قرار مجلس الوزراء رقم (21) لسنة 2013
بشأن لائحة أمن المعلومات في الجهات الاتحادية

مجلس الوزراء،

- 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 له،
- 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،
- وبناءً على موافقة مجلس الوزراء،

قرر:

المادة (1)
التعريفات

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

الدولة	:	الإمارات العربية المتحدة.
الجهة/ الجهات الاتحادية	:	الوزارات والهيئات والمؤسسات العامة والأجهزة التابعة للحكومة الاتحادية.
توفر الدخول	:	الدخول إلى نظام الحاسوب من قبل المستخدمين المصرح لهم.
النسخ الاحتياطي	:	نسخ أو حفظ البيانات في موقع آخر لأغراض استعادة البيانات في حالة فقدان البيانات الأصلية أو تلفها أو تدميرها.
الوحدة/ الوحدات المختصة	:	الوحدة التنظيمية المختصة في الجهات الاتحادية والتي تتولى القيام بمهام تقنية المعلومات والاتصال الإلكتروني.
المعلومات السرية	:	المعلومات التي لا يجوز الاطلاع عليها إلا من قبل المستخدمون المصرح لهم، وتشمل المعلومات السرية الموجودة في الأصول المعلوماتية والتي لا يستطيع المستخدمين الغير مصرح لهم الوصول إليها.

البرمجيات المشتركة 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.
البرامج المجانية Freeware	:	هي البرامج المتوفرة على شبكة الإنترنت أو غيرها من الطرق بدون مقابل مالي.
الأصول المعلوماتية	:	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 إلى الإنترنت، والوثائق، والبنية التحتية للشبكة، والبيانات.
الشبكة الرقمية للخدمات المتكاملة أو الشبكة الرقمية ISDN	:	شبكة الاتصالات عبر محولات الدائرة الكهربائية، والتي ترتبط بشكل وثيق بشبكة الهاتف العمومية التي تتيح الاتصال الهاتفي الرقمي بسرعات تصل إلى 128 كيلوبت في الثانية.
الوسيط	:	الجهاز الطرفي الذي يوصّل أجهزة الحاسوب مع بعضها البعض لإرسال الاتصالات عبر خطوط الهاتف.
القشرة الآمنة SSH	:	هو اختصار لكلمة Secure Shell وهو بروتوكول الشبكة المعرفة والمستخدمة خصيصًا مع نظام LINUX أو UNIX ومثيلاته.
رسائل البريد غير المرغوب فيها	:	هي الرسائل البريدية التي ترسل بطريقة عشوائية للأغراض الدعائية والتجارية.
المستخدم/ المستخدمون	:	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.
الشبكة الافتراضية الخاصة VPN	:	شبكة تستخدم الإنترنت لتوفير طريقة للوصول إلى الشبكة التنظيمية المركزية بالجهة المعنية للمستخدمين المصرح لهم، وتطالب الشبكة عادة أن تتم المصادقة الآمنة من هؤلاء المستخدمين للتأكد من هويتهم قبل الدخول.
الوسائل الخارجية لتخزين البيانات	:	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.

إلكتروني : ما يتصل بالتكنولوجيا الحديثة ويكون ذا قدرات كهربائية أو رقمية أو مغناطيسية أو لاسلكية أو بصرية، أو كهرومغناطيسية أو ضوئية أو ما شابه ذلك.

الرسالة الإلكترونية/ البريد الإلكتروني : معلومات تُرسل أو تسلّم بوسائل إلكترونية.

خادم المعلومات : 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.

التشفير : طريقة أمنية تهدف إلى حماية المعلومات أياً كان نوعها، من خلال ترميز تلك المعلومات وتحويلها إلى رموز غير مفهومة، لمنع الأشخاص غير المرخص لهم من الاطلاع عليها أو فهمها، بحيث يحتاج فك تلك الرموز إلى مفتاح.

التراسل الفوري (الدردشة) (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 الثابتة : البيانات المخزنة والمقروءة من وسائط التخزين مثل الأشرطة الممغنطة والأقراص المرنة أو الأقراص المدمجة، وما إلى ذلك.

