعلومات** الخاصّة بالهيئة المحليّة .
7) لا يجوز استخدام البريد الإلكتروني وأنظمة المعلومات الأخرى بطريقةٍ قد تكون مزعجةً أو مسيئةً للآخرين أو ضارَّة بالرُّوح المعنوية. يُحظر أي إرسالٍ أو استخدامٍ للبريد الإلكترونيّ الذي يحتوي على إهاناتٍ أو أي رسالةٍ

قد يتم تفسيرها على أنّها مضايَقة أو تكون مسيئةً للآخرين، ويمكن أن تؤدي تلك الممارسات إلى اتخاذ إجراءٍ تأديبيٍّ مناسب يتضمن ما يصل إلى انهاء الخدمة.

8) ينبغي عدم استخدام نظام البريد الإلكترونيّ لاستدراج الآخرين لمشاريعٍ تجاريّةٍ، أو قضايا سياسيّةٍ أو أمورٍ شخصيّةٍ أخرى لا علاقة لها بوظائفهم.
9) يجب ألا تحتوي رسائل البريد الإلكترونيّ على أيّ موادٍ يمكن اعتبارها مسيئةً أو مزعجةً أو تنطوي على تشهير أو تحط من قدر أيّ موظّفٍ، أو الهيئة المحلية، أو جهاتٍ خارجيّة.
10) يُمنع استخدام نظام البريد الإلكترونيّ بشكلٍ يخالف أيَّ قانونٍ فلسطينيّ، أو أيّ قوانين تابعة لهيئات فلسطينية أخرى.

11.2.9 الاحتفاظ بالبريد الإلكتروني

لا يوجد حاليّاً في دولة فلسطين قوانين خاصّةٍ بالسّجلات الوطنية لفرضِ وقتٍ محدَّد للاحتفاظ برسائل البريد الإلكترونيّ، ومع ذلك يُنصح بشدة باتّباع إجراءٍ مُحدّدٍ للتّعامل مع هذه السّجلات بناءً على "قيمتها" ولا يجوز التّخلص من رسائل البريد الإلكتروني التي تندرج تحت الفئات التّالية، ويجب الاحتفاظ بها إذا كانت:

1. تُعد دليلاً على معاملاتِ الهيئة المحليّة.
2. تُقرّ إجراءً، أو تُصرّحُ بفعلٍ، أو تحتوي على إرشاداتٍ أو مشورةٍ أو توجيهٍ.
3. تتعلق بالمشاريع والأنشطة الجارية وأصحاب المصلحة الخارجيين.
4. تُمثل عملاً رسميّاً.
5. تتضمن تواصلاً بين الموظفين، أو تحتوي على قراراتِ السّياسة.
6. إذا كانت اتصالات البريد الإلكترونيّ تحتوي على بياناتٍ يمكن اعتبارها جزءاً من سجل العميل، فسيحتفظ موظف الهيئةِ المحليّة بالاتصالات في سجلّ النّظام.

وبخلاف ذلك:

1. وفقاً **لسياسة النّسخ الاحتياطي**، ستقوم الهيئة المحليّة بحذف رسائل البريد الإلكترونيّ المُخزّنة في حسابات المستخدمين تلقائيّاً بعد فترةٍ زمنيّةٍ محددةٍ يوافق عليها مجلس الهيئة المحليّة .
2. إذا كانت هناك حاجة إلى الاحتفاظ باتصالات البريد الإلكترونيّ التي تحتوي على أيّ معلوماتٍ خاصّةٍ بالهيئة المحليّة إلى ما بعد فترة الحذف التّلقائي للبريد الإلكترونيّ، فيجب على موظّف الهيئة المحليّة حفظ الرّسائل بوسائلٍ أخرى (مثل الأرشفة، والنّسخ، واللّصق في مستنداتٍ أخرى أو الطّباعة).

11.3 حذف رسائل البريد الإلكتروني المُريبة

لتقليل فرصة إصابة بيئة تكنولوجيا المعلومات والاتصالات بفيروس، يجب على الموظّفين حذف أيّ بريدٍ إلكترونيٍّ يحتوي على مرفقٍ يبدو مريباً حذفاً نهائيّاً. قد لا تحتوي رسالة البريد الإلكترونيّ المُريبة على موضوعٍ أو قد تتضمن موضوعاً غيرَ متعلقٍ بالعمل، وغالباً ما تأتي من مصدرٍ غير معروف.

11.4 ملكية المعلومات

جميع المعلومات التي ينشئها الموظفون أو الاستشاريون في أي مشروعٍ تابعٍ للهيئة هي ملكٌ للهيئة، وستتولى الهيئة المحليّة حمايتها باعتبارها معلوماتٍ سريّةٍ وغير مُعلنَةٍ كما هو منصوصٌ عليه في **سياسة الأمان الرّقمي وعليه:**

1. يجوز للهيئةِ في أيّ وقتٍ وبدونِ إشعارٍ أو موافقةٍ من الموظف، الوصول إلى البريد الإلكتروني للموظف ومعلومات وظيفة المراسلة المُخزّنة في أنظمة الهيئة المحليّة .

2. تحتفظ الهيئة المحليّة بالحقّ في الوصول إلى نظام البريد الإلكترونيّ دون إشعار، ويجب ألا يفترض الموظفون والجهات الخارجيّة أنَّ أيّ معلوماتٍ، بما في ذلك الرّسائل "المحذوفة"، هي معلوماتٍ خاصّة.
3. يجوز للهيئةِ في أيّ وقتٍ ودون إشعارٍ أو موافقةٍ من الموظّف، حذف رسائل البريد الإلكترونيّ التي تعتقد الهيئة المحليّة أنّها تشكّل تهديداً لسريّة أو سلامة أو توفر المعلومات السّريّة والمُقيدة للهيئة أو أنظمة وأجهزة حواسيب الهيئة المحليّة ، أو تنتهك سياسة الهيئة المحليّة، ويشمل ذلك رسائل البريد الإلكترونيّ الخاطئة أو رسائل البريد الإلكترونيّ التي يُعتقد أنّها بريدٌ عشوائيّ أو رسائل البريد الإلكترونيّ التي يُعتقد أنّها تحتوي على فيروسات كمبيوتر أو برامجٍ ضارّةٍ أخرى.

11.5 تعليمات إضافية في حال عدم الامتثال

تحتفظ الهيئة المحليّة بالحقّ في تعليق وصول المستخدم أو إزالتِه بشكلٍ دائمٍ إلى بعض خدمات الاتصالات الإلكترونية المحددة في هذه السّياسة أو كلها، ويتعين على أي مستخدمٍ تمّ تعليق صندوق بريده التّشاور مع مسؤوله أو رئيس الوحدة، ووفقاً لخطورة الانتهاك، يلزم استشارة مدير الهيئة المحليّة أيضاً قبل إعادة حساب البريد الإلكترونيّ، وحينها يصدر رئيس الوحدة إذناً كتابيّاً لدائرة تكنولوجيا المعلومات والاتصالات لإعادة الحساب. تحتفظ الهيئة المحليّة كذلك بالحقّ في مراجعة، وتدقيق، واعتراض، والوصول إلى، ومراقبة، وحذف، والكشف عن جميع الرّسائل التي يتم إنشاؤها أو استلامها أو إرسالها أو تخزينها على نظام البريد الإلكتروني لأيّ غرضٍ من الأغراض. ومن خلال استخدام الموظف لنظام البريد الإلكترونيّ الخاصّ بالهيئة المحليّة، يُقرّ بحقوق الهيئة المحليّة السّالفة الذّكر ويوافق عليها.

11.6 السياسات ذات الصلة

1. سياسة أمن المعلومات.
2. سياسة النسخ الاحتياطي.
3. سياسة إدارة المخاطر.
4. سياسة تغيير كلمة المرور.

12. سياسة اصطلاحات تسمية الأجهزة

12.1 المقدمة والأهداف

12.1.1 بيان السياسة

حماية بيانات الهيئة المحليّة هي مسؤوليّة جماعيّة في الهيئة المحليّة، فعندما تصبح أجهزة الكمبيوتر التي توجد عليها البيانات مخترقة أو لا تعمل بطريقةٍ ما، يجب اتخاذ خطوات لتحديد موقع النّظام إمّا لإصلاحه أو لعزله عن بقيّة الأنظمة على الشّبكة حتّى يتم إصلاح الجهاز أو معالجة الخلل، وحتّى يتم الوصول إلى الجهاز بسرعةٍ لإصلاحه يجب أن يتم العرف عليه، وتحديد موقعه مع تحديد المستخدم والأشخاص الذين سيقومون بتقديم الدّعم التّقني، إنّ وضع ميثاق قياسيّ لتسمية الأجهزة يسمح بالتّعرف على الجهاز بسهولة.

12.1.2 نطاق العمل

1) جميع الموظفين المسؤولين عن إدارة أصول الحوسبة الخاصّة بالإدارات وخاصّةً أجهزة الكمبيوتر المكتبية وأجهزة الحوسبة المحمولة.
2) جميع الموظفين المسؤولين عن الحفاظ على السريّة والنّزاهة وتوفر الأصول على شبكة الهيئة المحليّة.
3) هذه السّياسة ملزمة عند شراء أي أجهزة نظامٍ جديدة وستتم تطبيقها على كل نظامٍ يتم استلامه وتهيئته بواسطة الموظّفين الفنيين في قسم تكنولوجيا المعلومات والاتّصالات.
4) يوصى بتنفيذ المعايير المحددة بهذه السّياسة على جميع الأنظمة الحاليّة.

12.1.3 الهدف

تهدف سياسة ميثاق تسمية الأجهزة على مساعدة قسم تكنولوجيا المعلومات والاتصالات على وضع نظام تسمية معياري لأصول تكنولوجيا المعلومات والاتصالات بحيث يكون مقروء، قابل للتوسع، وموحدة وتطبق على جميع الأصول ويسمح بتحديد تلك الأصول بشكلٍ سريعٍ وإيجابيّ حتى تتم خدمتها و\أو المحافظة عليها في الوقت المناسب.

12.1.4 المسؤوليات

1) تعتبر دائرة تكنولوجيا المعلومات والاتصالات مسئولة عن تنفيذ هذه السياسة.
2) إن وحدة إدارة الأصول أو من يقوم بدورها مسؤولة عن التأكد أن جميع أصول الهيئة المحلية لديها رقم تعريفي على أن يشمل بشكل إلزامي 6 أرقام في نهاية التعريف. مثلا: اسم الهيئة المحلية – 112456 أو اسم الهيئة المحلية -xxx- 112456
3) تقوم دائرة تكنولوجيا المعلومات والاتصالات بتقديم الإرشادات لتطبيق هذه السياسة.

12.2 السياسات والإجراءات

12.2.1 المعايير الأساسية

1) تضع هذه السّياسة مجموعة أساسيّة من المعايير لتحديد أيّ من المعلومات التي يجب أن تتضمنها أسماء المضيفين لتمكين فريق العمليّات لقراءة اسم الجهاز وفهم مكان الجهاز، وما يفعله الجهاز، ومدى أهميته، ونوع الجهاز .
2) بعض الأنظمة لها متطلبات محددة لاتفاقيات التّسمية، على سبيل المثال: لا يسمح Active Directory بأسماء الأجهزة التي تزيد عن 15 حرفاً، وبعض الأنظمة بها مشاكل في الأحرف الخاصة. في القسم التالي سنتأكد من أن الاسم صالح مع النّظام الذي نقترح أن تستخدمه الهيئة المحليّة مع الأخذ في الاعتبار أنّ اصطلاحات التّسمية الفعّالة يجب أن تكون عملية وقابلة للتّطوير.
3) تعليمات **المتطلبات الإلزاميّة:** لضمان إمكانيّة التّشغيل البيني مع سجّلات الهيئة المحليّة، نقترح استخدام الأحرف والأرقام فقط. يجب أن يكون لكلّ اسمٍ من أصول تكنولوجيا المعلومات والاتصالات مرتبط بهذه السّياسة الهيكل التّالي:

أ. **إجراء إلزامي - موقع (ملكية) الجهاز**: أول ثلاثة (3) أحرف لتعريف القسم التّابع له الجهاز مثل (الاختصارات المكونة من ثلاث خانات) كأول ثلاثة (3) أحرف من الاسم (إلزامي) مثل اسم القسم (acc) للمحاسبة.

ب. **إجراء اختياري:** يمكن استخدام الأحرف الستة (6) التّالية من الاسم (المواضع من الرابع إلى التاسع) وفقاً لتقدير القسم، أو عدم استخدامها على الإطلاق مثل :

i. مستوى خدمة الجهاز (dev، qa، prod) فيصبح على سبيل المثال: acc-p.
ii. دور الجهاز (web, database, mq) الآن أصبح لدينا التّالي: acc-pweb.
iii. يضاف رقم تسلسلي مكون من رقمين / ثلاثة أرقام للتعامل مع خوادم متعددة فيصبح لدينا: acc-pweb01 ، أو يمكنك استخدام الاختصارات التّالية من جامعة واترلو:

- **DC**: Domain Controller
- **FS**: File Server
- **PS**: Print Server
- **ORA**: Oracle database
- **SQL**: SQL database
- **DB**: other database(s)
- **EXH**: Microsoft Exchange
- **CTX**: Citrix Server
- **ESX**: VMware ESX Server

يمكن أن تتضمن أسماء المضيفين معلومات أخرى مثل اسم الخدمة ونوع الجهاز (على سبيل المثال المادية مقابل الافتراضية)، والتي تساعد في توفير معلومات حول الجهاز،مراجعة الافتراضية توصي بما يلي :

- **V**: (Virtual)
- **C**: (Cluster server)
- **P**: (Physical)
- **O**: (Outsourced or vendor supported system)

ج. **إجراء إلزامي- نهاية التعريف الخاص**: يجب أن تكون المواضع الستة (6) المتبقيّة هي الأرقام الست الموجودة في نهاية التّعريف الخاصّ بهذا الجهاز، ولتحسين إمكانيّة قراءة اسم الجهاز، يمكنك استخدام محدد لفصل موقع الجهاز عن تفاصيله الأخرى إذا كانت أنظمة الهيئة المحليّة تسمح بذلك.

ح. المحدد القياسي لفصل الجزء الأول من الاسم (الموقع ، النوع ، الدور) عن الجزء الثاني (المعرف الفريد) هو شرطة (-)وفي حالة عدم دعم نظام الهيئة المحلية للشرطة، يمكنك استخدام حرف قياسي آخر مثل $ أو # أو ببساطة تجاهل المحددات تماماً.

مثال:
قسم – محاسبة.
معرف القسم - Acc001.
مستوى الخدمة: الإنتاج.
دور الجهاز: الويب.
نوع الجهاز: Virtual.
رقم تعريف.
الجهاز: بلدية الخليل – 112456.

الأسماء المقبولة :
- Accpweb01-112456

- Acc00-112456
- Acc112456
- Accvir-112456

12.2.2 الإجراء - نظام جديد

عند استلام نظام جديد تم شراؤه حديثاً إلى الهيئة المحليّة، يجب تسليمه إلى قسم تكنولوجيا المعلومات والاتصالات ليتم تهيئته بصورة كاملة (نظام التّشغيل، الصورة، إلخ) وبطريقة مشفّرة وضمها إلى مجال الدّليل النّشط للهيئة. سيقوم قسم تكنولوجيا المعلومات والاتصالات بتعيين اسمٍ للجهاز وإنشاء حساب الدّليل النّشط المرتبط بالجهاز بحيث تشمل جميع أسماء الأجهزة ثلاثة (3) خانات تؤخذ من اسم القسم وأخر ستة (6) أرقام من رقم علامة معرف الجهاز، هذه الأسماء تفي بالمعايير المنصوص عليها في المتطلبات الإلزامية أعلاه.

12.2.3 الإجراء - الأنظمة القائمة

من المستحسن إعادة تسمية الأنظمة المستخدمة حاليّاً في الهيئة المحليّة . يجب أن تفي هذه الأسماء الجديدة بالمتطلبات الإلزامية الموضّحة سابقاً (إلزامية أول ثلاثة (3) وستة (6) أحرف) لكلٍّ من الجهاز وحساب الدّليل النّشط.

12.2.4 ملاحظات خاصة

1. **يجب أن يكون الاسم فريداً**: اصطلاح التّسمية الذي يسمح بالتّكرارات غير مجدي. استخدم جدول بيانات أو لوحة نصية لتحديد الأسطر المكررة في قائمة أسماء الأجهزة.
2. **تحقق من أنّ الاسم أبجدي رقمي** (إذا لزم الأمر): في الحالات التي لا تدعم فيها أنظمة الهيئة المحليّة الأحرف غير الأبجدية الرقميّة، قد تضطر إلى إزالة المحددات والأحرف الخاصة الأخرى.
3. تحقق من **عدم احتواء الاسم على مسافات**: تسبب المسافات مشاكل مع معظم الأنظمة.

12.3 السياسات ذات الصلة

1) سياسة شراء أصول تكنولوجيا المعلومات.
2) سياسة أمن المعلومات.

13. سياسة عنونة برتوكول الإنترنت

13.1 المقدمة والأهداف

13.1.1 السياسة

إنَّ الهيئة المحليّة مسؤولة عن حماية البنيّة التّحتيّة، وشبكات وأنظمة المعلومات، وكذلك البيانات التي تملكها، وكلّما زاد حجم الشّبكات والخدمات المقدَّمة من خلالها فإنّ ذلك يزيد التّحديات ويتطلب استثماراً أكبر، وإدارة أفضل، وتحسين مستمر، ورقابة مستمرة لتدفق البيانات عبر الشبكات. هذه السّياسة تقدم الأساس لتوجيه عمليّة إدارة وتطوير الشّبكات والممارسات المتعلقة بها في الهيئة المحليّة .

13.1.2 النطاق

تحدد هذه السّياسة المتطلبات والأدوار والمسؤوليات لحماية شبكة المعلومات في الهيئة المحليّة، وتقدم توجيه وأساس لتتبعه دائرة تكنولوجيا المعلومات ويشمل المجالات التالية:

1. التّأكد من وجود الدّعم الفنّي الكافي والمناسب الذي يغطِّي أنشطة وأعمال الهيئة المحليّة بشكلٍ كافي بما يسمح بتقديم الخدمات بشكلٍ فعّال.
2. ضمان توافرٍ عالي للخدمات الإلكترونيّة بشكلٍ دائم.
3. حماية الشّبكة من الدّخول غير المسموح به.
4. حماية الشّبكة من الأعطال العرضية.
5. حماية سريّة البيانات.
6. تصميم وتخطيط وإدارة وضبط أمن المعلومات على الشّبكة.
7. إدارة الوصول والدّخول للشّبكات والأنظمة الإلكترونية.
8. تسجيل عمليات الدّخول للشبكات والأنشطة المختلفة عليها، وضمان القدرة على تدقيق ذلك.

13.1.3 الهدف

تحسين إدارة وتنظيم شبكات المعلومات وأمنها لتخفيض مخاطر أعطال الأنظمة، وضعفها، والثّغرات والهجمات الإلكترونيّة.

13.1.4 الأدوار والمسؤوليات

1. **فريق الشّبكات والأنظمة بدائرة تكنولوجيا المعلومات:**
   أ. تعريف مجموعات المستخدمين والأدوار المناسبة لدعم التّحكم في الوصول المستند إلى الأدوار.
   ب. تدقيق المستخدمين وقوائم الوصول بشكلٍ منتظم للتّأكد من تحديد محاولات الدّخول غير المصرَّح بها ومحاولات استخدام شاذّة لحسابات مستخدمين لهم صلاحيّات مميزة على الأنظمة والشّبكات.
   ت. القيام بالمراجعات السّنوية للسّياسات والإجراءات.
   ث. إنشاء وصيانة الإجراءات، وتوثيق كافّة إعدادات الشّبكة وأمن المعلومات.
   ج. مراقبة وتحليل تدفق البيانات عبر الشّبكة للحصول على مستويات الأداء والأمن المثلى.

2. **جميع المستخدمين للشبكات:**
   أ. التّصرف بمسؤوليّة في جميع الأوقات وإدراك مخاطر انتهاك هذه السّياسة، بما في ذلك الإجراءات التأديبيّة المحتملة.

3. **مسؤول دائرة تكنولوجيا المعلومات:**
   أ. اعتماد السّياسة ومتابعة وضع المشاريع والإجراءات التي تهدف إلى الامتثال لهذه السّياسة.

4. **المدير العام للهيئة:**
أ. الاعتماد النّهائي لهذه السّياسة.

13.2 السياسات والإجراءات

13.2.1 تجزئة الشّبكة وعزلها

1. يجب أنْ تحدد تجزئة الشّبكة بناءً على وظائف الأنظمة وحساسيّة البيانات التي تخزنها وتعالجها وتنقلها، على سبيل المثال: يجب وضع الأنظمة التي تتطلب اتصالاً بالإنترنت في منطقة محميّة (DMZ) مفصولة ومعزولة عن الأنظمة الأكثر حساسيّة.
2. يجب فصل شبكات الخوادم عن شبكات المستخدمين.
3. يجب وضع خوادم قواعد البيانات في منطقة منفصلة عن خوادم التّطبيقات الأماميّة (front-end) باستخدام تصميم شبكة متعددة المستويات (multitier). يمكن استخدام شبكات VLAN لفصل الأنظمة ومجموعات المستخدمين، مما سيوفر حماية أكثر كفاءة.
4. سيؤدي تجزئة الشّبكات وعزلها إلى تحسين أداء الشّبكة وأمنها وتقليل آثار المخاطر المختلفة، مثل: الأخطاء البشريّة.
5. يوصّى بتجزئة وعزل مجموعات خدمات، والمستخدمين، وأنظمة المعلومات على الشّبكات. يجب تنفيذ التّوصيات التّالية من ISO 27001 و ISO 27002 على الأقل:

أ. تجزئة الشّبكات الكبيرة إلى أجزاء.
ب. اعتماد الفصل المادي والمنطقي عند تجزئة الشّبكات.
ت. تعريف حدود الأجزاء المختلفة للشبكات.
ث. تحديد قواعد تدفق البيانات بين أجزاء الشّبكة.
ج. استخدام المصادقة والتّشفير وتقنيات التّحكم في الوصول إلى الشّبكة على مستوى المستخدمين.
ح. النّظر في تكامل شبكة الهيئة المحليّة أجزائها مع تلك الخاصّة بالشّركاء (في حال وجود اتصال بين شبكة الهيئة المحليّة وشبكات شركات آخرين)

13.2.2 تصميم الشبكات

يجب اعتبار المفاهيم التّالية عند تصميم الشّبكات:

1. التّصنيف: يجب فصل الأنظمة المصنّفة حسب تصنيف سياسة أمن المعلومات (راجع السّياسة للتصنيف: عام أو داخلي أو سري وكذلك سياسة إدارة المخاطر).
2. مناطق الأمان: منطقة الأمان هي مجموعة من واجهات الشّبكة تشمل واجهة أو أكثر من الجدار النّاري (firewall) ومجموعة واجهات أخرى على الشّبكة المتصلة بها. يتم تحديد مستويات الحماية والضّبط لكل منطقة على حدى، بحيث تتلقى كل منطقة مستويات الحماية المناسبة وفقاً لتصنيف البيانات والمصادقة التي تتطلبها والتجزئة التي تحتاجها وحساسيّة بياناتها.
3. إدارة العناوين على الشبكة IP: يعزز مخطط عنونة IP المنَّظم بشكلٍ جيّد القدرة على التّعرف بسرعة على خصائص الأجهزة على الشبكة من العنوان IP وهذا يساعد في:
أ. إدارة الشّبكة واكتشاف الأخطاء وتصحيحها.
ب. تعريف محيط الشّبكة المحدّدة وحدودها.
ت. وضع قواعد وضوابط تدفق البيانات على الشّبكة.
4. يتم تحديد نطاقات عناوين IP الداخلية من قبل فريق الشبكة والأنظمة.
5. يجب استخدام DHCP لتخصيص عناوين الشّبكة IP الديناميكيّة لأجهزة الكمبيوتر والأجهزة الطرفية للمستخدمين.

6. **كوابل التوصيل وألوانها**
يجب أنْ يكون هناك فصل بين الدّوائر الكهربائية، والإلكترونيّة، والأجهزة، وكابلات المعدّات، والموصلات، والأنظمة المتّصلة بها.

7. حفظ **البيانات مركزياً**
يجب أنْ تقوم دائرة تكنولوجيا المعلومات بإنشاء مجمع مركزي لبيانات الشّبكات وعناوين IP والبروتوكولات والأجهزة، وهذا أمر بالغ الأهمية للتمكن من الحفاظ على التّحكم في الشّبكة بشكلٍ فعّال. سيكون هذا مجمع واحد وهذا يشمل الشّبكات وأجهزة المستخدمين والخوادم والأجهزة التي لا تتطلب اتصال دائم بالشّبكة أو يتم اتصالها لفترات محدودة ومتغيرة، والبيئات الافتراضية كذلك. سيمكّن ذلك القدرة على البحث عبر كل هذه المعلومات وتتبع التغييرات على الشّبكة بسرعة واستكشاف المشكلات وإصلاحها بسرعة عند ظهورها. بالإضافة إلى ذلك، تساعد البيانات عن الأعمال المرتبطة بالشّبكة ومواردها على الرّبط بين شبكة التّواصل المنطقي للأعمال وموارد تكنولوجيا المعلومات.

8. **تقييم المخاطر**
يجب أنْ يعتبر تقييم المخاطر أداة أساسيّة في هندسة وتصميم الشّبكات، ويجب أنْ يتم تحديد المخاطر، وتحليلها، وتقييمها، وضبطها من خلال تقنيات إدارة المخاطر (انظر سياسة إدارة المخاطر).

9. **بنية أمن المعلومات**
يجب مراعاة جميع متطلبات أمن المعلومات في تصميم الشّبكات وبنيتها بما في ذلك مبادئ تجزئة الشّبكة وعزلها وكذلك تصنيف الأنظمة وفق سياسة أمن المعلومات. تعمل بنية أمن المعلومات على تحقيق أقصى حد من كفاءة تصميم وتشغيل الشّبكات، بالإضافة إلى توفير ودعم متطلبات الأمان الأساسيّة لتصميم الشّبكة.

10. **تصنيفات وفئات أجزاء الشبكة**
تصنيف الأنظمة ضروري لجميع عناصر بنية الشّبكات وتصميمها وعملية توثيق الأنظمة. يجب استخدام نطاقات مختلفة لعنونة أجزاء الشّبكة مع التّحكم بقوائم الوصول بين الشّبكات المختلفة، ويجب استخدام جداران الحماية (firewalls) بين مناطق الشّبكة المختلفة. يجب وضع ضوابط أمن معلومات فعّالة بين الشّبكات.

11. **عناوين شبكة الهاتف**
يجب تعيين عناوين شبكات محليّة لشبكة الهاتف، لأنّها لا تتطلب اتصالاً مباشراً بالإنترنت.

13.2.3 الأمن المادي لشبكات المعلومات

1. يجب أنْ يتم استضافة موزّعات الشّبكة وأنظمة إدارتها وأنظمة إدارة منافذ الشّبكة في أماكن آمنة مع الأخذ بعين الاعتبار التّحكم بالوصول وتوفر أجهزة طاقة احتياطيّة UPS.
2. يجب الالتزام بما يلي فيما يتعلق بهذه الأماكن الآمنة:

أ. السّماح بالدّخول إلى الأماكن الآمنة التي تحتوي على معدات شبكة حرجة أو حسّاسة فقط لأولئك المصرَّح لهم بذلك.
ب. استخدام أنظمة وصول آمنة، مثل: بطاقات دخول، أو رموز سريّة.
ت. السّماح للزّوار أو مزودي الخدمات بالدّخول فقط إنْ وجد تصريح مسبق بذلك. يتم الاحتفاظ بقائمة المستخدمين المُصرَّح لهم بالدّخول ومراجعتها بشكلٍ منتظم.
ث. يمنع التّدخين والأكل والشُّرب في هذه الأماكن.

3. قبل منح أي زائرٍ أو طرفٍ ثالثٍ إمكانية الوصول إلى مناطق الشّبكة الآمنة، يجب أنْ يقوم بالتّوقيع على الامتثال لكافّة السّياسات ذات الصّلة مع التّوضيح لهم بمتطلبات أمن المعلومات.
4. يجب تسجيل الدّخول والخروج لجميع زوار مناطق الشّبكة الآمنة. سيحتوي السّجل على الاسم والمؤسسة والغرض من الزّيارة والتّاريخ ووقت الدّخول والخروج.

13.2.4 التحكم في الوصول إلى الشبكة

1. يتطلب الوصول إلى الشّبكة تسجيل دخول آمن.
2. سيتم إجراء تسجيل وإلغاء تسجيل وصول المستخدمين (من الموظفين) إلى الشّبكة من خلال نظام الموارد البشريّة في المقام الأول وذلك لإنشاء موظف / موظفين في المرحلة الأولى. ويطلب إذناً منفصلاً للوصول عن بعد إلى الشّبكة.
3. يتم منح حقوق الوصول إلى الشّبكة وفقاً لمتطلبات وظيفة المستخدم، وليس بناءً على تفضيل المستخدمين أو حاجتهم المتصورة.
4. يتم منح امتيازات التّحكم بالأمان، مثل('Power user' أو حقوق network administrator (مسؤول الشبكة)) للشبكة وفقاً لمتطلبات وظيفة المستخدم. يتم الاحتفاظ بقائمة هؤلاء المستخدمين بشكلٍ آمن ويتم مراجعتها بانتظام.
5. يجب أنْ يكون لجميع مستخدمي الشّبكة اسم مستخدم فريد وكلمة مرور (وذلك وفق سياسة الأمن الرّقمي).
6. يتحمّل المستخدمون مسؤوليّة ضمان الحفاظ على كلمات المرور الخاصّة بهم بشكلٍ آمن وعدم مشاركتها مع الآخرين (راجع سياسة الأمن الرقمي).
7. ستتم إزالة حقوق وصول المستخدمين أو مراجعتها ، بناءً على إشعار من الموارد البشريّة، وذلك للمستخدمين الذين يتوقف عملهم في الهيئة المحليّة .

13.2.5 معايير جدار الحماية

1. يُعرَّف جدار الحماية بأنّه أية أجهزة و / أو برامج مصممة لفحص مرور البيانات عبر الشّبكة باستخدام سياسات أو قواعد محددة وذلك لحظر الوصول غير المصرَّح به مع السّماح بالاتصالات المصرّح بها إلى أو من شبكة أخرى أو جهاز إلكتروني.
2. جميع جدران حماية الشّبكة (المادّيّة) التي تمّ تركيبها وتجهيزها، يجب أنْ يكون الإشراف عليها وتجهيزها من قِبل فريق الشّبكات والأنظمة.
3. يجب تسجيل جميع طلبات التّغيير على جدران الحماية لدى الدّعم الفنّي بدائرة تكنولوجيا المعلومات.
4. يجب توثيق كافّة التّغييرات التي يتم إجراؤها على إعدادات وقواعد جدران الحماية وتسجيلها.
5. يجب الاحتفاظ بجميع الوثائق ذات الصّلة من قِبل فريق الشّبكات والأنظمة وتخضع لمراجعة منتظمة.
6. يجب أنْ تتبنى جميع إعدادات جداران الحماية مبادئ "منح أقل الامتيازات" مع رفض جميع حركات المرور الواردة بشكلٍ افتراضي (يجب تعيين مجموعة القواعد ابتداءً على "وضع التّسجيل أو التّعلم" لمنع حدوث انقطاع في الخدمات). يتم التّعديل على مجموعة القواعد فقط بشكل تدريجي للسّماح فقط بمرور المسموح بها.
7. يجب تثبيت جدران الحماية داخل بيئات العمل الفعليّة ليتم فحص البيانات المحظورة وتقييدها، أو معالجتها، أو تخزينها للمساعدة في تحقيق الفصل الوظيفي بين خوادم الويب وخوادم التّطبيقات وخوادم قواعد البيانات.
8. يجب مراجعة إعدادات وقواعد جداران الحماية بشكلٍ سنوي وذلك للتّأكد من توفر مستويات الحماية المطلوبة.
9. يجب على فريق الشّبكات والأنظمة إجراء المراجعة والتوافق على جميع إعدادات وقواعد جداران الحماية عليها أثناء عمليّة التّشغيل الأولي لها.
10. يجب مراجعة جدران الحماية التي تحمي أنظمة الهيئة المحلية مرتين في السنة.
11. يجب على مسؤولي جداران الحماية الاحتفاظ بنتائج المراجعات لجدران الحماية والوثائق ذات الصّلة، جميع النتائج والوثائق تخضع لمراجعة منتظمة.
12. يجب إجراء نسخ احتياطي لإعدادات وقواعد جداران الحماية بشكلٍ متكرر إلى وحدة تخزين بديلة (ليست على نفس الجهاز). يجب الاحتفاظ بعدّة أجيال من النّسخ الاحتياطي والاحتفاظ بها من أجل الحفاظ على سلامة البيانات من التّغيير. عند استعادة النّسخ الاحتياطيّة، يجب أن يقتصر الوصول إلى إعدادات وقواعد ووسائط النّسخ الاحتياطي على المسؤولين عن إدارة جدران الحماية ومتابعتها.
13. يجب حفظ سجلات إدارة جداران حماية الشّبكة (التي تشمل الأنشطة الإدارية) وسجلات الأحداث (التي تظهر نشاط مرور البيانات) في وحدة تخزين بديلة (وليس على نفس الجهاز) ويتم مراجعتها بانتظام.
14. يقوم فريق الشّبكات والأنظمة بتنفيذ التغييرات المعتمدة على إعدادات وقواعد جدران الحماية نيابةً عن الهيئة المحليّة .

أ. الشبكات السلكية

1. يجوز توصيل المعدات المملوكة للهيئة فقط بالشّبكة السّلكية، وهذا يشمل خدمات الشّبكة المقدّمة لجميع مباني الهيئة المحلية .

2. أجهزة الكمبيوتر الشخصيّة غير مسموح بها على الشّبكة السّلكية بدون طلبات رسميّة يتم تسجيلها والموافقة عليها من طرف دائرة تكنولوجيا المعلومات. توفر الهيئة المحليّة شبكات لاسلكية مخصّصة لاتصال الأجهزة المتنقلة بما يشمل أجهزة الكمبيوتر المحمولة وأجهزة الموبايل والأجهزة الذّكية.
3. يحظر استخدام عناوين الشّبكة بخلاف تلك التي تقدمها دائرة تكنولوجيا المعلومات.
4. يقتصر الوصول إلى معدات الشّبكات في مراكز البيانات وغرف الاتصالات على موظفي دائرة تكنولوجيا المعلومات والموظفين المرَّخص لهم فقط.
5. يمكن توصيل جهاز واحد فقط بأي منفذ شبكة سلكي. لا يجوز توصيل أي موزعات (hubs, switches) أو نقاط وصول لاسلكية (access points) أو أجهزة توجيه (routing devices)، بشكلٍ مباشر أو غير مباشر دون الحصول على موافقة مسبقة من دائرة تكنولوجيا المعلومات.
6. يحق لفريق الشّبكات والأنظمة الحد من سعة الشّبكة أو تعطيل اتصالات الشّبكة التي تؤثِّر على نطاقها (bandwidth)، وذلك حيثما كان ممكناً، واعتماداً على شدّة الحادث، يتم القيام بذلك بالتفاوض مع الوحدات المتأثرة في الهيئة المحليّة .
7. لا يجوز لأي فرد توصيل أجهزة بشبكة الهيئة المحليّة السّلكيّة قد توفر وصول غير مرخص به لمستخدمين أو توفر عناوين IP غير مرخَّص بها.

ب. الشبكات اللاسلكية

على الهيئة المحليّة إنشاء شبكة لاسلكية مؤمنة ومخفية عبر مبانيها لاستخدام موظفيها. يتم توفير شبكة لاسلكية آمنة أخرى للزّوار منفصلة تماماً عن شبكة الهيئة المحليّة. تكون معايير أمن الشّبكات اللاسلكية كما يلي:

1. **طبقة الوصول**: سيتصل المستخدمون بشبكة WLAN عبر نقاط الوصول (access points)، والتي ستوفر معيار اتصال 802.10n / g للأجهزة.
2. **معرّف مجموعة الخدمة**، سيتم تحديد SSID للشّبكات اللاسلكية للهيئة بواسطة دائرة تكنولوجيا المعلومات وسيكون بتنسيق "اسم الهيئة المحلية " - خاص لشبكة الموظفين و "اسم الهيئة المحلية " - الزوار للزوار.
3. قد يوفر فريق الشّبكات والأنظمة لمزودي الخدمات والدّعم الفنّي الوصول إلى شبكة الموظفين اللاسلكية إذا كان ذلك ضروريّاً لتمكينهم من تقديم الدّعم الفنّي.
4. **تستخدم شبكات WLAN** مستوى تشفير AES (Advanced Encryption Standard). يعتبر معيار التّشفير هذا إلزامي.
5. **يتم تجهيز الإعدادات** كي تدعم خدمة شبكات WLAN فقط WPA2 (الوصول المحمي بتكنولوجيا Wi-Fi) وهو معيار الأمان المنخفض.
6. **سيتم فصل الأجهزة غير** المرخص لها والمتصلة بالشّبكة اللّاسلكية بشكلٍ فوري ودون التّحذير قبل تنفيذ ذلك.
7. يحظر على الموظفين توصيل نقاط اتصال لاسلكية إضافية بشبكة الهيئة المحليّة .

ت. التحكم في وصول الطرف الثالث إلى الشبكة

1. يعتمد وصول الطّرف الثّالث إلى الشّبكة على التفويض المناسب والامتثال لجميع السّياسات ذات الصّلة.
2. فريق الشّبكات والأنظمة مسؤول عن ضمان عملية تسجيل وصول جميع الأطراف الثّالثة إلى الشّبكة.
3. قد يتم توفير الوصول إلى الإنترنت لموظفي الهيئة المحليّة أو الزوار أو المقاولين ومزودي الخدمات عبر مكتب الدّعم الفنّي.
4. قد تتم الموافقة على الاتصال بالبنية التّحتيّة المخصّصة لموظفي الهيئة المحلية عبر شبكة Wi-Fi بشرط تقديم طلب كتابي لإنشاء حساب محدد أو إجراء عمليّة التّسجيل الذاتي وفق الأنظمة.

ث. الاتصال بالشبكات الخارجية

1. يُسمح بالاتصال بالشّبكات الخارجيّة بناءً على متطلبات العمل بعد الحصول على طلب من الدّوائر المعنيّة، تقوم تكنولوجيا المعلومات باستقبال الطّلبات، وتحليلها، ويتم التّوافق على متطلبات الاتصال مع الجهة صاحبة الطّلب، ثمَّ تقوم بإرسال توصياتها إلى المدير العام للموافقة النّهائيّة.
2. دائرة تكنولوجيا المعلومات هي المسؤولة عن تنفيذ جميع الاتصالات بالشّبكات الخارجيّة التي تتصل بشبكات الهيئة المحليّة ، كما أنّها مسؤولة عن ضمان امتثال وتوافق الأنظمة والشّبكات الخارجيّة ذات الصّلة مع القوانين واللّوائح والسّياسات المعتَمدة.

3. دائرة تكنولوجيا المعلومات هي المسؤولة عن تسجيل وتدقيق الاتصال بالشّبكات الخارجيّة، مع المراجعة الدّورية لمتطلبات تلك الاتصالات.

13.2.6 صيانة الشبكة والنسخ الاحتياطي

1. يتابع فريق الشّبكات والأنظمة الحفاظ على عقود الصّيانة ومراجعتها بانتظام لجميع معدّات الشّبكة الأساسيّة.
2. مكتب الدّعم الفنّي مسؤول عن الاحتفاظ بسجل لجميع الأعطال على الشّبكة.

أ. يكون فريق الشّبكات والأنظمة مسؤول عن ضمان تسجيل إعدادات الشّبكات. يتم الاحتفاظ بتوثيق التّغييرات التي تتم على الشّبكة وتخزينها بشكلٍ آمن وإجراء النّسخ الاحتياطي لها بانتظام. يقوم فريق الشّبكات والأنظمة بما يلي:

ب. توثيق إجراءات عمليّات النّسخ الاحتياطي والتّأكد من معرفة الموظفين المعنيين بذلك.

ت. يتم توثيق إجراءات تخزين النّسخ الاحتياطيّة من أشرطة أو وسائط (tapes or media) وإبلاغها لجميع الموظفين المعنيين.

ث. التأكد من تخزين جميع وسائط النّسخ الاحتياطيّ بشكلٍ آمن وتخزين نسخة خارج الموقع.

ج. يتم توثيق إجراءات التّخلص السّليم والآمن من وسائط النّسخ الاحتياطيّ، وإبلاغها لجميع الموظفين المعنيين.

ح. يتحمل المستخدمون مسؤولية نسخ بياناتهم إلى الخوادم على الشّبكة باستخدام محرّكات الأقراص على الشّبكة.

خ. يتم تطبيق التّحديثات والإصلاحات على الشّبكة للمعالجة منْ قِبل فريق الشّبكات والأنظمة فقط باتباع سياسة إدارة التغيير المناسبة.

13.2.7 الحماية والهجمات الخبيثة

1. يعمل فريق الشّبكات والأنظمة على ضمان ما يلي:

أ. تم وضع تدابير لاكتشاف الفيروسات والبرامج الضّارة الأخرى وحماية الشّبكة.

ب. وجود رقابة مناسبة على حركة مرور البيانات على الشّبكة، والوصول إلى الشّبكة، وكشف التّسلل.

ت. يتم مراقبة الشّبكة بحثاً عن انتهاكات أمنية محتملة. ستمتثل جميع عمليات المراقبة للقوانين واللّوائح والسّياسات المعتمدة.

2. تحتفظ دائرة تكنولوجيا المعلومات بالحقّ في الوصول إلى جميع البيانات المخزّنة أو المنقولة عبر شبكة الهيئة المحليّة أو تعديلها أو حذفها كجزءٍ منَ الدّفاع عن الشّبكة ومتطلبات الأمن الرّقمي. يتضمن ذلك البيانات الشّخصية المخزنة في المجلدات على الشّبكة وصناديق البريد الإلكتروني وما إلى ذلك. يجب تخزين البيانات ذات الطّابع الشّخصي في مجلد محدد أو يسمى "شخصي". وهذا لا يمنع الوصول إلى هذا المجلد أو إزالته على مسؤولية دائرة تكنولوجيا المعلومات.

13.2.8 بروتوكول نقل البريد البسيط (SMTP)

أولا: يجب أن تستخدم جميع حركات مرور بروتوكول البريد الإلكتروني بوابات البريد المركزية.
ويجب استخدام سجلات الـ DNS MX لنقل حركة مرور البريد الواردة والتي تتضمن عناوين وجهة لخوادم غير تلك التي تقوم بتشغيلها "خدمات تكنولوجيا المعلومات" لنقل تلك الحركة عبر بوابات البريد المركزية. ويجب أنْ تستخدم جميع حركات المرور الصّادرة من بوابةSMTP .
ثانيا: يجب أنْ يكون الاتصال بين عميل البريد الإلكتروني وخادم البريد الإلكتروني من خلال معايير حماية الاتصال والمغادرة مثل SSL أو TLS بحيث تكون جلسة عمل المصادقة هي الحركة المحميّة.

13.4 السياسات ذات الصلة

1) **سياسة الدّعم التّقني.**
2) **سياسة أمن المعلومات.**
3) **سياسة إدارة المخاطر.**

14. سياسة تكامل البيانات والأنظمة الإلكترونية

14.1 المقدمة والأهداف

14.1.1 مقدمة السياسة

نسعى من خلال هذه السّياسة إلى وضع معيار لعمليّة تكامل البيانات بين الأنظمة المختلفة وضبطها بطريقة تمكّن من الوصول لحالة توازن ما بين التّأكد من استخدام أفضل الممارسات وفعاليّة الخدمات من ناحية، وبين متطلبات أمن المعلومات من ناحية أخرى. يجب تطوير النّماذج الخاصّة لتطبيق السّياسة.

14.1.2 الهدف

تهدف السّياسة إلى التّأكد من فعاليّة التّكامل بين الأنظمة والبيانات والاستخدام الفعّال لتدفق البيانات بشكلٍ يعزز من فعاليّة العمليّات، مع الحفاظ على سلامة البيانات من التّغيير، سلامة سرّيتها وتوافرها وكذلك الوصول إليها وذلك مع الالتزام بسياسة أمن المعلومات.

14.1.3 نطاق العمل

تطبق هذه السياسة على كافة البيانات وأنظمة المعلومات والموظفين ومزودي الخدمات.

14.1.4 الأدوار والمسؤوليات

1. **دوائر الأعمال:**
   أ. تقدّم طلبات تكامل البيانات بين الأنظمة.
   ب. تقوم باعتماد خطّة تطبيق تكامل البيانات التي تعدها دائرة تكنولوجيا المعلومات.
   ت. تقوم بعمليّات الفحص والمراجعة بعد تنفيذ الخطّة.
   ث. قد تُطلب تعديلات وتحسينات إضافيّة بناءً على الفحص والمراجعات.
   ج. الحصول على موافقة إدارة الهيئة المحليّة على الخطّة النّهائيّة، وذلك بعد الحصول على موافقة دائرة تكنولوجيا المعلومات.
2. **مسؤول دائرة تكنولوجيا المعلومات:**
   أ. دراسة طلبات تكامل البيانات المقدَّمة من دوائر الأعمال.
   ب. تحليل الطّلبات وتحديد متطلبات التّنفيذ والتّكلفة.
   ت. تشكيل فريق لتنفيذ الطّلب من دائرة تكنولوجيا المعلومات والدّوائر ذات العلاقة على أنْ يكون بقيادة دائرة التكنولوجيا.
   ث. متابعة تنفيذ الخطّة بعد الحصول على موافقة إدارة الهيئة المحليّة .
   ج. متابعة توفير الدّعم والتّحسينات وذلك بعد تنفيذ الخطّة.

14.2 السياسات والإجراءات

14.2.1 مفاهيم عامة

1. يتم تمثيل البيانات في جميع الأنظمة الإلكترونيّة التّابعة للهيئة بشكلٍ موحَّد حسب السّياسات المعتمدة.
2. تشمل عملية إدارة البيانات التّأكد من أنَّ حاجات مستخدمي البيانات يتمّ أخذها بعين الاعتبار عند تطوير أنظمة جديدة، أو التّعديل على أنظمة قائمة بما يشمل بنية البيانات، ومجالاتها وقيمها.
3. من مسؤولية مالك البيانات التّأكد من صحة البيانات وصحة قيمها.
4. يجب تحديد مالك البيانات عبر الأنظمة الإلكترونيّة المختلفة.
5. يجب أنْ يتم ضبط سلامة البيانات من التّغيير بالاعتماد على حاجات الأعمال والموظفين، فمثلاً قد يتم السّماح لموظف بتغيير بيانات تملكها دائرة أخرى بعد الحصول على موافقة وصلاحيات مسبقة.
6. يجب الاحتفاظ بسجل الوصول للبيانات، وكذلك التّغيير عليها بما يشمل تحديد النّظام الإلكترونيّ الذي تم تغيير البيانات من خلاله، ولا يسمح بمسح السّجل دون موافقة المدير العام المسبقة وعلم التّدقيق الدّاخلي.

7. يجب أنْ تأخذ عمليّة تكامل البيانات مبدأ منح الحدِّ الأدنى من الصّلاحيات، وكذلك الحدِّ الأدنى من الوصول للبيانات، هذا بالإضافة لمتطلبات أمن المعلومات الأخرى.
8. يجب الاحتفاظ بسجلِّ البيانات حول عناصر البيانات المستخدمة (metadata) في الهيئة المحليّة مع منح صلاحيّات الوصول للتّدقيق الدّاخلي ليتمكن من التّدقيق والمراجعة، وسوف يشمل ذلك تعريف عناصر البيانات والجوانب الفنيّة لها مع توضيح معناها وكيف يتم استخدامها ومن يقوم باستخدامها.
9. ترد طلبات التّغيير بما يتعلق بتكامل البيانات من دوائر الأعمال موقّعة من مسؤول الدّائرة المعنيّة. دراسة إمكانية تنفيذ الطّلبات تقع على عاتق دائرة تكنولوجيا المعلومات بعد الحصول على موافقة مالكي البيانات.
10. إذا كان تنفيذ الطّلب ممكن بناءً على رأي دائرة التّكنولوجيا، تقوم دائرة التّكنولوجيا بتحديد متطلبات تنفيذ الطّلب، وملخص الميتاداتا metadata للبيانات التي سيتم التّغيير عليها أو إضافتها صلاحيات الوصول التي يتطلب تغييرها البرمجيات المطلوبة، والدّعم الفنّي الخارجي إنْ وجدت الحاجة له، ومتطلبات أمن المعلومات. تقوم دائرة التّكنولوجيا بالمراجعة مع الدّوائر ذات العلاقة للحصول على موافقتها وتوقيعها لتقوم الدّائرة صاحبة الطّلب بعد ذلك برفع الطّلب بتفاصيله إلى المدير العام للحصول على الموافقة النّهائية والموازنات المطلوبة.
11. تقوم دائرة التّكنولوجيا بقيادة تنفيذ الطّلب وعمليات الفحص والمراجعة مع الدّوائر ذات العلاقة قَبل جعل التّغيير متاحاً للاستخدام في بيئة العمل.
12. التّغييرات التي يتم تنفيذها في مجال تكامل البيانات يجب ألّا تخل بالالتزامات التّعاقدية بين الهيئةِ المحليّة ومزودي الخدمات والدّعم الفنّي.
13. يجب أن تكون التّغييرات التي يتم تنفيذها ممتثلة للقوانين والسّياسات والمعايير المعتمدة.
14. في حالة تكامل البيانات بين أنظمة داخلية مع أخرى خارجية بشكلٍ يتطلب انتقال البيانات عبر خطوط اتّصالٍ خارج شبكة الهيئةِ المحليّة، يجب تشفير جميع هذه البيانات.
15. بعد الانتهاء من التّغييرات المطلوبة بهدف تكامل البيانات بين الأنظمة، يجب إجراء مراجعة بمشاركة الدّوائر ذات العلاقة بهدف التّقييم والتّحسين.

14.2.2 إجراءات تكامل البيانات

يقدِّم إطار عمليّة تكامل البيانات الهيكل الذي تتم العمليّة من خلاله، والذي تشرف عليه دائرة تكنولوجيا المعلومات بهدف ضمان تنفيذ العمليّة بطريقة سليمةٍ وموثّقةٍ بشكلٍ كامل.

تتشكل هذه العمليّة من أربعة مراحل تقود إلى تحقيق هدف الجهة المعنيّة بطلب تكامل البيانات من خلال الأنظمة المختلفة بشكلٍ كامل ودقيقٍ وشاملٍ يوثّق انسياب البيانات، ويمكِّن من تتبع استخدام البيانات في الهيئة المحليّة، كما يمكن من استمرار التّحسين مستقبلاً.

المرحلة الأولى (أ): تحليل متطلبات تكامل البيانات

يتم تنفيذ هذه المرحلة من طرف دائرة تكنولوجيا المعلومات وبمشاركة الدّائرة المعنيّة صاحبة الطّلب، وتهدف هذه المرحلة إلى توضيح وتوثيق الوضع الحالي للبيانات والأنظمة وذلك تحضيراً للانتقال للوضع الجديد مع تحديد كافّة احتياجات التنفيذ للجهة صاحبة الطلب.

يجب اتّباع الخطوات التّالية:

1) **تقديم وصف للطّلب والهدف منه**: يتم تقديم ملخص موثق لطلب تكامل البيانات بين الأنظمة بما يشمل:

أ. الهدف من تكامل البيانات.
ب. الفوائد المتوقّعة.
ت. الجهات التي ستتأثر بذلك من مستخدمين ومديرين للأنظمة (مثل جميع المستخدمين، دائرة التّرخيص، دائرة خدمات المياه...).
ث. تحديد الأنظمة الإلكترونيّة التي ستتأثر بذلك مع توفير تفاصيل ذلك.

2) وصف وتوثيق الوضع الحالي (قبل تنفيذ عملية تكامل البيانات بين الأنظمة)

تقديم ملخص مختصر حول انسياب البيانات من وإلى النّظام. سيكون من المفيد استخدام مخططات تدفق البيانات.

3) تقديم ملخص بالبيانات التي سيشملها تكامل البيانات المقترح:
تقديمُ وصفٍ واضحٍ للبيانات التي ستتأثر بعمليّة التّكامل، وكذلك البيانات الجديدة التي سيشملها ذلك مع الميتاداتا metadata . ستساعد هذه المعلومات في تحديد تدفق بيانات الهيئة المحليّة وفي تحديد النُّظم (مجموعة الأنظمة) التي تستخدم تلك البيانات بشكلٍ موثوق.

4) وصف تدفق البيانات الجديد: يتم تقديم وصفِ تدفق البيانات المطلوب في الطّلب (بالخطوط العريضة). يجب أنْ يوضِّح ذلك الكيفيّة التي سيتم فيها استخدام البيانات، تكرار نقل البيانات بين الأنظمة وطريقة نقل تلك البيانات (مثلاً قد يتم نقل ملفات بعد ساعات العمل، الاستعلام الفوري من قواعد بيانات، الاستعلام من الدومين، الاستعلام من خلال خدمات الويب أو غير ذلك). سيكون من المفيد في هذه الخطوة وضع مخطط لتدفق البيانات.

المرحلة الثانية (ب): تحديد العمل والموارد المطلوبة لتنفيذ الطلب

1) يتم تنفيذ هذه المرحلة من طرف دائرة تكنولوجيا المعلومات وبالاعتماد على معارفهم وخبراتهم في البنية التحتية للبيانات، ومتطلبات الدوائر، واستجابة المستخدمين. الهدف من هذه المرحلة هو تحديد كمية العمل والموارد والموازنات اللازمة لتنفيذ الطلب، ليتم توفير الموارد بشكل متناسب.
2) **تحديد البيانات الحالية والجديدة ذات العلاقة بعملية التكامل:** ويشمل ذلك وضع قوائم بتلك البيانات واستخدامها وقواعد معالجتها.
3) **تحديد وتوضيح مصادر البيانات التي سيتم استخدامها لتنفيذ التكامل:** يتم تحديد وتوضيح مصادر البيانات اللازمة للتكامل. هذا يضمن اطلاع وإدراك كافة الأطراف ذات العلاقة حول وجهة البيانات من وإلى، كما أنَّه سيحافظ على فهم موثَّق لانسياب البيانات مع الوقت.
4) **توضيح طرق نقل البيانات بالتفاصيل:** يتم تقديم توضيح مفصَّل حول كيفيّة نقل البيانات من وإلى التّطبيقات ذات العلاقة، تكرار عملية النّقل، كما يتم توثيق تلك التفاصيل في سجلات بالإضافة إلى تسجيل عمليّات معالجة وتصحيح الأخطاء، وإجراءات التّحذير عند وقوع فشلٍ أو أيّ أخطاءٍ أخرى.
5) **تقدير العمل المطلوب وجدولته :**يتم تحديد الموارد المتوفرة، وتقدير العمل الذي تشمله كافّة مراحل المشروع (مشروع تكامل البيانات)، وتحضير خطة المشروع. سيوفر ذلك وصفاً للأعمال المطلوبة والموظفين الذين سيشاركون بها والتّاريخ المتوقع لتوفير مخرجات المشروع.

المرحلة الثالثة (ت) : الاختبار والتطبيق والمتابعة

1) يتم تنفيذ هذه المرحلة من طرف دائرة تكنولوجيا المعلومات وبمشاركة الجهة مقدمة الطلب، حيث يتم تقييم أمن المعلومات في إطار التكامل، كما يتم اختبار وتقييم مدى ملائمة التكامل المطلوب.
2) **تقييم أمن المعلومات:** يتم تقييم أمن المعلومات فيما يتعلق بالتطبيقات المستخدمة ونقل البيانات، وكذلك التأكد من وضوح وفهم مسؤولية الجهات ذات العلاقة عن أمن المعلومات. يجب توثيق الالتزام بمستوى مناسب من أمن المعلومات وما يتبع ذلك من إجراءات واحتياطات.
3) **الاختبارات:** يجب اختبار انسياب البيانات واختبار تكامل الأنظمة. هذه الخطوة تؤكد ملائمة وهدف انسياب البيانات، ومدى قدرة التطبيقات على الأداء وفق ما هو مطلوب.
4) **إعداد مصادر البيانات:** إعداد وتهيئة وتوثيق النظام لتوفير خدمة انسياب البيانات بشكلٍ فعّال.
5) **تسجيل ومتابعة الأحداث:** يتم إعداد أنظمة الرقابة لمراقبة عملية تكامل البيانات بشكلٍ تلقائي؛ وذلك للتمكن من اكتشاف الأعطال.

المرحلة الرابعة (ث): المسؤوليات، الحدود، التوثيق

1) يتم تنفيذ هذه المرحلة من طرف دائرة تكنولوجيا المعلومات وبمشاركة الجهة صاحبة الطلب، ويتم وضع السياسات والإجراءات التي تحكم استخدام انسياب البيانات والتكامل.
2) **الامتثال للقوانين وحماية البيانات:** يتم تحديد مسؤوليات حماية البيانات والإجراءات المرتبطة بتطبيق التكامل، كما يتم توفير معلومات الاتصال للمسؤولين عن البيانات وتوضيح قضايا تتعلق بالقوانين والامتثال للسياسات.
3) **تحديد هيكل الدّعم الفنّي:** يتم تحديد وتوزيع المسؤوليات بشكلٍ واضحٍ لتوفير الدّعم للمستخدمين مع توثيق معلومات الاتصال الخاصّة بالدّعم الفنّي.

4) **تحديد أوجه القصور:** يتم توفير المعلومات بخصوص أوجه القصور التي تم تحديدها، أو المحتملة في حلول التكامل المقدم من طرف دائرة تكنولوجيا المعلومات.
5) **التوثيق:** يجب أنْ تقوم دائرة تكنولوجيا المعلومات بتحديث وثائقها لكلِّ التّغييرات التي يتم إجرائها، مقدم طلب التكامل والأطراف ذات العلاقة عليهم أيضاً التوثيق وتحديد وثائقهم.

الامتثال مع السياسيات والمعايير

1. يجب أنْ تمتثل عمليّة التّكامل مع القوانين المطبَّقة في فلسطين.
2. يجب أنْ تتوافق عمليّة التّكامل مع سياسات دائرة تكنولوجيا المعلومات.
3. يجب أنْ تمتثل عمليّة التّكامل لسياسة أمن المعلومات وجميع الإجراءات المتعلقة بها في الهيئة المحليّة وعلى المستوى الوطني.

14.2.3 السياسات ذات الصلة

1. سياسة إدارة المخاطر.
2. سياسة تغيير كلمة المرور.
3. سياسة التّعافي من الكوارث.

15. سياسة وسائل التواصل الاجتماعي

15.1 المقدمة والأهداف

15.1.1 بيان السياسة

تم وضع هذه السّياسة لإدارة التّواجد الرّسمي للهيئة على الإنترنت، والمتمثل في موقع الهيئة المحليّة وتطبيقها على الهاتف المحمول وقنوات التّواصل الاجتماعي الأخرى. يعد تواجد الهيئة المحليّة على الإنترنت مصدراً أساسياً لتبادل المعلومات عبر الإنترنت مع الجمهور، ويعتبر أداة رئيسة لتقديم أخبار الهيئة المحليّة وبرامجها وخدماتها للمجتمع. يُنصح بشدة أنْ ترتبط حسابات وسائل التواصل الاجتماعي التّابعة للهيئة بموقع الهيئة المحليّة (حيثما أمكن) لغرض تنزيل النّماذج والوثائق، وتقديم معلومات محددة أو إضافيّة. إنَّ الهيئة المحليّة هي المالك الوحيد لموقعها الإلكتروني وأي حساباتٍ أخرى على وسائل التّواصل الاجتماعي ، وبالتالي فإنَّها ستبقى تحت السّيطرة الكاملة للهيئة بغضّ النّظر عن أيّ تغييراتٍ محتملة يتم إجراؤها في المجلس البلدي أو الإدارة العليا.

15.1.2 نطاق العمل

تنطبق هذه السّياسة على جميع موظفي ومسؤولي الهيئة المحليّة الذين يدلون بتصريحات نيابة عن الهيئة المحليّة على شبكات التّواصل الاجتماعي الخاصّة بها والتي تناقش أو تشارك أو تعلق على أخبار وأنشطة الهيئة المحليّة، كما أنَّها تنطبق على الجمهور الذي يزور موقع الهيئة المحليّة، أو قنوات التّواصل الاجتماعي المختلفة التّابعة للهيئة وينشر التعليقات، كما أنَّها تنطبق على أي جهات خارجيّة لديها تعاقد مع الهيئة المحليّة لتولّي إدارة (كلي أو جزئي) لأيٍّ من المواقع التّابعة للهيئة، كما أنَّها تنطبق على جميع قنوات وسائل الإعلام التّابعة للهيئة كما هو محدَّد في هذه السّياسة.

15.1.3 الهدف

الغرض من هذه السّياسة هو وضع مبادئ توجيهيّة ومعايير لضمان الاستخدام المناسب وإدارة وسائل التواصل الاجتماعي نيابةً عن الهيئة المحليّة . يجب استخدام وسائل التّواصل الاجتماعي كأداةِ اتصالٍ بهدف تعزيز التّواصل من الهيئة المحليّة للجمهور حول البرامج والخدمات للأغراض التّالية:

1. رفع الوعي وتبادل المعلومات.
2. تجنيد المتطوعين والموظفين.
3. الترويج لفعاليّات وبرامج وخدمات الهيئة المحليّة.
4. زيادة الوصول إلى المعلومات لجمهور معين.
5. تعزيز فرص المشاركة العامة والتعليق على منصة المشاركة عبر المواقع الخاصّة بالهيئة المحليّة.

15.2 السياسات والإجراءات

15.2.1 المسؤولية المحددة

يتولى فريق الإدارة العليا بالهيئة المحليّة مسؤوليّة تحديد دور مسؤول حساب وسائل التّواصل الاجتماعي، وحيثما أمكن يجب تعيين أو انتداب موظفٍ واحد (يستحسن أن يكون لديه خلفيّة في العلاقات العامّة والمعرَّفة بوسائل التّواصل الاجتماعي) كمسؤول حساب وسائل التّواصل الاجتماعي لكلّ حسابٍ تابعٍ للهيئة أو حسابٍ منفصلٍ مملوك من قِبل الهيئة المحليّة . هذا الموظف مسؤول عن نشر الحساب ومراقبته وصيانته نيابةً عن الهيئة المحليّة أو الإدارة أو اللّجنة الإعلاميّة ولديه الصلاحيّات لمتابعة متطلبات العمل مع أي جهات خارجيّة تمّ التّعاقد معها بهذا الخصوص. بالإضافة إلى مسؤول حساب الوسائط الاجتماعية العادي، يجب تحديد مسؤول بديل.

15.2.2 إنشاء الحساب وإدارته

يحتاج مسؤول حساب وسائل التّواصل الاجتماعي إلى موافقة الإدارة العُليا قبل إنشاء حساب على وسائل التّواصل الاجتماعي للهيئة، أو إضافة قناة وسائط اجتماعية جديدة. هذه خطوة مهمة لأنها قد تؤدي إلى الحاجة إلى توظيف أو

تعيين المزيد من الأشخاص للتّعامل مع الحسابات الجديدة. كما تحدد **سياسة التّوظيف في دائرة تكنولوجيا المعلومات** بوجوب توفير الموارد الكافية بما في ذلك وقت الموظفين والمواد كجزء من عملية اتخاذ القرار. يجب على مسؤول حساب وسائل التواصل الاجتماعي مراجعة أيّ وسائط اجتماعية موجودة لضمان الامتثال الكامل لهذه السّياسة ومراجعة الاكتشافات مع الإدارة العليا.

مسؤولية مسؤولي الحساب

1. يتصرف مسؤول حساب وسائل التّواصل الاجتماعي نيابةً عن الهيئة المحليّة عندما يشارك في أنشطة وسائل التّواصل الاجتماعي، لذلك يجب استخدام الحذر عند التّفاعل مع الجمهور لضمان الامتثال الكامل لمتطلبات الهيئة المحليّة وهذه السّياسة.
2. يجب عدم استخدام حسابات الهيئة المحليّة للتّعبير عن آراء شخصيّة أو أجندات شخصيّة.
3. تأكد من الحصول على البروتوكولات والأذونات المناسبة لنشر أي مواد محميّة بحقوق الطّبع والنّشر (بما في ذلك المستندات والمواقع الإلكترونيّة والشّعارات والصِّور).
4. تنطبق هذه السّياسة على أيّ أطرافٍ خارجيّة تعاقدت الهيئة المحليّة معها لتنفيذ أيّ مهامٍ تتعلق بوسائل التّواصل الاجتماعي كما تؤكد سياسة موردي تكنولوجيا المعلومات.

15.2.3 إدارة المحتوى العام

1. يجب على مسؤول الحساب إبقاء حسابات الهيئة المحليّة محدّثة بالمعلومات الجديدة عندما يكون ذلك ممكناً لان فترات التّعطيل الطّويلة والمتكررة (3-4 أسابيع) ستؤدي إلى إلحاق ضررٍ جسيم بمصداقيّة الهيئة المحليّة وقناة الاتصال القائمة.
2. يجب إبلاغ الإدارة العليا وبدء المناقشات مع رؤساء الأقسام للتّصديق على الوضع بما في ذلك الاحتمالات المتعلّقة بإغلاق وسيلة التّواصل الاجتماعي (القناة).
3. تعد عمليات التّدقيق المنتظمة المستمرة للحسابات أمراً ضروريّاً لضمان إزالة المنشورات غير المناسبة في الوقت المناسب مع التّأكيد أنَّ الهيئة المحليّة ليست مسؤولة عن أيّ تعليقات أو استخدام المواد المنشورة من قِبل المستخدمين.

15.2.4 إدارة محتوى مع روابط خارجية

يُحظر(وغير مسموح بها) مشاركة أو إعادة نشر المحتوى من حسابات وسائل التّواصل الاجتماعي الأخرى غير التّابعة للهيئة. يجب عدم مشاركة الرّوابط المؤدّية إلى حساب شخصي/ موقع ويب أو حساب تجاري فردي / موقع ويب أو مواد مرفوضة كما هو محدد في هذه السّياسة، أو إعادة نشرها على حساب وسائل التّواصل الاجتماعي الخاصّ بالهيئة المحليّة .

يجوز للأنواع التّالية من الرّوابط الخارجيّة

1. ربط الجمهور بالمعلومات والخدمات التي تقدمها الحكومة الفلسطينية أو الوكالات التّابعة للحكومة.
2. يوفر مزيداً من المعلومات حول الموضوع الموجود على موقع الهيئة المحليّة. يجب تقديم هذه المعلومات من قِبل مصدر رسمي و/ أو معتمد.
3. منظمة تابعة للهيئة أو نادي خدمي أو جمعية خيرية مسجلة باسم الهيئة المحلية.
4. جمعية مهنية أو أي منظمة يحددها المجلس البلدي.
5. المحتوى الذي يروّج لفعاليّات الهيئة المحليّة أو التي تنظمها أو تمولها الحكومة الفلسطينية، أو نادي خدمي يعمل داخل الهيئة المحلية يؤدي أعمالاً تعود بالنفع على السكان.
6. الأحداث التي تنظمها منظمة خيرية مسجلة تعمل داخل الهيئة المحلية.

15.2.5 قياس وسائل التواصل الاجتماعي

سينتج مسؤول حساب وسائل التواصل الاجتماعي تقريراً نصف سنويّ (حزيران، كانون ثاني) عن تحليلات حسابات وسائل التّواصل الاجتماعي التّابعة للهيئة بحيث تتضمن مقاييس الأداء الخاصّة بالقناة أو وسيلة التّواصل الاجتماعي مثل: إجمالي المتابعين، عدد الردود، إعادة التغريد، التّركيبة السّكانيّة (بالفيس بوك تحديداً)، عدد التعليقات، عدد الشكاوى، إبداء الإعجاب والتعليقات.

15.2.6 التواصل العام للموظفين

1. لا يُسمح لأيّ موظّفٍ أو مستشار ليس مسؤول حساب على وسائل التّواصل الاجتماعي بالنّشر أو التّعليق عبر وسائل التواصل الاجتماعي بأي طريقةٍ توحي بأنّهم يفعلون ذلك كممثلين عن الهيئة المحليّة أو فيما يتعلق بها.
2. يمكن التّعرف على الموظف أو المستشار للهيئة أو عضو المجلس البلدي بسهولة كموظف أو تابع للهيئة (حتى لو لم يعرّفوا عن أنفسهم بشكلٍ صريح على هذا النّحو)؛ لذلك يجب أخذ الاحتياطات المناسبة للتّأكد من أنّ المعلومات المنشورة تحدد بوضوح على أنّ المنشور يخص فقط الكاتب (المالك الوحيد) وليس الهيئة المحليّة .
3. يجب ألا تنتهك أي اتصالاتٍ عامّة تتعلق بالهيئة المحليّة أي إرشاداتٍ منصوص عليها في هذه السّياسة أو أي دليل موظفٍ أو عقد طرفٍ ثالثٍ.
4. لا يجوز للموظفين و\أو والأطراف الخارجيّة التي تعمل بعقد مع الهيئة المحليّة الكشف عن أيّ معلوماتٍ حسّاسة، أو خاصّة، أو سريّة، أو مالية عن الهيئة المحلية . يشمل ذلك الإيرادات والأرباح والتنبؤات والمعلومات الماليّة الأخرى وأيّ معلوماتٍ تتعلق بخدمات معيّنة أو عملاء أو مواطنين، بخلاف ما هو متاح للجمهور في أيٍّ من ملفات الهيئة المحليّة أو البيانات الصحفية.
5. لا يجوز للموظفين والأطراف الخارجية الكشف عن أي معلومات حساسّةٍ، أو خاصّةٍ، أو سريّةٍ، أو ماليّةٍ عن مواطني الهيئة المحلية ، بما في ذلك اسم أي مواطن في الهيئة المحليّة وحقيقة أنَّ أيّ عميلٍ محدّد لديه علاقة تجارية مع الهيئة المحليّة.
6. لا يجوز للموظفين والأطراف الخارجية التي تعمل بعقد مع الهيئة المحلية نشر أي مواد تتعلق بالهيئة المحلية و/أو مواطنيها و/أو والأطراف الخارجية التي تعمل بعقد مع الهيئة المحلية أخرى محمية بموجب قوانين الملكية الفكرية المعمول بها (بما في ذلك، على سبيل المثال لا الحصر، حقوق النّشر والعلامات التجارية) ما لم يتم الحصول على إذن كتابي من المالك للملكية الفكرية.
7. لا يجوز للموظفين والأطراف الخارجية مهاجمة زملائهم الموظفين أو الأطراف الخارجية التي تعمل بعقد مع الهيئة المحلية أو المواطنين والعملاء أو البائعين. يستطيع الموظفون والأطراف الثّالثة الاختلاف مع إجراءات الهيئة المحليّة أو سياساتها أو إدارتها باحترام.
8. يجب أنْ تلتزم جميع حسابات الهيئة المحليّة والحسابات المنفصلة على وسائل التّواصل الاجتماعي بالقوانين واللوائح والسياسات الفلسطينية المعمول بها ، بما في ذلك سياسات الهيئة المحليّة الأخرى المعمول بها.
9. يُسمح للموظف بالاستخدام الشّخصي العَرَضي، أو البسيط لوسائل التواصل الاجتماعي على الأجهزة الشخصية أو أجهزة مكان العمل بشرط أن لا يؤدي هذا الاستخدام المحدود إلى أي نفقات قابلة للقياس للهيئة في الوقت أو المواد أو الإنتاجية ويخضع المحتوى لقيود هذه السياسة.

15.2.7 حضور مجلس الهيئة المحلية على مواقع التواصل الاجتماعي

يجب إنشاء الحسابات الخاصّة برئيس الهيئة المحليّة أو أعضاء المجلس البلدي والاحتفاظ بها منْ قِبل المالك، وليس منْ قِبل موظف الهيئة المحليّة ما لم يتخذ المجلس قراراً بهذا الصدد. يُسمح لمسؤول حساب وسائل التواصل الاجتماعي بمشاركة / إعادة نشر محتوى من منشورات تخص رئيس الهيئةِ المحليّة أو أعضاء المجلس، إذا كان المحتوى لا يروج أو ينتقد بوضوح حزباً سياسياً أو مرشحاً أو أيديولوجية فلسطينية. في بداية عام الانتخابات سيتخذ مسؤول حساب وسائل التواصل الاجتماعي الاحتياطات فيما يتعلق بنشر الرّوابط وإبداء الإعجاب ومشاركة المحتوى المنشور على موقع رئيس الهيئة المحلية أو موقع أعضاء المجلس البلدي ويبقى القرار نافذ إلى حين الاجتماع الافتتاحي للمجلس المنتخب حديثاً أو نهاية الانتخابات. يتضمن المحتوى المناسب القابل للمشاركة في كل الأوقات، على سبيل المثال لا الحصر الأحداث المجتمعية، وإعلانات خاصّة بالهيئة المحليّة، وإعلانات القرارات المقرة، وما إلى ذلك.

15.2.8 إخلاء مسؤولية

حيثما أمكن يجب أنْ يحتوي كلّ حساب على وسائل التواصل الاجتماعي تستخدمه الهيئة المحليّة على إخلاء مسؤوليّة، يُعلم زوار الموقع بوضوح أنّ تعليقات الطّرف الثّالث ليست اتصالاتٍ رسميّةٍ للهيئة. يجب أن يشير إخلاء المسؤولية أيضاً إلى أنّ موقع الهيئة المحليّة أو تطبيق الهاتف المحمول الخاص به هو الوجهة الرسمية لمعلومات الهيئة المحليّة، وأنَّ حسابات وسائل التّواصل الاجتماعي تتم مراقبتها بانتظام من الأحد إلى الخميس خلال ساعات العمل العادية.

مثال على إخلاء المسؤولية:

"التعليقات التي أدلى بها أفراد الجمهور ليست اتصالاتٍ رسميّةٍ للهيئة وهي مملوكة للمعلّق المساهم. لا تعكس هذه التعليقات آراء أو سياسات الهيئة المحلية . تتم مراقبة هذه الصّفحة بشكلٍ أساسيّ خلال ساعات العمل العادية ، من الساعة 8:30 صباحًا حتى 2:30 مساءً من الأحد إلى الخميس. يجب استخدام موقع الشركة ps. ..... www أو تطبيق الهاتف المحمول الخاص بالهيئة المحلية كمصدر رسمي لمعلومات الهيئة المحلية. "

15.2.9 إدارة كلمة المرور والأمان

يجب أنْ تلتزم بيانات اعتماد وتفاصيل حسابات الهيئة المحليّة للشّركات والحسابات المنفصلة بـ **سياسة كلمة المرور** المتطلبات ويجب توثيقها وحفظها في مكانٍ آمنٍ داخلِ الهيئة المحليّة بمعرفة مدير عام الهيئة المحلية ومسؤول قسم تكنولوجيا المعلومات والاتصالات. إذا كان قسم تكنولوجيا المعلومات والاتصالات يوفر الاستضافة للموقع فسيتم منح الوصول إلى الموقع فقط لمسؤول حساب وسائل التواصل الاجتماعي. ستحتفظ إدارة تكنولوجيا المعلومات والاتصالات في الهيئة المحلية بقائمة رئيسة لمعلوماتِ تسجيلِ الدّخول إلى وسائل التواصل الاجتماعي الخاصَّة بالهيئة المحلية . يجب إبلاغ مسؤول قسم تكنولوجيا المعلومات والاتصالات على الفور بتغييرات كلمة المرور. يجب أنْ ترتبط الحسابات التي تم إنشاؤها لتمثيل الهيئة المحلية بعنوان بريد إلكتروني صالح للهيئة: (municipality.ps@-------).

15.3 تعطل الموقع

بالإضافة إلى التّوجيهات المذكورة في **سياسة التّعافي من الكوارث**، تساعد الإرشادات التّالية مسؤول حساب وسائل التّواصل الاجتماعي في معالجة الانقطاع المحتمل في موقع الهيئة المحلية و / أو حسابات وسائل التواصل الاجتماعي:

1. يجب إخطار مضيف موقع الويب على الفور، أو يجب إخطار مسؤول قسم تكنولوجيا المعلومات والاتصالات، أو لجنة الطوارئ الخاصة بتكنولوجيا المعلومات بالهيئة المحلية على الفور (إذا كان الموقع مستضافاً داخلياً) كما تحدد **سياسة إدارة المخاطر**.
2. تغيير كلمات المرور.
3. استبدل بنسخة نظيفة من البيانات.
4. توثيق الأحداث الخاصّة بالعطل وأسبابه.

15.4 إدارة السجلات والاحتفاظ بها

يجب الاحتفاظ بالمنشورات / المحتوى المستخدم الذي يعتبر سجلات رسمية وإزالته وفقاً لسياسة **سياسة النسخ الاحتياطي** المقرة من الهيئة المحلية. المنشورات / محتوى المستخدم الذي يعتبر سجلاً انتقالياً للهيئة غير مطلوب للاحتفاظ به، ويمكن إزالته من مواقع التواصل الاجتماعي. سيتم الاحتفاظ بأيّ محتوى تمت إزالته بناءً على الإرشادات منْ قِبل مسؤول حساب وسائل التواصل الاجتماعي، مع الاحتفاظ بوثائق داعمة، بما في ذلك الوقت والتاريخ وهوية الملصق وسبب الإزالة وأي إبلاغ عن الحادث.

15.5 إعلان هذه السياسة

داخليّاً سيتم إبلاغ هذه السّياسة للموظفين ونشرها على موقع الهيئة المحلية للاستخدام العام إذا لزم الأمر. جميع الحسابات التي تم إنشاؤها ونشرها على حسابات وسائل التواصل الاجتماعي للهيئة باستخدام تكنولوجيا الهيئة المحلية هي ملك للهيئة. سيتم اتخاذ تدابير تكنولوجية وإجرائية معقولة، بما في ذلك التدقيق والرصد العشوائي لحسابات وسائل التواصل الاجتماعي، لضمان الالتزام بسياسات ومعايير الهيئة المحلية.

15.6 سلوك المواطن

لن يُسمح بتعليقات المواطنين أو منشوراتهم أو مقالاتهم التي تحتوي على المحتوى التالي:

1. التعليقات التي لا تتعلق موضوعيّاً بالموضوع و/ أو القضية التي يتم التعليق عليها.
2. البريد العشوائي أو التَّصيُّد أو الإفراط في النشر.
3. المشاركات التي تهدف إلى طلب المبيعات أو المنتجات أو السلع والخدمات.
4. لغة أو محتوى بذيء، أو عدواني، أو بغيض، أو تشهيري، أو مهين، أو فظ، أو مسيء، أو عنيف.
5. المحتوى الذي يتضمن روابط لمواد مرفوضة، على النحو المحدد في هذه السياسة.
6. السلوك أو التشجيع على نشاط غير قانوني.
7. المعلومات التي قد تعرض خصوصيّة أو سلامة أو أمن الهيئة المحلية أو مواطنيها أو عملائها أو الأنظمة العامة للخطر.
8. التعليقات أو المنشورات التي تتضمن مواد غير دقيقة، أو تحريف الحقائق كما هو معروف من قبل الهيئة المحلية.
9. التعليقات أو المنشورات التي تنتحل شخصية أو تحرف شخصية شخص آخر، بما في ذلك الشخصيات العامة أو موظفي الهيئة المحلية أو مسؤولي الهيئة المحلية.
10. المحتوى الذي ينتهك حقوق الملكية القانونية لأيِّ طرف آخر.

15.7 السياسات ذات الصلة

1. سياسة إدارة المخاطر.
2. سياسة تغيير كلمة المرور.
3. سياسة التّعافي من الكوارث.

16.سياسة التوظيف في دائرة تكنولوجيا المعلومات

16.1 المقدمة والأهداف

16.1.1 بيان السياسة

تمّ وضع هذه السّياسة لضمان توظيف موارد كافية (بشكلٍ مباشر أو غير مباشر) كجزءٍ من قسم تكنولوجيا المعلومات والاتصالات. تتكون دائرة تكنولوجيا المعلومات والاتصالات من أنظمة ((أجهزة وبرمجيات)، والموارد البشريّة التي تعتبر العنصر الأساسي في نجاح العمليات والخدمات للمواطنين، ويجب إدراج احتياجات دائرة تكنولوجيا المعلومات والاتصالات في الخطط السنوية للهيئة على النحو المنصوص عليه في سياسة شراء الأصول. يجب اعتماد هيكل إداري واضح لقسم تكنولوجيا المعلومات والاتصالات مع وصف للأدوار الوظيفية الموافق عليها منْ قِبل المجلس البلدي ليتم تضمينها في هيكل إدارة الهيئة المحلية، وبالتالي سيتم تضمين التكاليف ذات الصلة في ميزانية الهيئة المحلية.

16.1.2 نطاق العمل

تنطبق هذه السياسة على جميع الوظائف المقرة في دائرة تكنولوجيا المعلومات والاتصالات بالهيئة المحلية، بحيث تؤكد وجود موارد كافية للسَّماح بالتّنفيذ الآمن لخطط الدائرة والتي تهدف إلى :

1. تحسين الإنتاجية العامة وأداء الهيئة المحلية .
2. تحقيق كفاءات أكبر.
3. التحقق من أنَّ استثمار الهيئة المحلية في تطوير دائرة تكنولوجيا المعلومات والاتصالات يحقق الأهداف الموضوعة للهيئة.

16.1.3 الهدف

يضع هذا الإطار للعمل معايير محددة للتوظيف والحفاظ على قوة عاملة لديها الكفاءة ومؤهلة للعمل بدائرة تكنولوجيا المعلومات والاتصالات بناء على معايير وإجراءات محددة ستستخدمها الهيئة المحلية؛ لإنشاء الوظائف وتعيين الموظفين واختيارهم وتوظيفهم، وسوف يتم ذلك بطريقة عادلة ومنصفة وبما لا يتعارض مع أي قوانين فلسطينية و\أو قوانين معتمدة بالهيئة المحلية.

16.1.4 المسؤوليات

1. يعتبر مسؤول قسم تكنولوجيا المعلومات والاتصالات مسؤولاً عن تطوير خطة تكنولوجيا المعلومات والاتصالات وتقديمها إلى مجلس الهيئة المحلية لاعتمادها.
2. في حالة عدم وجود دائرة لتكنولوجيا المعلومات والاتصالات، يجب على المجلس البلدي إنشاء لجنة تتولى مسؤولية الدائرة، وتولي مهام المسؤول المنصوص عليها بهذا الإطار للعمل وتنفيذ هذه السياسة.
3. تختص دائرة المالية بتضمين قرارات المجلس بهذا الخصوص في الميزانية.
4. قسم الموارد البشرية مكلف بإتمام عملية توظيف الموارد اللازمة.

16.2 السياسات والإجراءات

16.2.1 البيانات الأساسية

1. يقوم المجلس بدراسة واعتماد تمويل الميزانية لجميع وظائف الموظفين الدائمين الجديدة التي تنشئها الهيئة المحلية والتي تتطلب أموالاً إضافية.
2. يُسمح لمسؤول قسم تكنولوجيا المعلومات والاتصالات، تحت إشراف قسم الموارد البشرية بالاستفادة من جميع وظائف الموظفين الدائمين المنشأة والممولة، بالإضافة إلى ذلك يجب أنْ تتمتع إدارة قسم تكنولوجيا المعلومات والاتصالات بسلطة تقديرية إدارية في استخدام الموظفين المؤقتين والخدمات المتعاقد عليها شريطة أنْ يتم تضمين جميع التكاليف ذات الصّلة ضمن الميزانيات المعتمدة من المجلس.

3. يكون مسؤول قسم تكنولوجيا المعلومات والاتصالات وإدارة الموارد البشرية هو الممثل البلدي المعتمد لطلب توظيف والموافقة على تعيين ومتابعة الموظفين في إدارة تكنولوجيا المعلومات والاتصالات.
4. سيحدد مسؤول قسم تكنولوجيا المعلومات والاتصالات ما إذا كان سيتم شغل الوظائف الشاغرة، الدائمة والمؤقتة والعارضة والبدء في عملية النشر من خلال قسم الموارد البشرية.
5. فصل الموظفين هو قرار مشترك بين أقسام الموارد البشرية وتكنولوجيا المعلومات والاتصالات مع الأخذ في الاعتبار قوانين العمل الفلسطينية ذات الصلة.
6. يجب تصميم هياكل الموظفين العادية لاستيعاب معظم العمليات في الأنشطة اليومية لقسم تكنولوجيا المعلومات والاتصالات، ومع ذلك فمن المسلَّم به أنَّ هناك أوقاتاً وحالاتٍ يمكن فيها استخدام موظفين مؤقتين.

16.2.2 إطار العمل في هذه السياسة تتضمن المتطلبات القياسية التالية:

16.2.2.1 تحديد احتياجات الموارد البشرية

يجب أن يلتزم مسؤول قسم تكنولوجيا المعلومات والاتصالات بالنتائج المكتشفة في "تحليل الفجوة" كما هو منصوص عليه في سياسة شراء أصول تكنولوجيا المعلومات التي توضِّح تفاصيل الأصول الحالية لقسم تكنولوجيا المعلومات والاتصالات والعناصر المفقودة وكيفية تعويضها، و يتطلب التخطيط الموضوعي مراجعة أساسية سنوية لخطط قسم تكنولوجيا المعلومات والاتصالات، والتي يجب أن تكون خطة متجددة مدتها أربع سنوات.

16.2.2.2 متطلبات التأهيل والخبرة

بناء على نتائج خطة تكنولوجيا المعلومات والاتصالات، يجب على مسؤول دائرة تكنولوجيا المعلومات والاتصالات تحديد متطلبات الدور الوظيفي وفقاً لما يلي (كحدٍّ أدنى):

1. الخبرة اللازمة المتخصصة للتعامل مع الوظيفة (مقارنة بالمعرفة العامة مثلاً).
2. عدد سنوات الخبرة في نفس المجال.
3. مستوى التعليم المطلوب للقيام بهذه الوظيفة.
4. الشهادات الخاصة اللازمة للتعامل مع الوظيفة (مثل شهادات مايكروسوفت أو سيسكو مثلاً).
5. مدى المعرفة العامة بتطورات التكنولوجيا في المجال الذي سيعمل فيه.
6. المهارات الأخرى ذات الصلة مثل مهارات الاتصال والقدرة على التعامل كجزء من فريق عمل.
7. تحديد المعاش أو المكافأة مع الامتيازات (بناء على سلم الهيكل الوظيفي للهيئة).

16.2.2.3 إعلان الوظائف الشاغرة

1. سيتم نشر الوظائف الشاغرة على موقع الهيئة المحلية و / أو في الصحف المحلية، ومواقع التوظيف(jobs.ps) كمثال ومن خلال الجمعيات المهنية مثلاً.
2. سيتم الإعلان عن الوظائف الشاغرة لمدة 10 أيام على الأقل ما لم يكن منصباً إدارياً رفيعاً، فسيتم نشره بشكل مستمر لمدة 15 يوماً على الأقل.
3. سيشمل الإعلان الحدّ الأدنى من المتطلبات من حيث المهارات والخبرات والصفات الأخرى المطلوبة للتعيين. يضم أيضاً ملخصاً لمجالات الأداء الرئيسة \ الواجبات الأساسية للوظيفة وبيان واضح يعلن أنَّ الوظيفة دائمة، أو لفترة محدودة أو لمدة محددة .
4. إذا لم يكن هنالك مرشحون مناسبون، فيمكن تمديد إعلانات الوظائف حسب الحاجة.

استثناءات:

سيتم الإعلان عن جميع الوظائف الشاغرة، وستقام مسابقة توظيف وفقاً لهذه السياسة ما عدا في الحالات التالية:

1. وجود خطة موافق عليها من المجلس البلدي، ووفقاً لتقييمات المدير العام للهيئة لترتيب التعاقب بقسم دائرة تكنولوجيا المعلومات والاتصالات لتعيين الشاغر الوظيفي داخليّاً بأنْ يتم تعيين موظف يعمل حاليّاً مع الهيئة المحليّة بشرط أنْ يكون الموظف لديه تقييمات أداء جيدة واستيفائه لمؤهلات الوظيفة العليا، مثل: الانتقال من مسؤول قسم الى مدير دائرة.

2. لا حاجة لإعادة نشر وظيفة إذا تم شغلها في حال أنَّ المرشح أو الهيئة المحلية أنهت التّعاقد في أول ثلاثة (3) أشهر من التوظيف. عندها يجوز للهيئة وفقاً للأحكام المعمول بها في سياسة التّوظيف هذه ، تقديم فرص العمل للمتقدمين المؤهلين الآخرين بدلاً من إعادة نشر الوظيفة الشّاغرة.

اعتبارات التوظيف المحلية والداخلية

تشجع الهيئة المحلية التوظيف المحلي أو من داخل الهيئة المحلية من خلال الآتي:

أ. الإعلان عن الوظائف في مواقع عامة تابعة للهيئة بحيث يسهل على المجتمع المحلي رؤيتها.
ب. قد يقرر المجلس منح علامات إضافية بنسبة 14% مثلاً لمرشح للوظيفة يعيش ضمن حدود الهيئة المحلية.
ت. في حال تقدم موظف حالي لملء الشاغر الوظيفي المعلَن عنه، سيتم اعتباره مؤهلاً في حالة توافر لديه فقط مستوى الخبرة و\أو القدرة الكافية للقيام بالوظيفة، لديه تقييمات جيدة من مرؤوسيه، وحصل على توصية من مسؤول القسم.
ث. يقوم قسم الموارد البشرية بإضافة اسمه إلى قائمة المؤهلين للحضور للمقابلة، ولكن وضعه كموظف حالي، لا يعني حصوله على الوظيفة بشكلٍ تلقائي.
ج. على لجنة التعيينات مراجعة ملف الموظف للتأكد من أنَّه يستطيع القيام بالمهام المنصوص عليها للوظيفة.

16.2.2.4 المقابلة

1. باستثناء التعيينات التي يجب أن يقوم بها المجلس، يقوم رئيس الهيئة المحلية بتعيين **لجنة اختيار** مكونة من مسؤول الموارد البشرية أو أحد موظفي القسم، ومسؤول قسم تكنولوجيا المعلومات والاتصالات والمدير العام للهيئة.
2. بعد تاريخ إغلاق إعلان الوظيفة، ستعد الموارد البشرية قائمة رئيسية بتنسيق جدول توضح بالتفصيل:
3. اسم المتقدم.
4. مؤهلات المتقدمين وخبراتهم ذات الصلة بالوصف الوظيفي.
5. يجب الاحتفاظ بنسخة من السيرة الذاتية للمتقدم جاهزة لمراجعتها من قِبل لجنة الاختيار إذا طلب ذلك.
6. سيقوم قسم الموارد البشرية بدعوة جميع المتقدمين المؤهلين (تم فحصهم وفقًا للمعايير المناسبة المحددة على النحو المطلوب في الوصف الوظيفي لحضور مقابلة).
7. سيتم ترتيب الأسئلة حسب المهارات المطلوبة، حيث سيقوم أعضاء اللجنة بتوثيق إجابات المتقدمين على الأسئلة للمساعدة في تقييم مؤهلات كلّ متقدم.
8. سيتم طرح نفس الأسئلة على جميع الأشخاص الذين أجريت معهم المقابلات ويتم ترتيب الإجابات باستخدام نفس النظام.
9. سيقوم جميع الأشخاص الذين أجريت لهم مقابلة بعمل امتحان قدرات للتأكد من استطاعتهم القيام بالمهام المنصوص عليها بإعلان الوظيفة.

16.2.2.5 الاختيار

1. يجب على فريق الاختيار أنْ يسعى لتحقيق توافق في الآراء عند التّوصية بمرشح معين للتعيين إلى مدير عام الهيئة المحليّة الذي يتخذ قرار التوظيف النهائي. في حالة عدم وجود توافق في الآراء يجب أنْ يوافق المدير العام على الاختيار وكذلك مسؤول قسم تكنولوجيا المعلومات والاتصالات .
2. سيتم إبلاغ المتقدمين غير الناجحين الذين تمت مقابلتهم عن طريق البريد الإلكتروني.
3. سيتم تقديم الملاحظات للمتقدمين غير الناجحين إذا طلب ذلك، وستقتصر هذه التعليقات على العوامل المتعلقة بالوظيفة نفسها.

16.2.2.6 توظيف

جميع عروض التوظيف مشروطة بقيام المرشح للوظيفة :

1. بتوفير جميع الوثائق المتعلقة بالتوظيف التي قد تطلبها الهيئة المحلية.
2. بإبرام عقد عمل مكتوب مع الهيئة المحلية قبل بدء العمل.

16.2.2.7 تدريب

يجب أن يضمن مسؤول تكنولوجيا المعلومات والاتصالات تخصيص الموارد واستخدامها وفقاً للتعليمات العامة لإدارة أصول تكنولوجيا المعلومات والاتصالات، وأنَّ التدريب يتم وفقاً لتدريب مستخدمي تكنولوجيا المعلومات والاتصالات وإجراءات الهيئة.

16.2.3 تضارب المصالح

يجب على أيِّ فردٍ لديه تضارب في المصالح على النّحو المنصوص عليه في هذه السّياسة إبلاغ لجنة الاختيار بذلك؛ لدراسة إذا كان هنالك حاجة لاستبدال هذا العضو، ولتبيان مدى التأثير على قرار التوظيف الذي قد ينتج عنه أيّ تحيز فعلي، أو تضارب في المصالح المحتمل، أو المتصور في عملية التوظيف. لا يجوز لأي فردٍ مشاركٍ في عملية التوظيف استخدام سلطته من أجل مصلحته الخاصة، أو لمصلحة شخص آخر، أو وضع نفسه في حالة تضارب، أو تضارب محتمل بين مصلحته الشخصية وواجباته بخصوص هذه السياسة .

16.2.4 المحسوبيات

يجب أن يؤخذ بالاعتبار وبعناية إذا كان المرشح سيعمل في منصب يكون فيه المشرف المباشر عنه أو المرؤوس أحد أفراد الأسرة المباشرين (راجع التعريفات في هذه السياسة)، وعلى وجه الخصوص يحظر تعيين أفراد عائلات أعضاء المجلس في وظيفة تكون فيها علاقة العمل المباشرة بالمجلس، أيضاً إذا تطورت أي علاقة أسرية (بالزواج مثلاً) تضع أعضاء المجلس أو الموظفين في علاقة تنطبق عليها هذه السياسة، يجب على الفرد (الأفراد) المعنيين إبلاغ المجلس فوراً لمعالجة هذه المسألة بطريقة عادلة ومنصفة، ويجب توثيق جميع القرارات المتخذة لمعالجة الوضع لدى إدارة الموارد البشرية والاحتفاظ بها في ملف الموظف .

16.2.5 سرية عملية التوظيف

تخضع جميع المعلومات الشخصية للمرشحين أو المتقدمين للوظيفة والموجودة في عهدة الهيئة المحلية، على سبيل المثال: السير الذاتية، أو أي معلومات أخرى ذات صلة للحماية الكاملة ولا ينبغي توزيعها خارج إدارة الموارد البشرية ولجنة الاختيار وكجزء فقط من عملية الفرز، وفي حالة الإعلان عن مرشح ناجح سيتم الإعلان عن الاسم والمنصب فقط ولن يتم الإعلان عن أيِّ معلوماتٍ شخصيّة أخرى مثل: العمر، أو المؤهلات.

16.2.6 السياسات ذات الصلة

1. سياسة شراء أصول تكنولوجيا المعلومات.

مراجع

تم الاعتماد على أفضل الممارسات الدولية ومن ضمنها:

1. السياسة العامة لأمن المعلومات في الوزارات والمؤسسات الحكومية، وزارة الاتصالات وتكنولوجيا المعلومات، فلسطين وزارة الاتصالات-سياسات(pna.ps) ، قرار مجلس الوزراء الفلسطيني رقم (09\112\18\م.و.م.أ) لعام 2021
2. منظمة التعاون الاقتصادي والتنمية (2014) إدارة المخاطر الأمن الرقمي لتحقيق الازدهار الاقتصادي والاجتماعي، توصية منظمة التعاون والتنمية في الميدان الاقتصادي، باريس http://dx.doi.org/14.1787/9789264245471-ar
3. دليل إدارة المخاطر، 73 ISO
4. أهداف الرقابة لتقنية المعلومات (COBIT)
5. مكتبة البنية التحتية لتكنولوجيا المعلومات (ITIL)
6. ISO / IEC 17799: الإصدار 1 ، 2000 - تكنولوجيا المعلومات - قواعد الممارسة لإدارة أمن المعلومات
7. Information Technology Infrastructure Library “ITIL” Change management
8. ISO 73/2009
9. ISO/IEC 38500: Internationally accepted as the standard for Corporate Governance of ICT
10. NIST – www.nist.gov : Ross, R. (2011), Guide for Conducting Risk Assessments, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/14.6028/NIST.SP.800-30r1 (Accessed October 20, 2021)
11. ISO/IEC 38500: Internationally accepted as the standard for Corporate Governance of ICT
12. ISO/IEC 31414:2019 – Risk Management – Risk Assessment Techniques
13. ISO/IEC 27000-018 - Information technology -Security Techniques- Information security management systems- Overview and Vocabulary
14. ISO/IEC 24762:2008 Information technology- security techniques – guidelines for information and communications technology disaster recovery services.
15. ISO 24762 - 5 clauses:
    - Clause 5: ICT Disaster Recovery.
    - Clause 6: ICT Disaster Recovery facilities.
    - Clause 7: Outsourced service provider’s Capability
    - Clause 8: Selection of recovery sites
    - Clause 9: Continuous improvement
16. Guidance on Outsourcing-2014 :37500 ISO1
17. ISO/IEC 38500: Internationally accepted as the standard for Corporate Governance of ICT
18. ISO 9001: Quality Management
19. NIST password Guidelines and Best Practices for 2020, www.nist.com
20. ISO /IEC 27000:2018, Information Technology-Security Techniques-Information Security Management Systems – Overview and Vocabulary
21. ISO /IEC 27001:2012, Information Technology-Security Techniques-Information Security Management Systems - Requirements

22. ISO /IEC 27002:2012, Information Technology (Security Techniques – code of practice for information technology controls).
23. ISO 27002: Information technology — Security techniques — Information security management system
24. ISO/IEC 38500: Internationally accepted as the standard for Corporate Governance of ICT
25. ISO 9001: Quality Management
26. NIST: National Institute of Standards and Technology
27. ISO/IEC 38500: Internationally accepted as the standard for Corporate Governance of ICT
28. ISO 9001: Quality Management Systems – Requirements
29. NIST 800-53: Newton, J. (1987), Guide on Data Entity (Naming Conventions), Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=900402;
30. University of Waterlow Technology abbreviations: /www.allacronyms.com/technology/abbreviations
31. ISO 9001 – Quality Management Systems – Requirements
32. ISO/IEC 38500: Information Technology – Governance of IT for the Organization

ملحق رقم 1: أساسيات نظام تكنولوجيا المعلومات

	أساسيات نظام تكنولوجيا المعلومات (المعايير التشغيلية الدنيا)				ملاحظة توضيحية للإجابة على المعلومة
1	**الاتصال بالأنترنت:** اتصال مستمر عالي السرعة يوفر الوصول إلى البريد الإلكتروني وتحديثات البرامج والخدمات المهمّة الأخرى، مثل التطبيقات المستندة إلى الويب.	نعم	لا	غير متأكد	يجب أن يكون لدى الهيئة المحلية اتصال ثابت عالي السرعة مصنف: **الأفضل**: اتصال الألياف (DSL). **أفضل**: اتصال الكابل. **جيد**: اتصال.
2	**النسخ الاحتياطي للملفات:** يتم نسخ جميع البيانات المهمّة احتياطيّاً بانتظام بطريقةٍ ما.	نعم	لا	غير متأكد	هل يتم نسخ البيانات احتياطيّاً وتكرارها من أجل استمرارية الأعمال والتّعافي من الكوارث؟
3	**كلمات مرور قوية** تخضع كلمات المرور لقواعد رسمية بشأن الشكل (عدد الأحرف والأحرف والأرقام والرموز) التي تنطبق على حسابات الهيئة المحلية ويتم تغيير كلمات المرور بانتظام وعدم تكرارها وحمايتها.	نعم	لا	غير متأكد	يتم منح الإذن من خلال عمليات تسجيل دخول المستخدم والحسابات وكلمات المرور.
4	**مكافحة الفيروسات (مرخصة) على جميع أجهزة الكمبيوتر** لا تفي خيارات مكافحة الفيروسات المجانية (مقابل الاشتراك المدفوع) مثل AVG أو Microsoft Security Essentials غير المرخصة للاستخدام التجاري أو الحكومي بمتطلبات الاستجابة ب "نعم".	نعم	لا	غير متأكد	يمكن لمنتج مكافحة الفيروسات / مكافحة البرامج الضارة منع الإصابة من خلال تثبيت تقنيات الحماية.
5	**أجهزة الكمبيوتر التي تعمل ببرامج محدثة (مدعومة من الموردين)** التنزيل المنتظم والاستباقي وتثبيت تحديثات البرامج للإصدار الحالي (وليس ترقية الإصدار) بانتظام أو يتم تشغيلها تلقائياً لكل تطبيق برمجي (نظام التشغيل والمتصفح وبرامج الجهات الخارجية وما إلى ذلك)	نعم	لا	غير متأكد	يجب تحديد الصيانة الشهرية (التصحيحات والتحديثات والتنظيف وما إلى ذلك) وخطط المراقبة للأجهزة والبرامج. يمكن استخدام الفحص للتحقق من صيانة التحديثات.

ملحق رقم 2: القائمة المرجعية السنوية لتقييم تكنولوجيا المعلومات

	القائمة المرجعية السنوية لتقييم تكنولوجيا المعلومات: إدارة الأصول				ملاحظة توضيحية
1	**هل هناك جرد مفصَّل دقيق للأجهزة؟**	نعم	لا	غير متأكد	يقوم مسؤول أصول تكنولوجيا المعلومات بتأكيد بيانات المخزون المناسبة.
2	هل هناك جرد مفصَّل دقيق للبرامج؟	نعم	لا	غير متأكد	جمع بيانات المخزون هو مفتاح الإدارة السليمة للأصول.
3	هل هناك مراجعة مجدولة/دورية للأجهزة والبرامج لتحديث المخزون؟	نعم	لا	غير متأكد	يوصى بالصيانة والمراقبة لجميع الأجهزة والبرامج.
4	هل هناك جدول زمني لاستبدال الأجهزة؟	نعم	لا	غير متأكد	تتبع الاتفاقيات والاستخدام لأصول الأجهزة والبرامج بطريقة نظامية قياسية مفيدة لبناء إدارة أصول دقيقة.
5	هل هناك جدول زمني لاستبدال / ترقية البرنامج؟ (عام - MS Office ، على مستوى الإدارات)	نعم	لا	غير متأكد	تتبع الاتفاقيات والاستخدام لأصول الأجهزة والبرامج بطريقة موحدة قياسية مفيدة لبناء إدارة أصول دقيقة.
6	هل هناك رقابة واضحة على نفقات تكنولوجيا المعلومات؟	نعم	لا	غير متأكد	من المهم تضمينها في ميزانيات الهيئة المحلية - يقترح خطة مدتها ثلاث سنوات.
7	هل هناك بروتوكول ثابت للنفقات السنوية لتكنولوجيا المعلومات، سواء من خلال الميزانية التشغيلية أو الميزانية العامة؟	نعم	لا	غير متأكد	عنصر أساسي يجب تضمينه في أي خطة لتكنولوجيا المعلومات.

ملحق رقم 3 :نموذج طلب لتقديم خدمة (خدمات الدعم التقني)

بلدية (.....)، نموذج طلب خدمة - خدمات الدعم التقني		
اسم الموظف		
هاتف		
الدائرة أو الفرع		
تاريخ طلب الخدمة		
الخدمة المطلوبة بشكل مختصر		
نوع الخدمة:	☐ طلب خدمة جديدة	☐طلب خدمة دعم فني لمشكلة

توقيع مسؤول الدّائرة:

ملحق رقم 4: نموذج طلب تغيير على النظام (خدمات الدعم التقني)

<table>
<tr><th colspan="5">بلدية (.....)
نموذج طلب تغيير على النظام</th></tr>
<tr><td colspan="5">اسم مقدم الطلب:</td></tr>
<tr><td colspan="5">اسم المنفذ:</td></tr>
<tr><th colspan="5">معلومات عن التغيير المطلوب</th></tr>
<tr><td colspan="5">نوع التغيير:</td></tr>
<tr><td colspan="5">سبب التغيير:</td></tr>
<tr><td colspan="5">أثر التغيير:</td></tr>
<tr><td colspan="3">موقع التغيير:</td><td colspan="2">النظام:</td></tr>
<tr><td colspan="5">عدد الموظفين أو الدوائر المتأثرة بالتغيير:</td></tr>
<tr><td>تاريخ البدء بالتغيير</td><td>وقت البدء بالتغيير</td><td>تاريخ الانتهاء من التغيير:</td><td colspan="2">وقت الانتهاء من التغيير:</td></tr>
<tr><td colspan="5"></td></tr>
<tr><td colspan="5">ملاحظات</td></tr>
<tr><td colspan="5">التوقيع: _____ التاريخ:_____</td></tr>
</table>

يجب تقديم هذا الطلب إلى الدعم الفني قبل (#) أيام، ويجب الحصول على موافقة المجلس الاستشاري قبل تطبيق أي تغييرات وفقط في حالة الطوارئ يتم الإسراع بالتنفيذ.

ملحق رقم 5: نموذج تقرير بالحوادث الكبرى (خدمات الدعم التقني)

بلدية _____		
نموذج تقرير بالحوادث الكبرى		
القسم الأول- وصف الحادث		
إرسال تقرير توضيحي كل 24 ساعة حول الحدث إلى حين انتهائه.		
الحادث:		
تاريخ وقوع الحدث: _____	تاريخ الإبلاغ عن الحدث: _____	
رقم الطلب لدى دائرة الدعم الفني:_____	الوقت المتطلب للإصلاح:_____	مدة استمرار الخلل: _____
القسم الثاني- تفاصيل الحدث		
نوع الحدث: ☐ خلل في النظام ☐ خلل في تطبيق ☐ أخرى		
سبب وقوع الخلل		
موقع الخلل	☐ مقر الهيئة المحلية الرئيسي ☐ مكتب خارجي	إذا كان مكتب خارجي، اسم المكتب وموقعه:
النظم المتأثرة:		التطبيقات المتأثرة
النظم/ المعلومات المتضررة:		
شدة الضرر		إمكانية عمل نسخة احتياطية عن المعلومات أو استعادة المعلومات المتضررة
وقت وقوع الخلل:_____	وقت إصلاح الخلل: _____	مدة استمرار الخلل بالدقائق: _____
القسم الثالث- الملخص		
الموظف المبلغ عن الحدث:		
ملخص الحدث:		
تسلسل الأحداث:		
الخاتمة		
الإجراءات المتخذة		
التوصيات		

ملحق رقم 6: نموذج استثناء أمان المعلومات

نموذج استثناء أمان المعلومات الخاص بالهيئة المحلية

الهدف

- تتحمل كل وحدة مسؤولية إكمال هذا النموذج عندما يكون استثناء أمان المعلومات من سياسات أو معايير أمان الهيئة المحلية يُرجى الرجوع إلى معايير أو سياسات الأمان.
- سيقوم مسؤول أمان المعلومات بمراجعة الطلب للموافقة عليه

القسم الأول: معلومات مُقدِّم الطلب

اسم مُقدِّم الطلب			تاريخ الطلب		
اسم الدائرة			رقم هاتف مقدم الطلب:		
رقم تذكرة خدمة الدعم الفني		تاريخ البدء		**تاريخ الانتهاء**	

القسم الثاني: معلومات الاستثناء

ينطبق هذا الاستثناء على	☐ اسم التطبيق: _____	☐ اسم الخادم أو الجهاز: _____	
	☐ أخرى: _____	☐ مستوى الوصول _____	
الهدف			
المواقع المتأثرة	الموقع الرئيسي ☐ الفرع ☐	إذا كان الفرع، يُرجي ذكر اسم الفرع (الفروع)	
وصف الاستثناء:			
مبرر الاستثناء:			
تفاصيل الاستثناء:			

مُلخص الاستثناء: