سياسات المستخدم – الهيئة الوطنية لأمن وسلامة المعلومات

/nissa.demo.ly/policies

سياسة كلمة السر أو المرور

الهدف من السياسة

تعتبر كلمة المرور أو كلمة السر عنصراً مهماً في مجال أمن المعلومات. فهي تستخدم كإثبات للهوية للموافقة على الوصول وذلك لحماية المستخدمين وحفظ خصوصيتهم، ولحماية البيانات والأنظمة والشبكات. على سبيل المثال يتم استخدامها لمصادقة مستخدمي أنظمة التشغيل والتطبيقات مثل البريد الإلكتروني والوصول عن بعد، كما تستخدم أيضًا لحماية الملفات والمعلومات المخزنة الأخرى. وفي ظل هذه الحاجة إلى كلمات المرور لأمور ذات أهمية عالية اقتضى ذلك تركيب كلمات سر قوية ذات تشفير عالي، بحيث لا يمكن لأحد توقعها أو استنتاجها.

الغرض من السياسة

الغرض من هذه السياسة هو تحديد سياسات وإجراءات كلمة السر/المرور لتقديم أفضل مستوى للخدمة مع أعلى درجات الحماية والخصوصية للمستخدمين.

نطاق تطبيق السياسة

تسري هذه السياسة على جميع الموظفين في **(جهة العمل)** وتطبق على جميع كلمات المرور المستخدمة على كافة الأجهزة وملحقاتها والخدمات المرتبطة بها والأنظمة وفي جميع التطبيقات التي تعد جزءًا من شبكة **(جهة العمل)** التي توفر الوصول إلى بيانات **(جهة العمل)** المملوكة.

آلية تنفيذ السياسة

1. فرض كلمة مرور قوية: يجب أن تكون كلمة المرور قوية وألا تتضمن في تركيبها الكلمات التي يسهل على الأخرين إيجادها، وذلك وفق الآتي:

- يجب استخدام توليفة من الأحرف الكبيرة والصغيرة، مع أرقام، ورموز أو علامات الترقيم قدر الإمكان عند اختيارك لكلمة السر/المرور.
- لا يجب استخدام كلمات سر رائجة والتي يمكن التكهن بها بسهولة، كالأسماء وتاريخ الميلاد أو أرقام الهواتف.
- يجب ألا يقل عدد رموز كلمة السر/المرور عن 12 رمزاً.
- لا يجب استعمال اسم المستخدم في كلمة السر.
- لا يجب استخدام أرقاماً أو حروف متكررة مثل (3333 أو AAAA).
- في حالة اختيار كلمة تقليدية يفضل خلط حروفها بحيث لا تعطي معني متعارف عليه.
- يفضل أن تكون كلمة المرور "جملة مرور" لا يفهمها ألا المستخدم، مُكونة من تركيبة الأحرف والأرقام والرموز.
- تطبيق ضوابط صارمة على كلمات المرور على مستوى النظام وكلمة مرور الحسابات المشتركة.

2. يجب تخزين كلمة المرور بطريقة آمنة تضمن عدم كشفها

- يجب التعامل مع جميع كلمات المرور في (جهة العمل) على أنها بيانات سرية.
- لا يحتفظ بكلمات المرور كنص عادي يمكن قراءته، وإنما يتم حفظ كلمات السر على شكل نص مشفر لا يمكن فكه أو استخدامه من الشخص المخول.
- يجب ألا يتم تخزين كلمات المرور على أنظمة الكمبيوتر في شكل غير محمي.
- كلمات المرور للأنظمة (جذر النظام/مسؤول النظام Root/Administrator) يجب أن تخزن باستعمال برمجيات حفظ كلمات المرور بطريقة مشفرة.
- يجب ضمان عدم تفعيل خاصية حفظ كلمة المرور في المتصفح وإدخال البيانات في كل مرة من جديد.

3. الحفاظ على سرية كلمات المرور: يجب عدم مشاركة أو كشف كلمة المرور مع أي شخص لأي سبب من الأسباب.