الفايروس/ الفايروسات : 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 إلى الآتي:

1. تعزيز مفهوم أمن المعلومات لدى الجهات الاتحادية والمستخدمين.
2. تحديد معايير الاستخدام الأمثل للأصول المعلوماتية.

3. تشجيع التطبيق الفعال للأمن الإلكتروني 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 إلى تلف الأصول المعلوماتية.
6. توفير إطار قانوني للجهات الاتحادية لضمان أمن الأصول 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 الإلكتروني:

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**...إلخ).
4. يُحظر على المستخدم القيام بإرسال أو إعادة توجيه أو نقل أو توزيع أو الرد على رسائل البريد غير المرغوب فيها.
5. يحظر على 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 انتهاكًا 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 الإلكتروني 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 كلمات مرور آمنة وفعالة وحفظها بشكل آمن في جميع الأوقات، ولأجل إنشاء كلمة مرور 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 إلى 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 إلى 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 مرة خلال مدة (180) يومًا ولا تزيد على (90) يوماً، وألا يكون في استطاعة المستخدم القيام باستخدام نفس كلمة المرور أكثر من مرة 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 إلى المواقع المحظورة أو التي تحتوي على محتوى محظور بموجب سياسات الجهة الاتحادية.
2. ألا يقوم بالدخول إلى 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 ازدراءيه 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 إلى 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.
9. يتعين على الوحدات المختصة والمستخدمين في الجهات الاتحادية عند اكتشاف أية رسالة في البريد الإلكتروني تحمل فايروساً، وضع تلك الرسالة في مجلد العزل **(Quarantine)** إذا لم يُمكن التخلص منه.
10. على الوحدة المختصة في الجهة الاتحادية عند اكتشاف أي نوع من الفيروسات في البريد الإلكتروني إخطار المستخدم بذلك، وتقديم المشورة والدعم الفني اللازمين له.
11. يُحظر على المستخدم تعطيل أو إجراء أي تغييرات على برنامج مكافحة الفيروسات.
12. إذا انتاب المستخدم شك بأن نظام جهاز الحاسب الآلي قد تعرض لأية مخاطر أمنية على سبيل المثال (فيروسات أو برامج ضارة) وغيرها، فإن الإجراء الواجب الاتباع في هذه الحالة هو فصل الأجهزة عن الشبكة فوراً، والاتصال شخصياً بالوحدة المختصة للإبلاغ عن ذلك، واتباع التعليمات اللازمة بشأنه.
13. يتعين على المستخدم عدم تقييم أو تحليل المخاطر الأمنية دون تعليمات محددة من أحد موظفي الوحدة المختصة بالجهة الاتحادية.
14. يجب على الوحدة المختصة فحص أجهزة المستخدمين للتحقق من وجود برامج مكافحة الفيروسات وسجلاتها ومستوى التوقيع، وإذا اقتضى الأمر تقوم بتثبيتها أو تحديثها إلى آخر تحديثات التوقيع.

المادة (9)

ضوابط استخدام الأصول المعلوماتية

أولاً: التزامات الوحدة المختصة:

يجب على الوحدة المختصة الالتزام بما يلي:

1. القيام بإجراء فحص دوري لأجهزة الحاسوب بما في ذلك الأجهزة المحمولة مثل الحاسوب المحمول والمساعدات الرقمية الشخصية المستخدمة من قبل المستخدمين.
2. تقييم البرمجيات وإصدار توصية بشأنها وأن تأخذ بالاعتبار احتياجات المستخدمين.
3. . النظر في طلبات المستخدمين الذين يرغبون في تثبيت برمجيات مجانية أو مشتركة **(Freeware or Shareware)** وتقييم أدائها وأمنها.

ثانياً: التزامات المستخدم:

يجب على المستخدم عند استخدام الأصول المعلوماتية بشكل عام، والبرمجيات المرخصة للجهة الاتحادية بشكل خاص، الالتزام بالآتي:

1. عدم تنزيل أو تثبيت أي برمجيات على أي جهاز حاسوب.

