قرار مجلس الوزراء رقم 21

صادر بتاريخ 03/07/2013م.
الموافق فيه 24 شعبان 1434هـ.

بشأن لائحة أمن المعلومات في الجهات الاتحادية

:

- بعد الاطلاع على الدستور،
- وعلى القانون الاتحادي رقم 1 لسنة 1972، في شأن اختصاصات الوزارات وصلاحيات الوزراء، والقوانين المعدلة له،
- وعلى المرسوم بقانون اتحادي رقم 3 لسنة 2003، بشأن تنظيم قطاع الاتصالات، والقوانين المعدلة به،
- وعلى المرسوم بقانون اتحادي رقم 11 لسنة 2008، بشأن الموارد البشرية في الحكومة الاتحادية، والقوانين المعدلة له،
- وعلى المرسوم بقانون اتحادي رقم 5 لسنة 2012، بشأن مكافحة جرائم تقنية المعلومات،
- وبناء على موافقة مجلس الوزراء،

:

المادة الأولى – التعريفات

يقصد بالكلمات والعبارات التالية المعاني الموضحة قرين كل منها ما لم يقتض سياق النص غير ذلك:

: الإمارات العربية المتحدة.

/ : الوزارات والهيئات والمؤسسات العامة والأجهزة التابعة للحكومة الاتحادية.

: الدخول الى نظام الحاسوب من قبل المستخدمين المصرح لهم.

: نسخ أو حفظ البيانات في موقع آخر لأغراض استعادة البيانات في حالة فقدان البيانات الأصلية أو تلفها أو تدميرها.

/ : الوحدة التنظيمية المختصة في الجهات الاتحادية والتي تتولى القيام بمهام تقنية المعلومات والاتصال الالكتروني.

: المعلومات التي لا يجوز الاطلاع عليها إلا من قبل المستخدمون المصرح لهم، وتشمل المعلومات السرية الموجودة في الاصول المعلوماتية والتي لا يستطيع المستخدمين الغير مصرح لهم الوصول إليها.

Shareware: برامج الحاسوب التي يتم تطويرها لأغراض الاستخدام العام، والتي يمكن استخدامها أو نسخها دون التعدي على حقوق المؤلف، ويكون ذلك عادة بعد دفع رسوم رمزية.

Freeware: هي البرامج المتوفرة على شبكة الإنترنت أو غيرها من الطرق بدون مقابل مالي.

: كل ما يرتبط باستخدام نظام تقنية المعلومات وعملياته وتطويره في

الجهات الاتحادية، بما في ذلك على سبيل المثال لا الحصر: المعدات والبرمجيات، والأجهزة، وأنظمة التشغيل والتطبيقات، ووسائط التخزين والوسائل الخارجية لتخزين البيانات، وحسابات الشبكة، والبريد الإلكتروني، وبروتوكول نقل الملفات والوصول الى الإنترنت، والوثائق، والبنية التحتية للشبكة، والبيانات.

ISDN: شبكة

الاتصالات عبر محولات الدائرة الكهربائية، والتي ترتبط بشكل وثيق بشبكة الهاتف العمومية التي تتيح الاتصال الهاتفي الرقمي بسرعات تصل الى 128 كيلوبت في الثانية.

: الجهاز الطرفي الذي يوصّل أجهزة الحاسوب مع بعضها البعض لإرسال الاتصالات عبر

خطوط الهاتف.

SSH: هو اختصار لكلمة Secure Shell وهو بروتوكول الشبكة المعرفة

والمستخدمة خصيصاً مع نظام LINUX أو UNIX ومثيلاته.

: هي الرسائل البريدية التي ترسل بطريقة عشوائية

للأغراض الدعائية والتجارية.

/ **:** كل موظف يعمل في إحدى الجهات الاتحادية ويرخص له باستخدام

أنظمة تقنية المعلومات أو شبكات الحاسوب أو المواقع الإلكترونية أو الاتصالات الإلكترونية التابعة لجهة عمله.

VPN: شبكة تستخدم الإنترنت لتوفير طريقة للوصول الى

الشبكة التنظيمية المركزية بالجهة المعنية للمستخدمين المصرح لهم، وتطالب الشبكة عادة أن تتم المصادقة الآمنة من هؤلاء المستخدمين للتأكد من هويتهم قبل الدخول.

: الوسائط المعدة لتخزين البيانات والتي يمكن

توصيلها إما عن طريق محرك (USB) أو سلك بيانات أو بواسطة اتصال لاسلكي مباشر بأي أجهزة حوسبة أو أي جهاز تخزين خارجي.

: ما يتصل بالتكنولوجيا الحديثة ويكون ذا قدرات كهربائية أو رقمية أو مغناطيسية أو لاسلكية

أو بصرية، أو كهرومغناطيسية أو ضوئية أو ما شابه ذلك.

/ **:** معلومات تُرسل أو تسلّم بوسائل

إلكترونية.

: هو نظام تشغيل متصل بشبكة حواسيب، يقوم بالعديد من الوظائف ومنها تشغيل

وإدارة قواعد البيانات بين الحواسيب المتصل بها، وتلبية الطلبات التي ترده من مختلف الحواسيب على الشبكة.

: طريقة أمنية تهدف الى حماية المعلومات أياً كان نوعها، من خلال ترميز تلك المعلومات

وتحويلها الى رموز غير مفهومة، لمنع الأشخاص غير المرخص لهم من الاطلاع عليها أو فهمها، بحيث يحتاج فك تلك الرموز الى مفتاح.

( ) **(Instant Messaging):** عبارة عن مجموعة من التقنيات

التي تتيح إمكانية التواصل النصي الفوري بين اثنين أو أكثر من المشاركين عبر شبكة الإنترنت أو عبر الشبكة الداخلية (الإنترانت).

: البيانات المخزنة والمقروءة من وسائط التخزين مثل الأشرطة الممغنطة

والأقراص المرنة أو الأقراص المدمجة، وما الى ذلك.

/ : هو برنامج خارجي صنع عمداً بغرض تغيير خصائص الملفات التي يصيبها لتقوم بتنفيذ بعض الأوامر إما بالإزالة أو التعديل أو التخريب أو السيطرة على جهاز الكمبيوتر أو سرقة بيانات مهمة منه أو ما شابهها من عمليات.

المادة 2 – نطاق تطبيق اللائحة

تسري أحكام هذه اللائحة على الجهات الاتحادية وعلى الموظفين العاملين لدى هذه الجهات.

المادة 3 – الأهداف

تهدف هذه اللائحة الى الآتي:

1 – تعزيز مفهوم أمن المعلومات لدى الجهات الاتحادية والمستخدمين.

2 – تحديد معايير الاستخدام الأمثل للأصول المعلوماتية.

3 – تشجيع التطبيق الفعال للأمن الالكتروني عن طريق تعزيزه باعتباره جهد جماعي يتطلب مشاركة ودعم كافة المستخدمين.

4 – التأكد من أن المستخدمين على علم بالتزاماتهم فيما يتعلق باستخدام الأصول المعلوماتية.

5 – بيان الإجراءات التي يتعين على الجهات الاتحادية اتباعها لحماية المستخدمين من الأعمال غير القانونية أو الضارة والتي قد تؤدي الى تلف الأصول المعلوماتية.

6 – توفير إطار قانوني للجهات الاتحادية لضمان أمن الاصول المعلوماتية.

7 – إيجاد بيئة آمنة في الجهات الاتحادية لحفظ المعلومات من خلال ضمان سرية المعلومات والبنية التحتية للشبكة، وحمايتها بمنع الدخول أو التعديل أو التغيير غير المصرح به لتلك المعلومات، وحمايتها كذلك من الفقدان أو التسرب أو التلف أو الإضرار بها بأية وسيلة كانت.

8 – مواجهة المخاطر المتصلة بأمن المعلومات، وتحديد المخاطر المحتملة، وكيفية مواجهتها لضمان استمرارية سير العمل في الجهات الاتحادية عند التعرض لأي حادث أو هجوم.

المادة 4 – ضوابط استخدام البريد الإلكتروني

أولاً: الضوابط العامة لاستخدام البريد الالكتروني:

1 – يجب أن تكون كافة نظم البريد الإلكتروني الحكومية ملك للجهة الاتحادية.

2 – يُحظر على المستخدم مشاركة كلمة مروره الشخصية مع الآخرين.

3 – يجب الالتزام باستخدام نظام البريد الإلكتروني في المراسلات الرسمية فقط ويمنع استخدام البريد المجاني (مثل Yahoo, Gmail, Hotmail... الخ).

4 – يُحظر على المستخدم القيام بإرسال أو إعادة توجيه أو نقل أو توزيع أو الرد على رسائل البريد غير المرغوب فيها.

5 – يحظرعلى المستخدم القيام بإرسال أو إعادة توجيه أو نقل أو توزيع أو الرد على الرسائل الإلكترونية التي تحتوي على تصريحات مشينة أو تشهيرية أو تهجمية أو عنصرية أو بذيئة، وتشمل التعليقات المسيئة عن العرق أو الجنس أو اللون أو الإعاقات أو العمر أو أمور جنسية أو مواد إباحية أو مواد تتعلق بالمعتقدات والممارسات الدينية والسياسية.

6 – يُحظر على المستخدم القيام بإرسال أو إعادة توجيه أو نقل أو توزيع أو الرد على الرسائل الإلكترونية التي تحتوي على معلومات سرية أو تعد انتهاكاً لحقوق الملكية الفكرية.