- يجب عدم أفشاء كلمة المرور وعدم كتابتها بطريقة صريحة مما يجعلها عرضة للاطلاع أو حتى التلميح عن تركيبتها، إلا في حالةِ الضرورةِ القصوى ويجب تغييرها بعد الكشف عنها.
- يجب أخد الحذر من الأشخاص المتطفلين عند طباعة لكلمة السر/المرور أثناء عملية الولوج.
- يمنع إرسال كلمة المرور عبر البريد الإلكتروني أو من خلال أي وسيلة عبر الأنترنت.
- يجب تغيير كلمات المرور إذا ظهر أي مؤشر على احتمال اختراق للنظام أو لكلمة المرور.
- يجب تغيير كلمات المرور المستخدمة للحسابات المشتركة على الفور في حالة اختراقها أو عندما يغادر مالكها (جهة العمل).
- لا يجب استخدام نفس كلمة المرور لحسابات المسؤولين المتعددة.
- يجب على المستخدمين قدر الإمكان عدم استخدام كلمة المرور نفسها لحسابات مختلفة في (جهة العمل).
- يجب على المستخدمين عدم استعمال ذات كلمة المرور للحسابات والأجهزة داخل (جهة العمل) والحسابات والأجهزة الأخرى خارجها.

4. كلمات المرور الأولى (المؤقتة): يجب تغيير كلمات المرور الأولية للمستخدمين وفرض مدة انتهاء لصلاحيتها لإجبار المستخدم على تغييرها.

- على المستخدم تغيير كلمة المرور الأولية التي يستلمها من الجهة المختصة في أول استخدام له وقبل انتهاء وقت صلاحيتها؛ وذلك لضمان عدم تسريب كلمة السر لمستخدمين آخرين.
- يجب إعطاء كلمات المرور المؤقتة للمستخدمين بطريقة آمنة؛ ينبغي تجنب نقلها على ورقة مكشوفة (نص عادي) أو عن طريق أطراف ثالثة أو رسائل البريد الإلكتروني غير المحمية (النص الواضح) .
- وضع إجراءات للتحقق من هوية المستخدم قبل تقديم كلمة مرور جديدة أو بديلة أو مؤقتة.
- يجب على المستخدمين الإقرار باستلام كلمات المرور المؤقتة.

5. يتطلب فحص كلمات المرور الجديدة في قوائم كلمات المرور شائعة الاستخدام أو المخترقة.

6. يجب منع الولوج للأنظمة الداخلية والخاصة بعد 3 محاولات خاطئة خلال مدة زمنية لا تتجاوز 15 دقيقة. ويستمر المنع لمدة أقلها 30 دقيقة وأكثرها 3ساعات.

7. يجب على المستخدم في حالة أن يشتبه أو يلاحظ وجود مشكلة أمنية أو أن كلمة المرور الخاصة به قد تعرضت للاختراق الإبلاغ عن الحادث وتغيير جميع كلمات المرور.

8. يجب أن يُطلب من المستخدمين التوقيع على بيان للحفاظ على سرية كلمات المرور الشخصية؛ يمكن تضمين هذا البيان في شروط التوظيف.

9. يجب أن يكون المستخدم على علم ودراية أنه المسؤول الوحيد عن حماية كلمة السر/المرور الخاصة به.

سياسة استعمال البريد الإلكتروني

الهدف من السياسة

يعتبر البريد الإلكتروني أداة اتصال أساسية في معظم مجالات الأعمال لسرعته وفعاليته العالية، ولأنه أصبح وسيلة معتمدة وتعبر عن الجهة المرسلة، أصبح من الضروري وضع سياسة استخدامه تفادياً للمشاكل التي قد تحدث بسبب سوء الاستخدام.

الغرض من السياسة

تحديد سياسات وإجراءات التعامل بالبريد الإلكتروني من خلال البنية الأساسية لشبكة **(جهة العمل)**، والتي يستهدف من خلالها حصول المستخدمين على أعلى درجات الحماية والتقليل من أضرار الاختراق وضمان استخدام مهني.

نطاق تطبيق السياسة

تسري هذه السياسة على جميع الموظفين الذين يمكنهم استخدام البريد الإلكتروني في **(جهة العمل)** وجميع المصنعين والعملاء الذين يعملون باسم **(جهة العمل)**، وعلى نظام البريد الإلكتروني المستخدم داخل **(جهة العمل)**.

آلية تنفيذ السياسة

1. حساب البريد الإلكتروني:

- يمنح كل موظف حساب بريد إلكتروني، ويجب أن يكون محدد بشكل فريد لكل مستخدم.
- عند إنشاء بريد إلكتروني جديد للمستخدم، يجب على المستخدم تغيير كلمة المرور الأولية الخاصة به في تسجيل الدخول التالي، حيث يجب تكوين النظام يفرض على المستخدمين تغيير كلمات المرور الأولية الخاصة بهم.
- يجب أن تكون كلمة مرور البريد الإلكتروني الخاصة بالمستخدم تتوافق مع سياسة كلمة المرور الصادرة عن (جهة العمل).
- يجب التحكم في حجم صندوق البريد من خلال تحديد سعة الحصة المخصصة، وكل مستخدم مسؤول إذا تجاوز السعة المحدودة، لذا يجب على المستخدم أرشفة الرسائل المهمة بشكل دوري وحذفها من البريد الوارد.

2. استخدام البريد الإلكتروني: يجب على جميع المستخدمين التقيد بما يلي عند استخدام البريد الإلكتروني الخاص بـ (جهة العمل):

- يجب أن يكون استخدام البريد الإلكتروني متوافقاً مع سياسات (جهة العمل) وإجراءاتها ومع القوانين المعمول بها والممارسات السليمة والامتثال للقوانين المعمول بها.

- يجب استخدام حسابات البريد الإلكتروني لـ(جهة العمل) لأعمال تتعلق بـ(جهة العمل)، حيث يستخدم لمساعدة الموظفين في تأدية وظائفهم.
- لا ينبغي استخدام البريد الإلكتروني المخصص للموظف لأغراض شخصية.
- يجب تأمين جميع بيانات (جهة العمل) الواردة في رسالة بريد إلكتروني أو مرفق طبقًا لسياسة حماية البيانات.
- يجب توخي الحذر عند إرفاق المستندات أو الملفات بالبريد الإلكتروني، فقد تكون هذه المرفقات تابعة للآخرين، وإعادة توجيه هذه البيانات إلى مستلم آخر دون الحصول على إذن من المرسل قد يعتبر انتهاكاً لحقوق الطبع والنشر.
- يجب على جميع المستخدمين توخي الحذر عند فتح رسائل البريد الإلكتروني والمرفقات من مصادر غير معروفة.
- يجب على جميع المستخدمين ضمان أن يكون محتوى البريد الإلكتروني دقيقًا وواقعيًا وموضوعيًا، حيث يجب تجنب الآراء الشخصية حول الأفراد أو المؤسسات الأخرى.
- يجب أن يدرك المستخدمون أن رسائل البريد الإلكتروني قد تخضع للتدقيق للتأكد من أنها تلبي متطلبات هذه السياسة. ينطبق هذا على محتوى الرسائل والمرفقات والعناوين ورسائل البريد الإلكتروني الشخصية.
- تعتبر جميع الرسائل المرسلة عبر نظام البريد الإلكتروني الخاص لـ(جهة العمل) ملكية خاصة بـ(جهة العمل) وتشمل رسائل البريد الإلكتروني الشخصية أيضاً. يجب ألا يكون لدى المستخدم أي توقع للخصوصية في أي شيء يقوم بإنشائه أو تخزينه أو إرساله أو استلامه على نظام البريد الإلكتروني الخاص بـ(جهة العمل).
- يمكن مراقبة الرسائل الإلكترونية دون إخطار مسبق إذا رأت (جهة العمل) ذلك ضروريًا. إذا وجد دليل على أن الموظف لا يلتزم بالتوجيهات المنصوص عليها في هذه السياسة، تحتفظ (جهة العمل) بالحق في اتخاذ إجراءات تأديبيه وفق اللوائح المعمول بها.
- يجب انتقاء الألفاظ اللائقة وعدم كتابة أي لفظ مسيء أو مهين للآخر.
- يجب على المستخدمين عدم الإفصاح عن كلمات المرور الخاصة بحساباتهم أو السماح لأي شخص آخر باستخدام حساباتهم، كما يجب عدم استخدام حساب مستخدم آخر.
- في الحالات التالية (الاستقالة، الفصل/الطرد، الإيقاف) سوف يتم أعلام الموظف بأنه سيتم قفل حساب بريده الإلكتروني ومنحه فرصة محددة لنسخ وأرشفة محتويات بريده.
- يجب على من يتعرف على أو يلاحظ وجود مشكلة أمنية فعلية أو مشتبه بها، الاتصال على الفور بقسم أمن المعلومات في (جهة العمل) والإبلاغ بشكل فوري.
- إرفاق كل رسالة بتوقيع نصي في النهاية يحمل الاسم والوظيفة ورقم الهاتف والقسم التابع له واسم (جهة العمل).
- على المستخدم أخذ العلم والدراية أنه المسؤول الوحيد عما تحتويه الرسائل المرسلة من خلال حساب بريده الإلكتروني.
- يجب على المستخدمين ضمان إرسال رسائل البريد الإلكتروني إلى المستخدمين الذين يحتاجون إلى معرفة الأمر فقط.