2. عدم تثبيت برمجيات غير مرخصة أو مفكوكة التشفير **(cracked)** أو البرمجيات غير القياسية **(nonstandard)** على أي حاسوب بما في ذلك الأجهزة المحمولة مثل الحاسوب المحمول والمساعدات الرقمية الشخصية **(PDAS)**.
3. عدم حيازة أو توزيع أو نسخ أو استخدام برامج الحاسوب لفحص الشبكات أو اعتراض المعلومات أو الاستيلاء على كلمات المرور دون تفويض محدد للقيام بذلك.
4. التأكد من استخدامه البرمجيات ضمن حدود شروط ترخيص الجهة الاتحادية.
5. التأكد من أنه يستخدم البرمجيات بما يتفق مع القوانين الاتحادية أو المحلية في الدولة، ومنها على وجه والخصوص قوانين حقوق المؤلف والمعاملات التجارية وبراءات الاختراع.

المادة (10)

ضوابط الاتصال عن بعد بشبكة الجهة الاتحادية

يجب على المستخدم الذي لديه امتيازات الوصول عن بعد إلى شبكة الجهة الاتحادية الالتزام بالآتي:

1. عدم استخدام خدمات الوصول عن بعد إلى شبكة الجهة الاتحادية التي يعمل لديها لأغراض لا تتعلق بالعمل.
2. عدم السماح لأي شخص باستخدام خدمات الوصول عن بعد إلى شبكة الجهة الاتحادية من خلال الصلاحيات الممنوحة له.
3. التأكد من أن جهازه الموصول عن بعد بشبكة الجهة الاتحادية ليس موصول بأي شبكة أخرى في نفس الوقت، وذلك باستثناء الشبكات الشخصية الواقعة تحت السيطرة الكاملة للمستخدم.
4. أن تكون المعدات الشخصية التي يتم استخدامها للاتصال بشبكة الجهة الاتحادية متوافقة مع متطلبات وضوابط الوحدة المختصة في جهة عمله.

المادة (11)

ضوابط استخدام أجهزة الحاسوب المكتبية والمحمولة

يجب على المستخدم أن يلتزم أثناء استخدامه لأجهزة الحاسوب الخاصة بالجهة الاتحادية بالآتي:

1. حماية جهاز الحاسوب المكتبي والمعلومات المخزنة به من التلف أو الفقدان أو السرقة.
2. في حال سرقة جهاز الحاسوب المحمول، يتعين على المستخدم إبلاغ الشرطة في البلد الذي وقعت فيه السرقة فوراً، وإبلاغ الوحدة المختصة.
3. في حالة تلف أو فقدان جهاز الحاسوب المحمول، يتعين على المستخدم إبلاغ الوحدة المختصة فوراً عن الفقدان.
4. عدم ترك جهاز الحاسوب المحمول في مكان عام دون مراقبة.
5. قفل حسابه عند الانتهاء من استخدام جهاز الحاسوب المحمول.

6. عدم توصيل أجهزة الحاسوب الشخصية الخاصة على شبكة الجهة الاتحادية.
7. عدم تغيير الوظائف الإدارية بجهاز الحاسوب المحمول بأي شكل من الأشكال، مثل نظام التشغيل في الجهاز أو تعريف مدير النظام وكلمة المرور.
8. التقيّد بسياسة التشفير المعتمدة من قبل الجهة الاتحادية عند تخزين المعلومات الحسّاسة والسرّية على أجهزة الحاسوب المحمولة الخاصة بهم.
9. عمل نسخ احتياطي للملفات من جهاز الحاسوب المحمول إلى مجلّدات الشبكة المناسبة بصورة منتظمة.

المادة (12)

التشفير

أولاً: تلتزم الوحدة المختصة بتشفير البيانات في الجهة الاتحادية بما يلي:

1. أن توفر أكبر قدر من الحماية للمعلومات المصنفة والحساسة والسرية عن طريق الاستخدام الفعال لتشفير البيانات.
2. أن توفر تدابير التشفير المناسبة لأي بيانات مرسلة عبر شبكات الغير، وشبكات الاتصالات العامة الأساسية.
3. أن تقوم بتشفير وحماية البيانات السرية المنقولة على وسائط التخزين الثابتة المقروءة في جهاز الحاسوب.

