

سياسة و ضوابط أمن المعلومات الإلكترونية بمحافظة مسندم

الإصدار	التاريخ	الإعداد	مستوى الخصوصية	الإعتماد
2.0	أغسطس 2024	دائرة تقنية المعلومات	عام	محافظ مسندم



قائمة المحتويات:

3	مقدمة
3	الأهداف
4	المسؤوليات
5	نطاق تطبيق السياسة:
5	بيان السياسة:
6	ضوابط استخدام تخاويل دخول المستخدمين لنطاق شبكة المحافظة
7	ضوابط استخدام الموارد المعلومات والاتصالات
10	ضوابط استخدام البريد الإلكتروني الرسمي للمحافظة
12	ضوابط استخدام الإنترنت
13	ضوابط نقل المعلومات عبر الإنترنت
14	ضوابط استخدام كلمة المرور
15	ضوابط مواقع التواصل الاجتماعي الخاصة بالمحافظة
16	ضوابط استخدام حقوق الملكية الخاصة بالمحافظة
17	ضوابط حماية البيانات والخصوصية
18	معايير الاستثناء
18	الالتزام بالمعايير والقوانين واللوائح

التعريفات

في تطبيق أحكام هذه الضوابط يكون للكلمات والعبارات المعنى المحدد قرين كل منها ما لم يقتضي سياق النص خلاف ذلك:

الإدارة العليا: محافظ مسندم

المستخدم: هو أي شخص ذي صفة طبيعية (موظف أو غير موظف) أو اعتبارية عامة أو خاصة؛ مصرح له باستخدام الأنظمة المعلوماتية والأجهزة التقنية وأجهزة الاتصالات.

البنية الرئيسية: هي جميع الأجهزة ومتعلقاتها من غرفة البيانات والأجهزة الشبكية.

حساب المستخدم: البيانات السرية التي تخول المستخدم استخدام الأنظمة المعلوماتية، وتتكون في حدها الأدنى من اسم مستخدم وكلمة المرور.

الأنظمة المعلوماتية أو الموارد المعلوماتية: مجموعة برامج أو أدوات أو معلومات معدة لمعالجة البيانات وإدارتها وتشمل الحاسبات الآلية.

البيانات أو المعلومات الإلكترونية: كل ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنية المعلومات أيًا كان شكله كالكتابة والصور والأصوات والرموز والإشارات.

الوثائق الإلكترونية: البيانات المستخدمة لأغراض متعددة كالنماذج والخطابات والعقود والإحالات والتقارير والدراسات.

التعاملات الإلكترونية: أي تبادل أو تراسل أو تعاقد أو أي إجراء آخر يبرم أو ينفذ - بشكل كلي أو جزئي - بوسيلة إلكترونية.

الشبكة المعلوماتية: ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها مثل الشبكات الخاصة والعامة وشبكة الإنترنت الخاصة بالمحافظة.

الموقع الإلكتروني / البوابة الإلكترونية: مكان إتاحة المعلومات الإلكترونية على الشبكة المعلوماتية من خلال عنوان محدد.

البريد الإلكتروني الرسمي: هو البريد الإلكتروني المقدم من قبل المحافظة والمرتبط بالنطاق الخاص بها (mg.gov.om).

البريد الإلكتروني العام: هو البريد الإلكتروني غير المقدم من قبل المحافظة مثال (Hotmail, gmail)



مقدمة

قامت دائرة تقنية المعلومات بتطوير الضوابط الأساسية لأمن المعلومات بعد دراسة عدة معايير وأطر وضوابط لأمن المعلومات قامت بإعدادها سابقاً عدة جهات ومنظمات (محلية ودولية)، ودراسة متطلبات التشريعات والتنظيمات والقرارات الوطنية ذات العلاقة، وبعد الاطلاع على أفضل الممارسات والتجارب في مجال أمن المعلومات والاستفادة منها، وتحليل ما تم رصده من حوادث وهجمات سيبرانية على مستوى الجهات الحكومية وغيرها من الجهات الحساسة، ذات الطبيعة العمل المشابهة للمحافظة.