3. الاستخدام الغير مقبول للبريد الإلكتروني: تعد الممارسات التالية غير مقبولة عند استخدام البريد الإلكتروني الخاص بـ(جهة العمل):

- استخدام نظام البريد الإلكتروني لـ(جهة العمل) لإنشاء أو توزيع أي رسائل مدمرة أو هجومية. يجب على الموظفين الذين يتلقون أي رسائل بريد إلكتروني بهذا المحتوى من أي موظف بـ(جهة العمل) إبلاغ الأمر إلى المسؤول على الفور.

- استخدام حساب البريد الإلكتروني لـ(جهة العمل) لتسجيل الدخول في أي من مواقع الشبكات الاجتماعية ما لم يكن ذلك لأغراض العمل، كما يجب الحصول على موافقة من الإدارة العليا لذلك.
- استخدام هوية مزيفة في رسائل البريد الإلكتروني الخاصة بـ(جهة العمل).
- العبث بمحتوي وعناوين الرسائل المعاد توجيهها أو مرفقاتها بدون توضيح ذلك بشكل صريح.
- إرسال رسائل بريد إلكتروني غير مرغوب فيها بما في ذلك إرسال "بريد غير هام" JUKE MAIL ، أو مواد إعلانية إلى أفراد لم يطلبوها تحديداً كـ (رسائل البريد الإلكتروني المزعج SPAM).
- استخدام غير مصرح به لمعلومات البريد الإلكتروني أو تزويرها.
- إنشاء أو إجراء تحويل لـــ "سلسلة رسائل chain letters "، "بونزي Ponzi " ، أو أي أشكال هرمية من أي نوع .
- استخدام رسائل بريد غير مرغوب بها داخل شبكات (جهة العمل) لمزودي خدمات آخرين نيابة عن أو للدعاية لأي خدمة مستخدمة من قبل (جهة العمل) أو متصلة عبر شبكتها.
- نشر الرسائل غير ذات العلاقة بالعمل أو ما شابه ذلك لعدد كبير من مجموعات الأخبار newsgroups أو ما يسمى بـ (newsgroup spam).
- تغيير محتوى و/أو عناوين البريد الإلكتروني للرسائل المعاد توجيهها أو مرفقاتها دون الحصول على موافقة.

سياسة استخدام الإنترنت

الهدف من السياسة

يعتبر الإنترنت أحد أكثر مصادر المعلومات استخدامًا، فهو يوفر موارد متعددة من البيانات والأفكار والأبحاث والأخبار، ويسهّل على المستخدمين الحصول على المعلومات والبيانات لتشجيعهم على إجراء الأبحاث وتبادل المنافع.

الوصول إلى الإنترنت من قبل الموظفين بشكل يتعارض مع احتياجات العمل قد يؤدي إلى إساءة استخدام الموارد، وهذا قد يعرض **(جهة العمل)** لمخاطر يجب معالجتها لحماية أصول المعلومات الخاصة بـ**(جهة العمل)**. بالإضافة إلى ذلك قد تواجه **(جهة العمل)** خطر تشويه السمعة أو التعرض لمشاكل قانونية من خلال أنواع أخرى من سوء الاستخدام. يساعد اتباع **سياسة استخدام الإنترنت** في حماية كلاً من الموظف والمؤسسة من تبعات سوء استخدام الإنترنت.

الغرض من السياسة

تهدف هذه السياسة إلى تحقيق الاستخدام الآمن للإنترنت وذلك بتزويد الموظفين بالقواعد والمبادئ التوجيهية حول الاستخدام الملائم لمعدات وشبكة **(جهة العمل)** والاتصال بالإنترنت لضمان استخدام الموظفين للإنترنت بطريقة آمنة وأكثر فاعلية.

نطاق تطبيق السياسة

تنطبق هذه السياسة على جميع مستخدمي الإنترنت (الموظفين وجميع الأطراف الثالثة) الذين يتصلون بالأنترنت من خلال أجهزة الكمبيوتر أو الشبكات الخاصة بـ**(جهة العمل)** والخدمات المرتبطة بها.

آلية تنفيذ السياسة

1. استخدام الموارد:

- يتم الموافقة على الوصول إلى الإنترنت فقط إذا تم تحديده ضمن احتياجات العمل. يتم منح خدمات الإنترنت على أساس مسؤوليات الوظيفة الحالية للموظف.
- ستقوم إدارات (جهة العمل) بمراجعة متطلبات وصول المستخدمين إلى الإنترنت بشكل دوري لضمان استمرار احتياجهم للإنترنت.
- يصرح لمستخدمي الأنترنت في (جهة العمل) باستخدامها لأغراض تخص العمل وبطريقة لا تخالف الأنظمة واللوائح المعمول بها في (جهة العمل)، أو بما يؤدي إلى الإضرار بها او بسمعتها.
- لا تكفل (جهة العمل) دقة المعلومات التي يتم الحصول عليها عن طريق الإنترنت، ذلك يقع على عاتق مصدر ومنتج هذه المعلومات.
- تحتفظ (جهة العمل) بحق فرض السعة المسموح بها لاستعمال الاتصال بالإنترنت حسب ما تراه الجهة الفنية المختصة وبما يتناسب مع متطلبات كل إدارة.

2. الاستخدام المسموح

- التواصل بين الموظفين وغير الموظفين لأغراض العمل.
- ما يقوم به فنيي دعم تكنولوجيا المعلومات من تنزيل لتحديثات البرامج والتصحيحات.
- استعراض مواقع الويب للبائعين المحتملين للحصول على معلومات عن المنتجات.
- مراجعة المعلومات التنظيمية أو البيانات الفنية.
- إجراء الأبحاث.

3. الاستخدام الشخصي:

- قد يُعد استخدام أجهزة كمبيوتر (جهة العمل) للوصول إلى الإنترنت لأغراض شخصية، دون موافقة مدير المستخدم وقسم تكنولوجيا المعلومات، سببًا لاتخاذ إجراءات تأديبيه حسب اللوائح المعمول بها.
- يجب أن يكون جميع مستخدمي الإنترنت مدركين أن شبكة (جهة العمل) تقوم بإنشاء سجل تدقيق يبين طلب الخدمة، سواء في العناوين الداخلية أو الخارجة، حيث يتم مراجعتها هذه السجلات بشكل دوري.
- المستخدمون الذين يختارون تخزين أو نقل المعلومات الشخصية مثل المفاتيح الخاصة أو أرقام بطاقات الائتمان أو الشهادات أو الاستفادة من "محافظ" الإنترنت يقومون بذلك على مسؤوليتهم الخاصة. (جهة العمل) ليست مسؤولة عن أي فقدان للمعلومات، مثل المعلومات المخزنة في المحفظة، أو أي ما قد ينتج من خسائر لاحقة للممتلكات الشخصية.
- المستخدم مسؤول مسؤولية كاملة عن أجهزة الكمبيوتر الخاصة به واستخدامها، وعليه أن يكون على دراية بأمن وحفظ موارد تكنولوجيا المعلومات.
- يجب على المستخدمين الذين يتعرفون على أو يلاحظون وجود مشكلة أمنية فعلية أو مشتبه بها، الاتصال على الفور بالقسم المختص في (جهة العمل) والإبلاغ بشكل فوري.

4. الاستخدام المحظور:

- يمنع منعاً باتاً استخدام الأنترنت أو استغلالها بطريقة تعرض شبكة (جهة العمل) للخطر، أو فتح ثغرات أمنية في الشبكة أو نشر برمجيات ضارة أو غير مشروعة.
- لا يجوز انتحال شخصية الأخرين أو جهاز آخر.
- يمنع استخدام اسم (جهة العمل) أو أي من أقسامها أو أي من موظفيها دون إذن كتابي رسمي.
- يمنع العبث بالمعلومات الخاصة بموظفين آخرين أو بجهات أخرى أو الاطلاع عليها بشكل غير قانوني.

- يمنع نشر المعلومات الخاصة بـ (جهة العمل) أو الخاصة بالآخرين دون إذن صريح بذلك.
- يمنع محاولة فك تشفير بيانات الآخرين في الأنظمة المعلوماتية بدون تصريح رسمي من الجهة المعنية.
- لا يجوز الإخلال بأي من حقوق النشر أو التأليف، أو حقوق الملكية الفكرية لأي بيانات، تطبيقات، برامج أو معلومات.
- يمنع مراقبة الاتصالات الإلكترونية للمستخدمين الآخرين لغرض التجسس وانتهاك الخصوصية.
- لا يجوز استخدام الأنترنت بشكل يؤثر سلباً على المستخدمين الآخرين، أو على أداء الأجهزة والشبكات.
- يمنع استخدام الأنترنت لأي أغراض غير قانونية أو غير شرعية. ومن الأمثلة على ذلك إرسال مواد عنيفة أو تهديدية أو خداعية أو إباحية أو فاحشة أو غير قانونية أو غير شرعية والذي يمكن أن يتسبب في أي تهديد، أو تخريب، أو إزعاج، أو مضايقة لأي شخص أو جهة أو أمنها السيبراني.
- يمنع إهدار الموارد المعلوماتية، أو إحداث أي تغيير في الموارد المعلوماتية دون امتلاك صلاحية تخول ذلك.
- يمنع إنشاء موقع إلكتروني أو حساب على مواقع التواصل الاجتماعي يمثل (جهة العمل)، أو إدارتها أو أي جزء منها دون إذن كتابي رسمي من صاحب الصلاحية.
- عدم استخدام قنوات اتصال بالموارد المعلوماتية الأخرى أو الارتباط بها إلا من خلال القنوات المتاحة والمصرح بها رسمياً من (جهة العمل).
- يمنع استخدام الموارد المعلوماتية بشكل يؤدي إلى إهدار وقت الموظف.
- يجب عدم استخدام الاتصال بالإنترنت الخاص بـ (جهة العمل) لأغراض تجارية أو سياسية، أو بهدف تحقيق ربح شخصي أو تجاري أو تسويقي.
- يمنع إنشاء نسخ إلكترونية غير مصرح بها من المستندات والوثائق التي تخص (جهة العمل) وإداراتها أو لأي مواد محمية بحقوق نشر لغرض نشرها أو إرسالها عبر شبكة (جهة العمل).

سياسة أمان محطات العمل (الكومبيوتر وملحقاته)

الهدف من السياسة

تستخدم أجهزة الكمبيوتر وملحقاتها (طابعات، ماسحات ضوئية، أجهزة كمبيوتر محمولة، الخ) في أداء العمل يومياً بطريقة معقولة ومتناسبة مع أهداف واستراتيجيات **(جهة العمل)**، ولتقديم أفضل مستوى للخدمة مع أعلى درجات الحماية والخصوصية للمستخدمين، وضعت **"سياسة محطات العمل"** لضمان استخدام مهني لمحطات العمل.

الغرض من السياسة

تهدف هذه السياسة لحماية المستخدم ومحطات العمل من المخاطر المحتملة وذلك بتحديد سياسات وإجراءات استخدام أجهزة الكمبيوتر وملحقاتها في **(جهة العمل)**.

نطاق تطبيق السياسة

تسري هذه السياسة على جميع الموظفين والمستخدمين الذين يستعملون أجهزة الكمبيوتر وملحقاتها والخدمات المرتبطة بها.

آلية تنفيذ السياسة

1. يسمح للمستخدم باستعمال أجهزة الكمبيوتر المخصصة له، أو التي المصرح له باستعمالها. ولا يجوز استخدام أجهزة الآخرين، أو محاولة الدخول عليها.
2. تقع المسؤولية الكاملة على المستخدم للاستخدام الملائم لجميع الموارد المخصصة له بما فيها من أجهزة الكمبيوتر وملحقاتها أو برمجيات الأجهزة.
3. لا يسمح للمستخدمين بالوصول إلى الشبكة باستخدام الحواسيب الشخصية واللوحية والهواتف الذكية. ألا بتصريح من الإدارة الفنية المختصة.
4. يجب عدم محاولة الوصول إلى أجزاء ممنوعة الوصول من الشبكة، مثل نظام التشغيل الرئيسي، برامج الأمان وغيرها دون الموافقة من الإدارة المختصة.
5. يجب عدم وضع أو تنصيب أو استخدام أي برامج أو أدوات أو أجهزة قد تؤدي إلى أو تساعد على تلف البرامج أو الأجهزة أو مكونات النظام.
6. يمنع تثبيت أو استخدام الأدوات التي عادةً ما تستخدم لمهاجمة أنظمة الأمن أو اختراق أنظمة الكمبيوتر أو الشبكات الأخرى (مثل كاشفات كلمات السر أو ماسحات الشبكة... إلخ).
7. يجب احترام الخصوصية الشخصية وحقوق الآخرين وعدم الحصول على بيانات تخص مستخدم آخر، إضافة إلى البرامج أو الملفات الأخرى من دون إذن مسبق.
8. يطلب موافقة خاصة من قسم تقنية المعلومات قبل تنصيب أي برامج أو تركيب أجهزة خاصة على أنظمة (جهة العمل).
9. أجهزة الكمبيوتر تعتبر إعارة من (جهة العمل) لذا فهي للاستخدام الرسمي لـ(جهة العمل) فقط ولا يجوز استخدامها من قبل أفراد الأسرة أو الأصدقاء تحت أي ظرف من الظروف.
10. عند إرجاع جهاز الكمبيوتر، تحتفظ إدارة تقنية المعلومات بالحق في تنظيف القرص الثابت من أي بيانات وإعادة تثبيت كافة البرامج المبدئية. المستخدم مسؤول عن أي بيانات يتركها على الكمبيوتر المحمول عند إعادتها إلى (جهة العمل).
11. تحتفظ إدارة تكنولوجيا المعلومات بحقها في استرجاع جميع المعدات التي تم أعارتها للمستخدمين من أجل إجراء تحديثات وتحسينات للبرامج، و / أو استبدال أو تحديث الأجهزة في أي وقت.
12. لا يقوم موظفو إدارة تقنية المعلومات بالدخول (login) للأجهزة الشخصية لأعمال الصيانة ألا بعد اخذ الأذن من صاحب العلاقة مباشرة.
13. أجهزة الكمبيوتر وملحقاتها موجودة لخدمة الموظفين والمستخدمين لأداء الأعمال بطريقة أفضل، وعليه فإنه ليس من الممكن استغلالها لأغراض شخصية.
14. توفر (جهة العمل) مجموعة واسعة من الطابعات المتصلة بالشبكة للمساعدة في أداء أعمال (جهة العمل)، كما يُسمح بطابعات سطح المكتب الفردية، وسيتم دعمها من قِبل قسم تقنية المعلومات.
15. يحظر على موظفي (جهة العمل) شراء معدات الشبكات الخاصة بهم، بما في ذلك على سبيل المثال لا الحصر: بطاقات الشبكة المحلية والبطاقات اللاسلكية وأجهزة التوجيه والمبدلات وتوصيل كابلات الشبكة والطابعات الجاهزة للربط بالشبكة.
16. يعتبر استقرار الشبكة أمرًا بالغ الأهمية في بيئة (جهة العمل)، وقد تؤدي إضافة معدات الشبكة غير المصرح بها لشبكة (جهة العمل) إلى حدوث مشكلات يصعب تشخيصها.
17. عند استعمال الكمبيوتر يجب أن يكون الدخول باستخدام اسم المستخدم وكلمة المرور الخاص به، وعند ترك الجهاز ولو لفترة وجيزة يجب قفل شاشة الجهاز بكلمة المرور.
18. لا يجب تخزين أي وثائق أو ملفات لا علاقة لها بالعمل في المساحات المخصصة للموظفين على الخادم المخصص لذلك.
19. مسؤولية المستخدم أن يتعلم كيفية استعمال جهاز الكمبيوتر وملحقاته بشكل سليم، وإذا شعر أنه بحاجة إلى التدريب، فعليه التوجه وطلب المساعدة من المعنيين في القسم المختص.

20. لا يسمح لأي شخص من خارج (جهة العمل) باستخدام حواسيب (جهة العمل) إلا بإذن كتابي رسمي.
21. يجب على المستخدم عدم أبطال عمل برامج مكافحة الفيروسات والبرامج الخبيثة على أجهزة كمبيوتر (جهة العمل)، كما يجب أن يتم فحص وسائل تخزين البيانات (مثل الأقراص المضغوطة أو محركات الأقراص الثابتة أو ذاكرة الفلاش) قبل فتح أي ملف أو برنامج.
22. يحظر على المستخدمين نسخ أية مواد أو برامج من أجهزة الكمبيوتر الخاصة بـ (جهة العمل) لتوزيعها خارجها دون موافقة خطية وصريحة.