ثانياً: يلتزم المستخدم فيما يتعلق بتشفير البيانات بما يلي:

1. استخدام الخوارزميات المثبتة والقياسية التي تقوم الوحدة المختصة بإعدادها على أجهزة الحاسوب الخاصة بهم كأساس لتقنيات التشفير.
2. عدم استخدام وسائل التشفير التي لم تتم مراجعتها والموافقة عليها من قبل الوحدة المختصة في الجهة الاتحادية.
3. تشفير كافة البيانات الحساسة أو السرية الموجودة عند تخزينها أو إرسالها.

المادة (13)

ضوابط استخدام النسخ الاحتياطي واستعادة المعلومات

يجب على الوحدة المختصة بالجهة الاتحادية الالتزام بما يلي:

1. تسجيل وحفظ متطلبات النسخ الاحتياطي لجميع النظم ويجب أن يشمل ذلك على سبيل المثال لا الحصر (تفاصيل عدد مرات النسخ الاحتياطي، والمعلومات المطلوب نسخها احتياطياً، ووسائط التخزين، ومدة حفظها، وإعادة تدويرها).

2. إعداد نسخ احتياطية لكافة برمجيّات النظم وبرمجيّات التطبيقات وبيانات المستخدمين ومعلومات قاعدة البيانات والوثائق بصورة منتظمة لتسهيل استرجاعها في حال وقوع انقطاع غير متوقع للنظم، ويجب أن يكون عدد مرات عملية النسخ الاحتياطي كحد أدنى كما يلي:
   أ. برمجيات النظم: تكون عملية النسخ الاحتياطي قبل وبعد أي تغييرات في الأنظمة مثل الترقية، والتغييرات في التكوين، والتحديثات التكميلية، وغيرها.
   ب. برمجيات التطبيقات: تكون عملية النسخ الاحتياطي قبل وبعد أي تغييرات على التطبيق مثل صدور نسخة جديدة أو تعديل تعليمات مُصدر البرمجية للتطبيق.
   ج. بيانات المستخدمين/ معلومات قاعدة البيانات: تكون عملية النسخ الاحتياطي بصورة دورية (يومية/ أسبوعية/ شهرية/ سنوية)، وذلك على أساس عدد مرات النسخ الاحتياطي المحددة للأنظمة المختلفة.
   د. تكوينات الأجهزة: تكون عملية النسخ الاحتياطي قبل وبعد أية تغييرات على تكوينات الأجهزة الحساسة مثل أجهزة التوجيه (**Router**)، وجدران الحماية، وأنظمة توصيل الإنترنت (**IDS**) وغيرها.
   هـ. الوثائق: تكون عملية النسخ الاحتياطي لأحدث نسخ من وثائق النظام (مثل الكتيبات المرجعية الفنية، وأدلة المستخدم وما إلى ذلك)
3. تقع على المستخدم مسؤولية التأكد من إعداد نسخ احتياطية لبياناته المخزنة على جهاز الحاسب الآلي الخاص به بصورة منتظمة، وتكون بيانات الاسترداد والاسترجاع متوفرة فقط إذا كانت هذه البيانات مخزنة على شبكة خوادم الجهة الاتحادية، كما يستطيع المستخدم عمل نسخ احتياطي لبياناته بنقل أو نسخ البيانات إلى مجلدات محرك أقراص الشبكة الخاصة به، حسب الإجراءات المتبعة في الجهة الاتحادية بشأن عمل النسخ الاحتياطي على وسائط مناسبة.
4. يتعين على الوحدة المختصة في الجهة الاتحادية التأكد من المعلومات المطلوب نسخها احتياطياً وعدد مرات النسخ الاحتياطي.

المادة (14)

درجات السرية

1. تحدد درجات السرية بالنسبة لوثائق ومستندات الجهات الاتحادية ومعلوماتها والأشخاص الذين لهم حق الاطلاع على كل درجة من درجات السرية على النحو التالي:
   أ. **درجة سري للغاية** : تعطى للمعلومات ذات الأهمية الاستراتيجية للدولة وللجهة الاتحادية، حيث تحتاج إلى أعلى مستويات الحماية، ولا يعطى الحق في الاطلاع على هذه المعلومات إلا لعدد قليل من المستخدمين المختصين.

ب. **درجة سري** : تعطى للمعلومات التي قد يكون لها تأثير ضار على الجهة الاتحادية، ويكون عدد المستخدمين الذين لهم الحق في الاطلاع على هذه المعلومات محدوداً (مثلاً أن يقتصر على إدارة معينة أو مسمى وظيفي معين).

ج. **درجة محظور** : تعطى للمعلومات التي لا يضر تداولها بين مختلف الإدارات في الجهة الاتحادية.

د. **درجة عام** : لا تعتبر من درجات السرية وتعطى للمعلومات التي يمكن إطلاع العامة عليها.

2. على جميع الجهات الاتحادية مسؤولية تحديد درجات السرية بالنسبة لمعلوماتها بشكل صحيح واختيار وسائط تخزينها والمراجعة الدورية لهذا التصنيف، وتحديد صلاحيات المستخدمين على حسب التصنيف من حيث الاطلاع أو التعديل أو الحذف أو النسخ أو الإرسال أو الطباعة.

المادة (15)

النفاذ عبر الشبكة المحلية اللاسلكية (Wi-Fi)

أولاً: بالنسبة لكافة أجهزة البنية التحتية اللاسلكية الموجودة في مكاتب الجهة الاتحادية، والمتصلة بشبكة الجهة الاتحادية، أو التي توفر إمكانية الاطلاع على معلومات مصنفة بأنها سري للغاية أو سري أو محظور يجب أن تستوفى ما يلي:

1. استخدام بروتوكولات التوثيق والبنية التحتية المعتمدة في الجهة الاتحادية.
2. الحفاظ على عنوان الجهاز (عنوان مراقبة الوصول للوسائط) الذي يمكن تسجيله وتتبعه.
3. أن تكون مركبة من قبل الوحدة المختصة في الجهة الاتحادية وهي التي توفر لها الدعم والصيانة.
4. استخدام بروتوكولات التشفير المعتمدة في الجهة الاتحادية.

ثانياً: يجب على أجهزة البنية التحتية اللاسلكية التي توفر إمكانية الوصول المباشر إلى شبكة الجهة الاتحادية أن تستوفي ما يلي:

1. تمكين خاصية التبادل السري للوصول المحمي بتقنية عالية الموثوقية.
2. أن تكون مهيأة لتعطيل بث معرف الشبكة المحلية اللاسلكية (SSID) عند استخدام الشفرات المفتاحية أو رموز الوصول الأمني.
3. أن تكون مهيأة لتغيير اسم معرف الشبكة المحلية اللاسلكية الافتراضي.
4. أن تكون مهيأة لتغيير اسم المستخدم وكلمة المرور الافتراضية لتسجيل الدخول.

المادة (16)

ضوابط تخزين البيانات

يجب عند تخزين المعلومات والبيانات الرسمية في الوسائل الخارجية لتخزين البيانات الالتزام بما يلي:

1. أن يكون الغرض من التخزين هو حفظ بيانات ومعلومات الجهة الاتحادية وفي السياق العادي للأعمال اليومية.
2. ألا يقوم باستخدام الوسائل الخارجية لتخزين البيانات إلا بعد الحصول على موافقة الوحدة المختصة وألا يقوم بنقل البيانات والمعلومات المخزنة على هذه الوسائل إلى أي جهة خارجية بدون موافقة السلطة المختصة بالجهة الاتحادية حسب الإجراءات المعمول بها في كل الجهات الاتحادية.
3. أن يتم فحص الوسائل الخارجية لتخزين البيانات المسموح باستخدامها من قبل الجهة الاتحادية، وأن يتم التأكد من عدم احتوائها على أية برمجيات خبيثة.
4. يتعين على المستخدم عدم استخدام الوسائل الخارجية لتخزين البيانات التي تحتوي على معلومات شخصية.
5. يتعين على الوحدة المختصة إخطار المستخدمين بوجود فايروس في الوسائل الخارجية لتخزين البيانات وإذا تم اكتشاف مزيد من الفيروسات على الرغم من الإخطار الأول، فإنه يتعين على الوحدة المختصة منع المستخدم المتسبب من استخدام الوسائل الخارجية لتخزين البيانات نهائياً.
6. يجب على الوحدة المختصة في الجهة الاتحادية القيام بمراجعة منتظمة للوسائل الخارجية لتخزين البيانات المستعملة من قبل المستخدمين للتأكد من التزامه بالشروط اللازمة.

المادة (17)

الجزاءات

دون الإخلال بالمسؤولية الجزائية المنصوص عليها في القوانين العقابية ذات العلاقة، يجازى كل مستخدم يخالف أحكام هذه اللائحة بالجزاءات التأديبية الواردة في القوانين واللوائح الخاصة بالموارد البشرية المطبقة في الجهة الاتحادية التي يعمل لديها.

المادة (18)

أحكام ختامية

تتولى الهيئة العامة لتنظيم قطاع الاتصالات تعميم هذا القرار على جميع الجهات الاتحادية.

المادة (19)

تصدر السلطة المختصة في الجهات الاتحادية القرارات اللازمة لتنفيذ أحكام هذا القرار.

المادة (20)

ينشر هذا القرار في الجريدة الرسمية ويعمل به بعد (90) يوماً من اليوم التالي لتاريخ نشره.

محمد بن راشد آل مكتوم

رئيس مجلس الوزراء

صدر عنا:

بتاريخ: 24/ شعبان / 1434هـ

الموافق: 3 / يوليو / 2013م

مرفق بقرار مجلس الوزراء رقم (21) لسنة 2013
بشأن لائحة أمن المعلومات في الجهات الاتحادية

تعهد بطريقة استخدام نظام البريد الإلكتروني عبر الهاتف المحمول

تعتبر رسائل البريد الإلكتروني التابعة للجهة الاتحادية رسائل سرية ويجب حمايتها، وتقع مسؤولية ضمان المحافظة على رسائل البريد الإلكتروني في جميع الأوقات على عاتق المستخدم الذي يتم الموافقة عليه لاستخدام نظام البريد الإلكتروني عبر الهاتف المحمول.

1. **مسؤولية مستخدمي نظام البريد الإلكتروني عبر الهاتف المحمول:**

على المستخدم التابع للجهة الاتحادية الممنوح ميزة استخدام نظام البريد الإلكتروني عبر الهاتف المحمول الالتزام بالآتي:

أ. الإجراءات والواجبات المنصوص عليها في هذا التعهد.

ب. الواجبات والإرشادات المنصوص عليها في لائحة أمن المعلومات المعتمدة من مجلس الوزراء.

2. **إجراءات الالتزام باستخدام البريد الإلكتروني عبر الهاتف المتحرك:**

أ. يجب على المستخدم التأكد من أن ميزة قفل الأمان متاحة على جهازه المحمول وأن يتم ضبط قفل الجهاز تلقائياً في أقصر فترة ممكنة (أقل من خمسة دقائق).

ب. يجب على المستخدم التأكد من أن الوصول إلى الجهاز المحمول واستخدامه يتم فقط من قبله.

ج. يجب أن لا يترك جهاز الهاتف المحمول غير مقفل ودون رقابة.

د. على المستخدم إبلاغ الوحدة المختصة على الفور ما إذا تمت سرقة أو فقدان هاتفه المحمول، حيث ستقوم الوحدة المختصة بمسح الهاتف المحمول وسيتم حذف بيانات البريد الإلكتروني من الجهاز تلقائياً فور اتصاله بالشبكة.

هـ. يجب على المستخدم إبلاغ الوحدة المختصة والتنسيق معهم قبل بيع أو منح الجهاز لمستخدم آخر، بحيث يتسنى الوحدة المختصة مسح معلومات البريد الإلكتروني من الجهاز.

3. **الجزاءات الإدارية:**

سيتم اتخاذ إجراءات ضد المستخدم، الذي لا يحافظ على أمن جهازه المحمول والتي قد تشمل إلغاء ميزة استخدام نظام البريد الإلكتروني عبر الهاتف المحمول.

أتعهد و أقر أنا الموظف الموقع أدناه بأنني قد قرأت وفهمت ما جاء في هذا التعهد ويجب أن ألتزم به.

الاسم:

المسمى الوظيفي:

القسم:

التوقيع:

التاريخ: