قرار مجلس الوزراء رقم (6) لسنة 2020م
بإدارة أمن المعلومات

مجلس الوزراء،

استناداً لأحكام القانون الأساسي المعدل لسنة 2003م وتعديلاته،

وبعد الاطلاع على أحكام القرار بقانون رقم (15) لسنة 2017م، بشأن المعاملات الإلكترونية،

والاطلاع على أحكام القرار بقانون رقم (10) لسنة 2018م، بشأن الجرائم الإلكترونية وتعديلاته،

وبناءً على تنسيب وزارة الاتصالات وتكنولوجيا المعلومات،

وعلى الصلاحيات المخولة لنا،

وتحقيقا للمصلحة العامة،

قرر مجلس الوزراء في جلسته المنعقدة بتاريخ 2020/12/28م، الآتي:

مادة (1)

تعاريف

يكون للكلمات والعبارات الواردة في هذا القرار المعاني المخصصة لها أدناه، ما لم تدل القرينة على خلاف ذلك:

المؤسسة: الدائرة الحكومية ومن في حكمها.

المخاطر: الأثر السلبي المتوقع حدوثه على الأصول، الناتج عن احتمالية حدوث تهديد.

التهديد: حدث محتمل في حال تحققه قد يتسبب في إحداث ضرر للمؤسسة أو أنظمتها.

الأصول: الموارد المحسوسة وغير المحسوسة التي تعود بالقيمة للمؤسسة، كالبرامج والعتاد (أجهزة الكمبيوتر والشبكات والبرامج والأنظمة ...).

المراجعة الدورية: المراجعة التي تتم خلال سنة ميلادية واحدة، ما لم يتم تحديد غير هذه المدة في أنظمة المؤسسة الخاصة.

السياسة: المبادئ المعتمدة من المؤسسة لتحديد طبيعة وملامح الإجراءات التفصيلية للعمل بخصوص أمن المعلومات.

الإجراء: خطوات متسلسلة يتم تطبيقها بترتيب وترابطية معينة، على أن تشمل تحديد العمل المطلوب، والشخص المسؤول، وطريقة التنفيذ.

متطلبات أساسية: الحد الأدنى من المتطلبات الواجب على المؤسسة استخدامها، المعتمدة من مجلس الوزراء، وتشمل السياسات والإجراءات.

مسؤول أمن المعلومات: الشخص أو الفريق المسؤول عن تطبيق رؤية المؤسسة واستراتيجيتها في مجال أمن المعلومات، وضمان درجة أمان مناسبة لتحافظ على أصولها.

البرامج "الأنظمة" المطورة خارجياً: الأنظمة أو البرامج التي يتم تطويرها من خلال عقود مع شركات أو أفراد من خارج المؤسسة.

المناطق ذات الخصوصية العالية: المناطق التي لا يسمح لأي شخص بالتواجد فيها إلا بموافقة مسؤول المؤسسة أو من يفوضه كغرفة الخوادم.

المرجع الإلكتروني للجريدة الرسمية
ELECTRONIC REFERENCE FOR THE OFFICIAL GAZETTE
mjr.lab.pna.ps

مادة (2)
نطاق التطبيق
تطبق أحكام هذا القرار على المؤسسة، وعلى جميع أصول تقنيات المعلومات.

مادة (3)
اللجان
يشكل مجلس الوزراء بتنسيب من وزارة الاتصالات وتكنولوجيا المعلومات اللجان الدائمة التالية لتطبيق أحكام هذا القرار:
1. لجنة إعداد ومراجعة المتطلبات الأساسية.
2. لجنة مساعدة المؤسسات.
3. لجنة مراقبة ومتابعة مدى الالتزام بتطبيق أحكام هذا القرار.

مادة (4)
التزامات المؤسسة
يجب على المؤسسة الالتزام بالآتي:
1. تطبيق أحكام هذا القرار والمتطلبات الأساسية عند إعداد سياساتها الخاصة.
2. المتطلبات الأساسية لضمان الأمن السيبراني.
3. التأكد من أن الأهداف التي يحققها نظام أمن المعلومات الخاص بها يتوافق مع أهداف المؤسسة وخططها الاستراتيجية.
4. توفير الموارد المطلوبة لتطبيق أحكام هذا القرار.
5. مراجعة دورية لجميع السياسات والإجراءات المنبثقة عن هذا القرار خلال سنة ميلادية واحدة، ما لم يتم تحديد غير هذه المدة في أنظمة المؤسسة الخاصة.
6. مواصفات ومبادئ تصنيع الأصول.
7. تعيين شخص أو فريق عمل يكون مسؤولاً عن تطبيق أحكام هذا القرار، ويكون له تبعية مباشرة للإدارة العليا للمؤسسة.

مادة (5)
سياسات أمن المعلومات
يجب أن تكون سياسات أمن المعلومات مكتوبة ومعممة داخل المؤسسة.

مادة (6)
تقييم المخاطر
لغايات تقييم المخاطر يجب على المؤسسة القيام بالآتي:
1. اعتماد وتطوير الإجراءات لتحديد المخاطر المتعلقة بأمن المعلومات وتطبيقها.
2. التأكد من أن نتائج تقييم المخاطر متسقة وصحيحة وقابلة للمقارنة.
3. تقييم وتحليل المخاطر على أساس الخسارة المحتملة.
4. تحديد المستوى المقبول للمخاطر.

المرجع الإلكتروني للجريدة الرسمية
ELECTRONIC REFERENCE FOR THE OFFICIAL GAZETTE
mjr.lab.pna.ps

مادة (7)
تحليل المخاطر

يجب أن تشمل إجراءات تحليل المخاطر الآتي:

1. تحديد التهديدات المحتملة.
2. تقييم العواقب المحتملة للتهديدات.
3. تقييم واقعية حدوث التهديد.
4. قياس مستوى واقعية المخاطر استناداً إلى درجة العواقب المحتمل حدوثها.
5. مقارنة تحليل المخاطر بالمعايير المحددة في هذا القرار.
6. تحديد أولويات المخاطر المحللة لمعالجتها.

مادة (8)
معالجة المخاطر

يجب على المؤسسة تحديد وتطبيق خطة معالجة مخاطر أمن المعلومات بناءً على نتائج تقييم المخاطر.

مادة (9)
الأدوار والمسؤوليات

تلتزم المؤسسة بتحديد وتخصيص الأدوار والمسؤوليات المتعلقة بأمن المعلومات، وتعيين مسؤول أمن المعلومات.

مادة (10)
كفاءة الموظفين

1. يجب على المؤسسة تأهيل وتدريب الموظفين ورفع كفاءتهم في مجال أمن المعلومات.
2. يتم تحديد الكفاءة بناءً على أسس التعليم والتدريب والخبرة المناسبة، والحصول على الشهادات التخصصية المعتمدة.
3. يجب أن توثق متطلبات الكفاءة في بطاقة الوصف الوظيفي.
4. يتم إجراء تقييم دوري للموظفين العاملين بأمن المعلومات، ويتم وضع إجراءات تصحيحية أو علاجية عند الحاجة.

مادة (11)
السرية

1. يلتزم جميع موظفي المؤسسة بالمحافظة على سرية المعلومات التي يحصلون عليها وعدم إفشائها حتى بعد انتهاء خدمتهم.
2. يلتزم المتعاقدون مع المؤسسة في مجال أمن المعلومات توقيع اتفاقية حفظ السرية.

مادة (12)
الأصول والعهد

يجب على المؤسسة القيام بالآتي:

1. تحديد الأصول والعهد المرتبطة بأمن المعلومات، والاحتفاظ بقائمة محدثة لهذه الأصول.

المرجع الإلكتروني للجريدة الرسمية
ELECTRONIC REFERENCE FOR THE OFFICIAL GAZETTE
mjr.lab.pna.ps

2. تحديد المستخدم أو المسؤول لكل أصل في قائمة الأصول.
3. المراجعة الدورية للأصول وإجراءات العهد وإجراءات التخلص من الأصول.
4. وضع سياسة تحكم بالوصول إلى الأصول، وتوثيقها ومراجعتها بشكل دوري.

مادة (13)
نقل الأصول

1. يجب على المؤسسة اعتماد إجراءات واضحة لنقل الأصول.
2. لا يتم نقل الأصول والمعدات دون أخذ الأذونات الرسمية اللازمة، وبناءً على إجراءات نقل الأصول المعتمدة من قبل المؤسسة.
3. يجب توثيق البيانات التعريفية والوظيفية لكل من يقوم بعمليات نقل الأصول.

مادة (14)
الوصول للمعلومات

يجب على المؤسسة القيام بالآتي:
1. تصنيف المعلومات المسموح للمستخدمين الوصول إليها حسب حاجات العمل.
2. اعتماد إجراء عمل رسمي لمنح أو إلغاء حقوق الوصول.

مادة (15)
التخلص من وسائط أمن المعلومات

1. يجب أن يتم التخلص من وسائط أمن المعلومات بشكل آمن.
2. على المؤسسة اعتماد إجراء موثق للتخلص من وسائط أمن المعلومات.

مادة (16)
المناطق ذات الخصوصية العالية

1. يجب على المؤسسة تعريف حدود المناطق ذات الخصوصية العالية، بما يتناسب مع متطلبات أمن المعلومات ونتائج تقييم المخاطر.
2. يجب بناء حواجز مادية لمنع الوصول المادي للمستخدمين غير المرخص لهم، حيثما لزم.

مادة (17)
ضوابط الدخول المادية

1. تضع المؤسسة ضوابط مكتوبة ومعلنة خاصة بالوصول للمناطق ذات الخصوصية العالية، لا سيما تحديد وتوثيق تصاريح الدخول للأفراد أو الموظفين، والأماكن المصرح الوصول لها، ويتم مراجعتها وتحديثها بشكل دوري.
2. يجب التحقق من هوية الزائرين، وتوثيق الدخول والخروج من وإلى المناطق ذات الخصوصية العالية في سجل خاص يحفظ في مكان آمن.

المرجع الإلكتروني للجريدة الرسمية
ELECTRONIC REFERENCE FOR THE OFFICIAL GAZETTE
mjr.lab.pna.ps

مادة (18)
موقع المعدات وحمايتها

يجب على المؤسسة بناءً على تقييم المخاطر تحديد جميع الأصول الحساسة الواجب إيداعها في المناطق ذات الخصوصية العالية، وتأمينها وحمايتها لتجنب الوصول غير المصرح به.

مادة (19)
تأمين التمديدات

1. يجب أن تكون خطوط الكهرباء وخطوط نقل البيانات الواصلة إلى المؤسسة محمية تحت الأرض أو محمية بوسائل مناسبة.
2. يجب فصل خطوط الكهرباء عن خطوط نقل البيانات.

مادة (20)
الصيانة

1. يجب إعداد سجل يدون فيه أي خطأ يحدث في الأجهزة والمعدات، ويتم تسجيل حركات الصيانة التي يتم تنفيذها.
2. يسمح للأشخاص المخولين من المؤسسة فقط بإجراء عمليات الصيانة للأجهزة والمعدات ذات العلاقة بأمن المعلومات.
3. يجب على المؤسسة اتخاذ الإجراءات الكفيلة للتأكد من عدم العبث بالمعدات والأجهزة التي تم إجراء الصيانة لها، والتأكد من أنه قد تم إجراء الصيانة المطلوبة لها.

مادة (21)
بيئة التطوير والفحص والتشغيل

يجب فصل بيئة التطوير والفحص عن البيئة التشغيلية للنظم المعتمدة في المؤسسة، وذلك لتقليل الوصول غير المصرح به.

مادة (22)
الحماية من البرمجيات الخبيثة

يجب على المؤسسة تطبيق إجراءات الكشف والحماية من البرمجيات الخبيثة.

مادة (23)
النسخ الاحتياطي

يجب على المؤسسة اعتماد سياسة النسخ الاحتياطي لجميع الأنظمة والبرامج الإلكترونية، وفحصها ومراجعتها بشكل دوري.

مادة (24)
سجلات الحركات

1. يجب أن يتم حماية الأماكن والمعلومات المتعلقة بسجلات الحركات من التلاعب بها أو الوصول إليها من قبل الأشخاص أو الجهات غير المصرح لها.

المرجع الإلكتروني للجريدة الرسمية
ELECTRONIC REFERENCE FOR THE OFFICIAL GAZETTE
mjr.lab.pna.ps

2. يتم مراجعة سجلات الحركات بشكل دوري للتأكد من عمليات تخزينها، وعدم وجود حركات تثير الشكوك والشبهة بوجود خلل.
3. يجب تسجيل الحركات والتعديلات التي يقوم بها الأفراد الذين يتولون مهمة إدارة وتشغيل الأنظمة في المؤسسة.

مادة (25)
إدارة أمن الشبكات

1. يجب على المؤسسة تشغيل أجهزة أو برمجيات مراقبة ومتابعة مناسبة في المناطق ذات الخصوصية العالية.
2. يجب على المؤسسة تحديد إجراءات عمل واضحة خاصة بإدارة الشبكات وأجهزتها والصلاحيات عليها.

مادة (26)
فصل الشبكات

تقوم المؤسسة باعتماد خطة فصل الشبكات فيها لضمان الحماية وتسهيل إدارة هذه الشبكات، بما يتناسب مع طبيعة عملها.

مادة (27)
نقل البيانات والمعلومات

1. يجب على المؤسسة وضع سياسات وإجراءات لحماية البيانات والمعلومات المنقولة بحسب طبيعة هذه البيانات والمعلومات والجهة المنقولة لها.
2. يتم تصنيف البيانات والمعلومات في المؤسسة للدلالة على درجة السرية، وتوثيق الأطراف الداخلية والخارجية المصرح لها بالاطلاع عليها.
3. يجب توقيع اتفاقيات لضمان حماية البيانات والمعلومات المصنفة المنقولة ما بين المؤسسة والجهات الخارجية.
4. يجب اعتماد مستويات وسائل حماية مشددة عند نقل البيانات على الشبكات العامة (الشبكات الخارجية وشبكة الإنترنت).

مادة (28)
متطلبات الحماية لأنظمة المعلومات

يجب على المؤسسة القيام بالتالي لحماية نظم المعلومات:

1. اعتماد إجراءات الأمن والحماية في جميع مراحل شراء الأصول وتطويرها وصيانتها.
2. تطبيق معايير الأمن والحماية لأخذها بعين الاعتبار في الأنظمة، على سبيل المثال:
   أ. حاجات العمل والمعايير القانونية والتنظيمية.
   ب. المحددات الإدارية والتقنية والمادية المتاحة لدعم أمن نظم المعلومات.

المرجع الإلكتروني للجريدة الرسمية
ELECTRONIC REFERENCE FOR THE OFFICIAL GAZETTE
mjr.lab.pna.ps

مادة (29)
قبول النظم المعلوماتية

لغايات قبول المؤسسة للنظم المعلوماتية يجب عليها:

1. تنظيم شروط ومعايير قبول الأنظمة الجديدة أو المحدثة.
2. تطبيق إجراءات فحص معتمدة قبل قبول الأنظمة.
3. اعتماد تشغيل الأنظمة فقط بعد اعتمادها من المؤسسة وفق أحكام هذا القرار.

مادة (30)
التحقق من البيانات المدخلة

يجب على المؤسسة أن تتحقق من صحة وصلاحية البيانات المدخلة على الأنظمة وقواعد البيانات، وفق إجراءات عمل تعتمدها لهذه الغاية.

مادة (31)
الأنظمة المطورة خارجياً

يشترط في الأنظمة المطورة خارجياً الآتي:

1. أن تشرف عليها المؤسسة.
2. أن يتم تدقيقها واعتمادها من مدقق مختص قبل إطلاق خدماتها.
3. أن توقع المؤسسة اتفاقية "عهدة حفظ الأنظمة" في الحالات التي لا تملك فيها المؤسسة الشيفرة المصدرية.

مادة (32)
العلاقة مع مزود الأنظمة

1. يجب أن تكون هناك سياسة مكتوبة للتعاقد مع مزود الأنظمة والأصول.
2. يجب الاحتفاظ بسجلات لدخول وخروج المزود.
3. يجب أن يكون هناك اتفاقية عمل رسمية بين المؤسسة والمزود وفق التشريعات السارية، على أن تتضمن تدقيق ومراقبة الولوج للأنظمة إلكترونياً أو ورقياً.

مادة (33)
التعامل مع حوادث أمن المعلومات

يجب على المؤسسة القيام بالآتي:

1. اعتماد إجراءات مكتوبة للتعامل مع حوادث أمن المعلومات.
2. توثيق الحوادث ونقاط الضعف والأحداث المشبوهة التي يتم رصدها، والإبلاغ عنها لمسؤول أمن المعلومات، الذي يقوم بالتعامل معها وفق إجراءات تعتمدها المؤسسة لهذه الغاية.

المرجع الإلكتروني للجريدة الرسمية
ELECTRONIC REFERENCE FOR THE OFFICIAL GAZETTE
mjr.lab.pna.ps

مادة (34)
النسخ الاحتياطي والاستعادة من الكوارث
يجب على المؤسسة أن تعتمد خطة الاستعادة من الكوارث والنسخ الاحتياطي.

مادة (35)
الإلغاء
يلغى كل ما يتعارض مع أحكام هذا القرار.

مادة (36)
السريان والنفاذ
على الجهات المختصة كافة، كل فيما يخصه، تنفيذ أحكام هذا القرار، ويعمل به من تاريخ نشره في الجريدة الرسمية.

صدر في مدينة رام الله بتاريخ: 2020/12/28 ميلادية
الموافق: 13/جمادى الأولى/1442 هجرية

د. محمد اشتية
رئيس الوزراء

المرجع الإلكتروني للجريدة الرسمية
ELECTRONIC REFERENCE FOR THE OFFICIAL GAZETTE
mjr.lab.pna.ps