7 – يُحظر على المستخدم القيام بإرسال أو إعادة توجيه أو نقل أو توزيع أو الرد على الرسائل الإلكترونية التي تتضمن مرفقات تحتوي على فيروسات أو أية برامج قرصنة أو تخريبية أو محتويات ممنوعة بحكم القانون.

8 – يُحظر فتح رسائل البريد الإلكتروني الغير مرغوب فيها (spam) وعلى المستخدم حذفها من نظام البريد الإلكتروني الخاص به.

9 – يُحظر استخدام البريد الإلكتروني الرسمي للجهة الاتحادية لأغراض شخصية.

10 – يُحظر على المستخدم المشاركة في نشر الرسائل الإلكترونية لأسباب شخصية أو تجارية أو دينية أو سياسية.

11 – يُحظر على المستخدم المشاركة في نشر رسائل إلكترونية لأسباب خيرية بدون إذن مسبق من الجهة الاتحادية.

12 – يُحظر على المستخدم استخدام نظم البريد الإلكتروني لانتحال صفة شخص آخر.

13 – يُحظر على المستخدم القيام بإرسال أو إعادة توجيه أو نقل أو توزيع أو الرد على الرسائل الإلكترونية عند استخدام نظام البريد الإلكتروني الخاص بشخص آخر.

14 – يُحظر على المستخدم إدخال أي تغييرات على محتوى الرسالة الإلكترونية أو تغيير التاريخ والوقت أو المصدر أو الجهة أو التسمية أو أية معلومات أخرى.

15 – يجب على المستخدم القيام بالفحص والتحقق من أن الملفات المرفقة بالرسائل الإلكترونية لا تحتوي على فيروسات أو تعليمات برمجية ضارة.

ثانياً: ضوابط استخدام البريد الإلكتروني للهاتف المتحرك:

يجب على المستخدم عند استخدام البريد الإلكتروني للهاتف المتحرك الالتزام بما يلي:

1 – أن يكون جهاز الهاتف المتحرك مزوداً بميزة قفل أمان) كلمة مرور (pass word - مفعلة، وينبغي أن يكون الجهاز مزوداً بميزة القفل التلقائي أثناء استخدام خاصية البريد الإلكتروني للهاتف المتحرك التي قد توفرها الجهة الاتحادية.

2 – أن يقفل الهاتف المتحرك الذي تم توصيله مع البريد الإلكتروني للجهة الاتحادية بقفل الأمان) كلمة مرور (pass word –عند تركه في أي مكان.

3 – إبلاغ الوحدة المختصة فوراً إذا فُقد هاتفه المتحرك، لكي تقوم الوحدة المختصة بحذف بيانات البريد الإلكتروني تلقائياً من الجهاز بمجرد وصله بالشبكة.

4 – إبلاغ الوحدة المختصة والتنسيق معها قبل بيع هاتفه المتحرك أو إعطائه لشخص آخر، وتقوم الوحدة المختصة بحذف معلومات البريد الإلكتروني الخاص بالجهة الاتحادية من جهاز الهاتف المتحرك.

5 – التوقيع على نموذج التعهد الأمني المرفق بهذا القرار والذي يحدد المسؤوليات والإعدادات الأمنية التي يجب عليه تطبيقها عند استخدام نظام البريد الإلكتروني من قبل جهاز الهاتف المتحرك، والتي سبق ذكرها أعلاه.

المادة 5 – إخلاء المسؤولية

يتعين تذييل كافة رسائل البريد الالكتروني الصادرة عبر البريد الإلكتروني للجهة الاتحادية التي يتبع لها المستخدم بنص إخلاء المسؤولية، على أن يكون مضمون النص كالتالي:

"يعد هذا البريد الإلكتروني والملف/الملفات المرسلة معه سرية وتخص فقط الشخص أو الجهة الموجهة لها وفي حال لم تكن أنت المتلقي المعني بالرسالة، أو وصلتك هذه الرسالة على بريدك الإلكتروني عن طريق الخطأ، الرجاء إبلاغ المرسل وحذف هذا البريد الإلكتروني (والملف/الملفات المرفقة) من النظام الخاص بك، ولا يحق لك نسخ أو طبع أو توزيع أو استخدام هذا البريد الإلكتروني أو أي من مرفقاته، أو التصريح أو الإفصاح عن محتواه لأي طرف آخر بأي صورة من الصور إلا بموافقة مسبقة من المرسل، وفي حال مخالفتك لما تم توضيحه آنفاً فإنك ستتعرض للمساءلة القانونية.

المادة 6 – ضوابط استحداث كلمة المرور

1 – يجب على المستخدم التأكد من استخدام كلمة مرور آمنة وفعالة وحفظها بشكل آمن في جميع الأوقات، ولأجل إنشاء كلمة المرور فإنه يتعين على المستخدم الالتزام بما يلي:

أ – أن تحتوي كلمة المرور على مركب من الأحرف اللاتينية الكبيرة والصغيرة مثل (A-Z) (a-z) والأرقام وكذلك على علامات التنقيط مثل $#@!)٪(>'-()*^.

ب – ألا يقل طول كلمة المرور عن ثمانية خانات من حروف أبجدية وأرقام ورموز.

ج – ألا تستند كلمة المرور الى معلومات شخصية يمكن الوصول إليها أو تخمينها بسهولة.

2 – عند تخصيص الوحدة المختصة لمستخدم كلمة مرور أولية، فإنه يجب على المستخدم تغييرها فور تسجيل الدخول الى النظام للمرة الأولى.

3 – يتعين على الوحدة المختصة التحكم في تاريخ انتهاء صلاحية كلمات المرور على ألا تقل مدة صلاحيتها عن (60) يوماً، وألا يكون في استطاعة المستخدم القيام باستخدام نفس كلمة المرور أكثر من مرّة خلال مدة (180) يوماً ولا تزيد على (90) يوماً، وألا يكون في استطاعة المستخدم القيام باستخدام نفس كلمة المرور أكثر من مرّة خلال مدة (180) يوماً، وألا يتم تكرار نفس كلمة المرور ضمن دورة (6) تغييرات لكلمة المرور.

4 – على الوحدة المختصة في الجهة الاتحادية تفعيل خاصية الإقفال التلقائي بكافة أجهزة الحاسوب.

المادة 7 – ضوابط استخدام الإنترنت

يجب على المستخدم عند استخدام الإنترنت في الجهات الاتحادية الالتزام بالآتي:

1 – أن يكون استخدامه للإنترنت لأغراض العمل فقط، أو لزيادة خبراته في مجال عمله في الجهة الاتحادية، وألا يقوم بالدخول الى المواقع المحظورة أو التي تحتوي على محتوى محظور بموجب سياسات الجهة الاتحادية.

2 – ألا يقوم بالدخول الى المواقع المسيئة أو المساهمة فيها أو تنزيل ملفات منها، وتشمل هذه المواقع المسيئة على سبيل المثال لا الحصر المواقع التي تشجع على العنصرية، والمواقع التي تحتوي على مشاعر دينية إزدرائية أو لغة بذيئة أو تشهير أو تهجم أو إساءة لأي فرد أو جماعة، والمواقع ذات المحتوى الإباحي.

3 – عدم المشاركة في أي نشاط من شأنه أن يؤدي الى توقف عمليات أنظمة الحاسوب.

4 – عدم تنزيل أو تحميل أو تثبيت برمجيات من الإنترنت، إلا بموافقة الوحدة المختصة.

المادة 8 – ضوابط مكافحة الفيروسات

يتعين على الوحدات المختصة والمستخدمين في الجهات الاتحادية اتخاذ كافة الإجراءات اللازمة لمكافحة الفيروسات والالتزام بالضوابط الآتية:

1 – يمنع استخدام أي حاسوب مكتبي أو محمول غير مجهز ببرنامج مكافحة الفيروسات الخاصة بالجهة الاتحادية ضمن شبكتها.

2 – يجب أن تقوم الوحدة المختصة في الجهة الاتحادية بتحديث جميع برمجيات مكافحة الفيروسات بشكل دوري، وفحص الأنظمة بشكل مستمر للتأكد من خلو الملفات من الفيروسات.

3 – يتعين على الوحدات المختصة والمستخدمين في الجهات الاتحادية التحقق من أن جميع الملفات المنزلة عبر البريد الإلكتروني خالية من الفيروسات.

4 – يتعين على الوحدات المختصة في الجهات الاتحادية تجهيز كافة الخوادم ببرنامج مكافحة الفيروسات واختبارها دورياً للتأكد من كفاءتها للحماية من الفيروسات.

5 – يتعين على الوحدات المختصة والمستخدمين في الجهات الاتحادية فحص جميع الوسائط غير الثابتة من خارج الجهة الاتحادية وفحصها للبحث عن الفيروسات قبل استعمالها من قبل المستخدم.

6 – على المستخدمين الذين يسمح لهم باستخدام شريحة ذاكرة (USB) في أجهزتهم، فحصها للتأكد من خلوها من الفيروسات قبل استخدامها.

7 – يتعين على الوحدات المختصة والمستخدمين في الجهات الاتحادية فحص جميع رسائل البريد الإلكتروني الواردة والصادرة للتأكد من خلوها من الفيروسات والمحتوى الضار.

8 – يجب تحديث خادم البريد دورياً بأحدث البرمجيات (service packs/patches) لأغراض الحماية من الفيروسات.