الأهداف

تهدف هذه الضوابط إلى توفير الحد الأدنى من المتطلبات الأساسية لأمن المعلومات الالكترونية المبنية على أفضل الممارسات والمعايير لتقليل المخاطر السيبرانية على الأصول المعلوماتية والتقنية للجهات من التهديدات الداخلية والخارجية. وتتطلب حماية الأصول المعلوماتية والتقنية للجهة التركيز على الأهداف الأساسية للحماية، وهي:



Availability

توافر المعلومة



Integrity

سلامة المعلومة



Confidentiality

سرية المعلومة

وتأخذ هذه الضوابط بالاعتبار اربعة محاور أساسية يركز عليها الأمن السيبراني، وهي:



الأشخاص



الاستراتيجية



التقنية



الإجراء

المسؤوليات

• الإدارة العليا :

1. ضمان تنفيذ سياسات حماية المعلومات في بيئة المحافظة لحماية الأصول والأنظمة.
2. ضمان توافق سياسات حماية المعلومات مع المتطلبات القانونية والتعاقدية للمحافظة.
3. الموافقة على استخدام أجهزة ونظم المعلومات التي توظف في معالجة وتخزين أو طباعة المعلومات الحساسة.
4. اعتماد السياسات الجديدة لحماية المعلومات أو الموافقة على تعديل السياسات الحالية.
5. الموافقة على طلبات الاستثناءات المقدمة من الموظفين والمستخدمين وفق حاجة العمل المبررة بالأسباب المقنعة.

• دائرة تقنية المعلومات :

1. نشر وثائق حماية المعلومات.
2. ضمان حماية نظم المعلومات والبنية التحتية وفقا للآليات التقنية المعتمدة من قبل جهات الاختصاص.
3. مراقبة وحماية الأنظمة والتطبيقات والشبكات.

• دور قسم أمن المعلومات:

1. القيام بالتدقيق الدوري لضمان تطبيق الضوابط والسياسات الأمنية في مختلف المستويات الوظيفية وعلى جميع قطاعات عمل المحافظة.
2. تحديد وإدانة سياسات حماية المعلومات والأصول التقنية
3. العمل وبشكل دوري على إعداد وتحديث السياسات والضوابط الأمنية اللازمة لرفع مستوى حماية المعلومات والأصول التقنية في المحافظة
4. تطبيق ضوابط ملائمة لحماية سرية وسلامة المعلومات الحساسة ووضع منهجية واضحة لتداولها والتصريح باستخدامها ونقلها إلى خارج المحافظة.

• دور المستخدم:

1. الالتزام بسياسات وضوابط ومعايير وإجراءات حماية المعلومات ومختلف الأصول التقنية.

2. الإبلاغ عن نقاط ضعف الحماية الفعلية أو تلك التي يشك بوجودها، والتي تؤثر على سرية وسلامة وتوافر المعلومات الحساسة.
3. استخدام المعلومات وفقا لسياسة الاستخدام المعتمدة.

نطاق تطبيق السياسة:

تطبق هذه السياسة على كل المستخدمين المخولين باستخدام أي شكل من أشكال موارد تقنية المعلومات ويمكنهم الدخول إلى خدمات / أنظمة شبكة المحافظة.

تسري أحكام الضوابط على أي موظف أو متدرب يعمل لدى المحافظة، كما تسري على أي طرف ثالث تتعاقد معه المحافظة لتنفيذ عمل ما.

بيان السياسة:

عند استخدام موارد وأصول تقنية المعلومات التابعة للمحافظة ينبغي على المستخدم مراعاة القوانين واللوائح المعمول بها في السلطنة ذات العلاقة وما يستجد عليها من تشريعات منظمة لاستخدام هذه التقنيات، ويتعين إتباع هذه القوانين والتقييد بالتعليمات والضوابط والأطر التي تحدد الطريقة المثلى للاستفادة من هذه الخدمات، كما ينبغي على المستخدم استشارة دائرة تقنية المعلومات لتلافي أي مسألة قد تترتب على سوء الاستخدام فيما لم يرد في هذه السياسة.

تشتمل هذه السياسة على الضوابط الأمنية الآتية:

- ضوابط استخدام تخاويل دخول المستخدمين لنطاق شبكة المحافظة (mg)
- ضوابط استخدام الموارد المعلوماتية والاتصالية.
- ضوابط استخدام البريد الإلكتروني.
- ضوابط استخدام الإنترنت.
- ضوابط استخدام كلمة المرور.
- ضوابط مواقع التواصل الاجتماعي.
- ضوابط استخدام حقوق الملكية الخاصة.
- ضوابط حماية البيانات والخصوصية.



ضوابط استخدام تخاويل دخول المستخدمين لنطاق شبكة المحافظة

1. أجهزة الحاسب الآلي التي توفرها دائرة تقنية المعلومات مخصصة لموظفي المحافظة الإداريين والفنيين ومن تخول لهم المحافظة استخدام هذه الموارد من الزوار والموردين والباحثين والمتعاقدين.
2. يتطلب الوصول إلى شبكة المحافظة واستخدام الإنترنت والبريد الإلكتروني وبوابة المحافظة الإلكترونيّة وقواعد البيانات والتطبيقات توفر تخويل دخول يحتوي على اسم المستخدم وكلمة المرور بطريقة رسمية من دائرة تقنية المعلومات.
3. يتعين على طالبي الخدمة التقدم لدائرة تقنية المعلومات للحصول على تخويل رسمي للدخول إلى الشبكة مع ضرورة وجود موافقة من المسؤول المباشر للموظف.
4. تسلم طلبات الخدمة للموظفين من قبل دوائهم التي ينتسبون إليها حيث تقوم دائرة تقنية المعلومات بإصدار تخاويل الدخول للموظفين الجدد وتسليمها إلى دوائهم.
5. الموظف أو المستخدم هو المسؤول بصفة كاملة عن سوء الاستخدام الذي يكون مصدره إعطاء كلمة المرور الخاصة به للآخرين أو نشرها سواء بطريقة متعمدة أو غير متعمدة.
6. تجنب استخدام الخدمات والأصول التقنية للمحافظة لأغراض شخصية أو الترويج لأفكار سياسية أو مخلة بالقيم الدينية والآداب والعادات والتقاليد.
7. على المستخدم التوقيع على قبول سياسة أمن المعلومات في المحافظة قبل السماح له باستخدام الموارد المعلوماتية. للمحافظة الحق في إيقاف حساب أي مستخدم للشبكة في حالة إساءة استخدامه للخدمات المقدمة له.

ضوابط استخدام الموارد المعلومات والاتصالات

1. يجب على المستخدمين المصرح لهم باستخدام الموارد المعلوماتية والاتصالية التقييد بجميع السياسات والإجراءات الخاصة بالأنظمة المعلوماتية التي يستخدمونها.
2. يجب على مستخدمي موارد المعلومات والاتصالات بالمحافظة باستخدامها بشكل مثمر ومسؤول ولأغراض تخص العمل فقط. ولا يجوز استخدامها لأغراض شخصية أو أغراض تخالف القوانين واللوائح المعمول بها في السلطنة، أو بما يؤدي إلى الإضرار بالمحافظة أو بسمعتها ويشمل ذلك على سبيل المثال لا الحصر:
 - استخدامها في أي عمل أو غرض غير شرعي.
 - استخدامها بما يتعارض مع الاخلاق والآداب العامة.
 - الدخول إلى حسابات المستخدمين أو محاولة استخدامها دون تصريح.
 - إشراك الآخرين في أي من حسابات الاستخدام أو التنازل لهم عن تلك الحسابات.
 - استخدام الخدمة أو استغلالها بطريقة تعرض الشبكة الداخلية للخطر أو فتح ثغرات أمنية في الشبكة أو نشر برمجيات ضارة أو غير ذلك.
 - تثبيت أو نشر برامج حاسب آلي غير مخول بها من قبل المحافظة وبدون الحصول على تصريح مسبق بذلك.
 - نشر مواد أو بيانات خاصة بالمحافظة أو أية مؤسسة حكومية أخرى دون التحويل من قبل الجهة الحكومية صاحبة البيانات وبدون إجراءات أمنية مناسبة تضمن سرية تلك البيانات.
 - انتحال شخصية أو جهاز آخر.
 - العبث بالمعلومات الخاصة بموظفين آخرين أو الاطلاع عليها.
 - نشر المعلومات الشخصية أو الخاصة بالآخرين دون تصريح بذلك.
 - محاولة فك تشفير بيانات الآخرين في الأنظمة المعلوماتية.
 - الإخلال بأي من حقوق النشر أو التأليف أو حقوق الملكية الفكرية لأي بيانات أو معلومات.
 - مراقبة الاتصالات الإلكترونية للمستخدمين (التجسس).
 - الاستخدام بشكل يؤثر سلباً على المستخدمين الآخرين أو على أداء الأجهزة والشبكات.
 - الاستخدام الذي من الممكن أن يتسبب في أي تهديد، أو تخريب، أو إزعاج، أو إهانة، أو مضايقة لأي شخص أو جهة أو أمنها الإلكتروني، مثل إرسال بريد إلكتروني بشكل متكرر أو غير مرغوب فيه أو لفرض الغش أو لخداع الآخرين.
 - إحداث أي تغيير في الموارد المعلوماتية أو الاتصالية للمحافظة دون امتلاك صلاحية.
 - إنشاء موقع إلكتروني يمثل المحافظة أو إدارتها دون إذن كتابي رسمي من صاحب الصلاحية.



- استخدام الموارد المعلوماتية والاتصالية لأغراض شخصية لا تخص المحافظة أو يشكل يؤدي إلى إهدارها. عدم استخدام قنوات اتصال بالموارد المعلوماتية والاتصالات الحكومية أو الارتباط بها إلا من خلال القنوات المتاحة من قبل المحافظة.
- يعتبر المستخدم مسؤولاً ومسؤولية كاملة عن كل ما يصدر من استخدام لجهازه أو من خلال الحاسب الخاص به وعليه الحرص على الدخول للموارد المعلوماتية المنوطة به.
- على المستخدم تجنب استخدام الموارد الخاصة بالآخرين أو تلك التي يتم توفيرها للاستخدام العام.
- على المستخدم استخدام أجهزة ونظم الحاسب الآلي بمسؤولية وحسب الأهداف التي وضعت من أجلها، متبعاً في ذلك تعليمات التشغيل الصحيحة وأن يطلب المساعدة إذا لزم الأمر من دائرة تقنية المعلومات.
- يحظر على المستخدم فتح الأجهزة أو القيام بأي أعمال صيانة أو إصلاح.
- يحظر على المستخدم تحريك أو نقل الأجهزة الغير محمولة كأجهزة الحاسب الآلي المكتبية والطابعات وغيرها من مكانها قبل التنسيق مع دائرة تقنية المعلومات.
- يحظر استبدال أو تعديل لبرامج ونظم التشغيل التي تم تنصيبها على الأجهزة إلا من قبل المختصين في دائرة تقنية المعلومات.
- يحظر المساس أو العبث بأنظمة وأجهزة الحاسب الآلي كما يحظر اللجوء إلى الاستخدام غير المصرح أو مقاطعة عملها الطبيعي بغض النظر عن موقع تلك الأجهزة أو النظم
- في حالة السماح للمستخدم بالاشتراك مع الآخرين في استخدام جهاز أو خدمة ما، عليه تجنب نسخ أو تعديل الملفات أو الاطلاع على بيانات الغير دون الحصول على موافقة مسبقة.
- يحظر اختراق ضوابط أو نظم الأمان التي وضعت كحماية موارد الحاسب الآلي كتجاوز الدخول والأرقام السرية.
- يعتبر المستخدم مسؤولاً عن جميع التعاملات على الشبكة الصادرة من حسابه. المستخدم مسؤول عن حفظ ونسخ الملفات والبيانات الخاصة به والمخزنة على جهازه المكتبي.
- يحظر استخدام موارد المحافظة لاختراق مواقع أو استخدام موارد معلومات محلية أو خارجية غير مصرح بها.
- يحظر استخدام ما يمكن أن يؤدي إلى الإضرار أو خلق مشاكل لنظم وشبكة المحافظة، كنشر الفيروسات أو فتح موارد المحافظة للآخرين أو حرمان الآخرين من استخدام خدمة ما.
- يحظر مراقبة حركة البيانات على الشبكة أو استخدام نظم لهذا الغرض إلا بتصريح مسبق من قبل المحافظة.

- يحظر لغير المختصين من دائرة تقنية المعلومات توصيل الأجهزة المصرح بها إلى شبكة الحاسب الآلي ويتعين استشارة الدائرة في هذا الشأن والحصول على موافقة الدائرة بالنسبة لتوصيل الأجهزة الأخرى.
- يحظر القيام بأي أنشطة أو خدمات على الشبكة مخلة بالقوانين وضوابط الخدمة.
- على المستخدم إبلاغ دائرة تقنية المعلومات في حالة حصول أي مشكلة في استخدام موارد تقنية المعلومات.

ضوابط استخدام البريد الإلكتروني الرسمي للمحافظة

1. ضرورة التزام الموظفين في المحافظة باستخدام البريد الإلكتروني الخاص بالمحافظة في كافة المراسلات الرسمية (الخارجية) وعدم استخدام موفر خدمة بريد إلكتروني خارجي لذات الغرض مثل (Gmail, Yahoo, Hotmail) وغيرها والالتزام بذلك.
2. لا يسمح بإرسال المستندات الرسمية سواء السرية منها وغير السرية الخاصة بالمحافظة إلى مستلمين غير مصرح لهم باستقبالها بما في ذلك إرسالها إلى البريد الشخصي للمستخدم.
3. كل موظف مسئول مسئولية منفردة عن الحفاظ على سلامة بريده الإلكتروني وتأمينه.
4. يجب أن تكون كافة حالات الدخول إلى سيرفر البريد الإلكتروني من خلال اسم مستخدم خاص وكلمة السر ولا يجوز لأي مستخدم أن يقرأ/ يرسل رسائل بريد إلكترونية باستخدام حساب مستخدمين آخرين.
5. في حالة وجود أي نشاط غير معتاد مثل رسائل البريد الإلكتروني الطفيلية "سام (Sam)" أو رسائل فيروسات فإنه ينبغي على المستخدم أن يبلغ عن ذلك إلى دائرة تقنية المعلومات.
6. لا يسمح بإعادة توجيه رسائل بريد إلكترونية رسمية إلى حساب بريد إلكتروني شخصي أو إلى حساب بريد إلكتروني رسمي أو عام لمستخدم آخر ما لم تتطلب حاجة العمل ذلك.
7. على المستخدم إبلاغ دائرة تقنية المعلومات عند الحاجة إلى نسخة احتياطية من رسائل البريد الإلكتروني.
8. لا ينبغي إرسال المعلومات عالية السرية مثل كلمة السر وغير ذلك عبر البريد الإلكتروني، وعند الحاجة إلى إرسال مستندات سرية فينبغي أن ترسل عبر البريد الإلكتروني الرسمي وأن تكون محمية بكلمة سر وينبغي إرسال كلمة السر إلى المستلم بطريقة آمنة أو مشفرة.
9. يحظر على المستخدمين تسجيل عناوين بريدهم الإلكتروني الرسمي الخاص بالعمل في المواقع غير المرغوب فيها والتي ليس لها علاقة بالعمل أو المنتديات العامة؛ حيث إن ذلك من شأنه أن يجعل المستخدم يتلقى رسائل بريد إلكترونية طفيلية رسائل بريد إلكترونية للتصيد.
10. يحق للإدارة العليا وفق الضوابط والإجراءات القانونية المعمول بها مراجعة محتوى البريد الإلكتروني لأي مستخدم إذا ما ساورها الشك في قيام ذلك المستخدم بالتورط في أعمال مريبة أو سلوك غير لائق. تعد المراسلات عن طريق البريد الإلكتروني للمحافظة ملكا لها ولإدارة حق الاطلاع على تلك المراسلات وفقا للقوانين المعمول بها في حالة وجود تحقيق رسمي أو الحاجة إلى ذلك. يحظر استخدام البريد الإلكتروني الشخصي في أي معاملات متعلقة بالمحافظة.



11. يقع على المستخدم مسؤولية البريد الإلكتروني الصادر من حسابه. يحظر إرسال رسائل بأسماء وهمية أو بتقمص شخصية الآخرين. يحظر قراءة أو مسح أو نسخ أو تعديل رسائل الآخرين. يحظر استخدام البريد الإلكتروني في إرسال رسائل تهديد أو تحرش أو إهانة أو غيرها.
12. يحظر استخدام البريد الإلكتروني الرسمي لأهداف تجارية أو للترويج لأفكار أو إرسال بريد لمجموعات أو لأفراد لا تخدم أهداف المحافظة. يجوز إنشاء قوائم بريدية لأهداف مشاريع مشتركة ولكن يحظر إرسال بريد لقوائم بريدية خارج نطاق العمل الجماعي أو لجميع مستخدمي البريد الإلكتروني في المحافظة دون الحصول على تصريح من الجهات المعنية بالمحافظة.
13. يقتصر استخدام خدمة البريد الإلكتروني بشكل أساسي على أغراض العمل ولا ينبغي للموظف استغلال البريد الإلكتروني الرسمي المخصص له في أغراض شخصية.
14. لا يحق للموظف إضافة مجموعات أخبار لا علاقة لها بالعمل إلى السجل الخاص لعناوين البريد الإلكتروني بالمحافظة.
15. يحظر استخدام خدمة البريد الإلكتروني لإرسال رسائل بريد إلكتروني طفيلية إلى المستخدمين الآخرين داخليا أو خارجيا.
16. يحظر الرد على الرسائل المشبوهة والتي تطلب تعبئة اسم المستخدم وكلمة السر.

ضوابط استخدام الإنترنت

1. يتطلب على الموظفين استخدام خدمة الإنترنت من خلال حصولهم على موافقة دائرة تقنية المعلومات.
2. يشترط استخدام الخدمة من قبل مزود خدمة الإنترنت الرسمي فقط ولا يسمح لأي مستخدم أن يتصل بالإنترنت عن طريق أي جهاز خارجي مثل أجهزة "مودم 4 جي 5 جي أو ربط الأجهزة الإلكترونية الذكية بالشبكة) حيث سيؤدي ذلك إلى فتح ما يسمى بالباب الخلفي للنظام.
3. يحظر استخدام تجهيزات هواتف الإنترنت أو برامج الاجتماعات التواصل عبر الإنترنت لمناقشة الأعمال التي تحمل طابع السرية.
4. يقتصر استخدام الإنترنت على الأغراض الخاصة بالعمل فقط ولا يسمح باستخدام أنظمة المحافظة وشبكاتها ومبانيها للدخول إلى المواقع التي لا علاقة لها بالعمل مثل حسابات البريد الإلكتروني العامة ومواقع المقامرة وبوابات الإنترنت والمواقع الإباحية والمواقع التي تحتوي على مواد ممنوعة والمواقع التي لا تتعلق بالعمل.
5. يحظر استخدام موارد المحافظة لإنشاء وصلات أو صفحات شخصية.
6. لا يجوز تنزيل أي برنامج أو تثبيتها دون الحصول على موافقة مسبقة من دائرة تقنية المعلومات.
7. يحظر استخدام كافة برامج المحادثات عبر الإنترنت باستخدام الإنترنت الخاص بالمحافظة.
8. ينبغي فحص كل المعلومات التي يتم تنزيلها عبر الإنترنت إلى أجهزة الحاسب الآلي بالمحافظة قبل استخدامها وذلك من خلال برامج للكشف عن الفيروسات أو طلب الدعم من المختصين في دائرة تقنية المعلومات.
9. يحظر استخدام موارد الإنترنت التي تخل بقوانين السلطنة والقيم السوية.
10. لا يسمح باستخدام تجهيزات أو معدات المحافظة في استخدامات مسيئة أو غير أخلاقية أو غير لائقة" وإلا سيتم اتخاذ الإجراءات القانونية.
11. يحظر نقل المعلومات السرية أو غير المسموح بتداولها عبر الإنترنت دون الحصول على موافقة مسبقة من الإدارة العليا واتخاذ التدابير الأمنية اللازمة (مثل التشفير أو غيره من الوسائل المناسبة).

ضوابط نقل المعلومات عبر الإنترنت

1. يحظر إرسال أسماء المستخدمين وكلمات السر المستخدمة لتسجيل الدخول وغير ذلك من البيانات الشخصية وبيانات النظام التي يمكن استخدامها في الحصول على الخدمات عبر الإنترنت بصيغة يمكن قراءتها.
2. يحظر على المستخدمين استخدام وصلات إنترنت جديدة أو موجودة لإقامة قنوات عمل جديدة دون الحصول على موافقة دائرة تقنية المعلومات.
3. يحظر وضع معلومات أو بيانات المحافظة في أي موضع أو على أية أجهزة متصلة بشبكات المحافظة الداخلية أو على الإنترنت ما لم يكن لدى جميع الأشخاص الذين يمكنهم الدخول إلى ذلك الموقع سبب مشروع للاطلاع عليها.
4. على المستخدم من أجل منع أي سلوك غير لائق على الإنترنت ولتقليل تعرض المحافظة للمخاطر الامتناع عن القيام بالآتي:
 - إبرام اتفاقيات تعاقدية عن طريق الإنترنت مثل إبرام عقود ملزمة بالنيابة عن المحافظة عبر الإنترنت.
 - استخدام شعارات أو مواد المحافظة في أية صفحة إنترنت أو نشرها عبر الإنترنت ما لم تكن الإدارة قد وافقت على ذلك مسبقاً.
 - استخدام صور أو ملفات البرمجيات أو غيرها من المعلومات التي تم تنزيلها من الإنترنت والتي لم يسمح للعامة باستخدامها مجاناً أو تلك التي لم تحصل المحافظة على ترخيص صريح باستخدامها. تقديم مواد غير لائقة أو مسيئة أو لها علاقة بإنتاج أو استخدام أو نقل مواد مسيئة أو تناول مواد إباحية تناو لا صريحاً على شبكة المحافظة أو أنظمتها.
 - محاولة الدخول غير القانوني إلى أنظمة بعيدة على الإنترنت. محاولة الدخول غير الملائم عن بعد إلى أنظمة بعيدة أو مسح منافذ تلك الأنظمة.
 - استخدام أو حيازة أدوات لمسح منافذ الإنترنت أو أدوات لتقييم مدى إمكانية اختراق التدابير الأمنية دون تصريح من دائرة تقنية المعلومات.
 - نشر مواد على الإنترنت بما يخالف قانون حقوق الطبع والنشر.
 - إنشاء وصلات شبكية خارجية يمكنها أن تسمح لمستخدمين آخرين بالدخول إلى أنظمة المحافظة ومواقع المعلومات بها.



ضوابط استخدام كلمة المرور

1. يحظر الإفصاح عن كلمات المرور أو كتابتها أو إرسالها بالبريد الإلكتروني أو التلميح بها أو مشاركتها أو أن يعرفها شخص غير المعني بذلك.
2. يحظر الدخول إلى أنظمة المحافظة ومصادرها بدون أسماء المستخدمين أو كلمات المرور الخاصة بهم.
3. يجب إبلاغ دائرة تقنية المعلومات فوراً إذا تم كشف كلمة المرور لمستخدمين آخرين.
4. يجب أن تعطل حسابات المستخدمين بينما هم خارج مكاتبهم لفترة طويلة.
5. يجب إلغاء حسابات المستخدمين بعد إنهاء خدماتهم من العمل أو استقالتهم فوراً.
6. يجب أن لا تكتب كلمة المرور الخاصة على الورق أبداً ولا يتم كتابتها أو إخفاؤها بالقرب من موقع العمل يجب أن تستخدم جميع أجهزة الحاسوب خاصية شاشة التوقف والتي تتطلب إدخال اسم المستخدم وكلمة المرور معاودة الوصول عند ترك النظام لفترة أطول من ثلاث دقائق.
7. على المستخدم تغيير كلمات المرور بعد مرور مدة زمنية وينصح بعدم إعادة استخدام كلمات المرور التي تم استخدامها مسبقاً.
8. يجب على المستخدمين إبلاغ دائرة تقنية المعلومات عند تعرضهم لسوء استخدام كلمات المرور الخاصة بهم.
9. يفضل تعقيد كلمة المرور، ومن الطرق اللازمة لذلك الآتي:
 - أن تكون بطول (8) وحدات على الأقل.
 - أن تحتوي على حروف و أرقام.
 - أن تحتوي على رموز مثل: @\$% متى ما أمكن ذلك.
 - أن تتنوع بين أحرف صغيرة وكبيرة.
 - أن لا تتضمن جزء من الاسم الشخصي أو العنوان أو تاريخ الميلاد أو اسم العائلة أو الألقاب المتداولة.

ضوابط مواقع التواصل الاجتماعي الخاصة بالمحافظة

1. لا يسمح لأي موظف أن ينشر على أي موقع من مواقع التواصل الاجتماعي بالنيابة عن المحافظة دون الحصول على موافقة رسمية.
2. احترام أية معلومات تعود ملكيتها إلى جهة معينة إضافة إلى احترام محتواها وسريتها.
3. التمهّل والتروي دائماً قبل الإرسال أو الرد على التعليقات والملاحظات.
4. لا يجوز إرسال رسائل ليس لها علاقة بالموضوع أو مسيئة.
5. يحظر استخدام عبارات غير لائقة عند النقاش مع الآخرين.
6. عدم تجاوز نطاق الخبرة عند مناقشة موضوع ما على أن يكون الرأي صحيحاً وفردياً.
7. أن لا يستخدم مواقع التواصل الاجتماعي المصالح الشخصية أو أغراض تجارية.

ضوابط استخدام حقوق الملكية الخاصة بالمحافظة

1. برامج الحاسب الآلي والمواد السمعية والمرئية وغيرها لها حقوق ملكية وهي خاضعة لتخاويل استخدام ولا يجوز استخدامها إلا حسب الضوابط المتبعة في هذا الشأن
2. يحظر استخدام نظم البرمجة والتطبيقات الشخصية على أجهزة المحافظة بغض النظر عن امتلاك لحقوق الاستخدام.
3. تجنب نسخ البرمجيات والتطبيقات الخاصة بالمحافظة للاستخدام الخاص أو المنزلي دون الحصول على تصريح من دائرة تقنية المعلومات.

ضوابط حماية البيانات والخصوصية

1. على الموظفين حماية أجهزة الحاسب الآلي التي بحوزتهم باستخدام ميزة الرقم السري في حامي الشاشة.
2. على الموظفين الحذر عند مشاركة الآخرين على الشبكة للبيانات المخزنة على الأجهزة الشخصية، وإذا كان لابد من مشاركة الآخرين فعليهم استخدام وسائل الحماية المتيسرة كتحويل الدخول والأرقام السرية وإعطاء إمكانيات محدودة للآخرين لاستخدام الموارد التي بحوزتهم واتباع تعليمات دائرة تقنية المعلومات في هذا الشأن.
3. يتعين على الموظفين حماية البيانات المتداولة عبر الرسائل البريدية والبيانات الأخرى إذا كانت سرية باستخدام نظم وآليات الحماية المخصصة لذلك.
4. لدائرة تقنية المعلومات الحق في مراقبة التعاملات على الشبكة كلما كان ذلك ضروريا.



معايير الاستثناء

تهدف هذا السياسة إلى معالجة موضوع متطلبات حماية المعلومات وعند الحاجة الى استخدام بيانات أو معلومات إلكترونية أو برامج غير متاحة وغير متوفرة فيمكن التقدم بطلبات الحصول على استثناءات بصورة رسمية إلى دائرة تقنية المعلومات، مع توضيح مسوغات الاستثناء والمزايا التي قد تنجم عنه ومن ثم الحصول على الموافقة الرسمية عليها.

الالتزام بالمعايير والقوانين واللوائح

1. على موظفي المحافظة الالتزام بالسياسات والضوابط المذكورة أعلاه.
2. على موظفي المحافظة الالتزام بالقوانين واللوائح التي تنظم استخدام تقنية المعلومات والاتصالات.

يتوافق هذا الإصدار مع الضوابط والأطر والسياسات التي وردت في تعاميم وزارة النقل والاتصالات وتقنية المعلومات (هيئة تقنية المعلومات سابقا) التالية:

- تعميم رقم (4/2012) بشأن استخدام البريد الإلكتروني الحكومي في المراسلات الرسمية.
- تعميم رقم (1/2013) سياسات وضوابط أمن المعلومات بالمؤسسات الحكومية (السياسة الأمنية لاستخدام شبكة المعلومات الدولية (الإنترنت) والبريد الإلكتروني.
- تعميم رقم (3/2015) بشأن السياسة العامة لأمن المعلومات (ضوابط استخدام وسائل الاتصالات والحاسبات الآلية وشبكة المعلومات الدولية (الإنترنت) في الجهات الحكومية).
- التعميم الصادر بالرسالة رقم (111/2016) بشأن إتباع عدد من الضوابط للتقليل من المخاطر المرتبطة بالبريد الإلكتروني والمواقع الإلكترونية والحفاظ على خصوصية البيانات.