قرار المجلس التنفيذي رقم (13) لسنة 2012
بشأن
أمن المعلومات في حكومة دبي

نحن حمدان بن محمد بن راشد آل مكتوم ولي عهد دبي رئيس المجلس التنفيذي

بعد الاطلاع على قانون العقوبات الصادر بالقانون الاتحادي رقم (3) لسنة 1987 وتعديلاته،
وعلى القانون الاتحادي رقم (7) لسنة 2002 في شأن حقوق المؤلف والحقوق المجاورة وتعديلاته،
وعلى القانون الاتحادي رقم (1) لسنة 2006 في شأن المعاملات والتجارة الإلكترونية،
وعلى القانون الاتحادي رقم (2) لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات،
وعلى القانون رقم (2) لسنة 2002 بشأن المعاملات والتجارة الإلكترونية،
وعلى القانون رقم (3) لسنة 2003 بشأن إنشاء مجلس تنفيذي لإمارة دبي،
وعلى قانون إدارة الموارد البشرية لحكومة دبي رقم (27) لسنة 2006 وتعديلاته،
وعلى القانون رقم (7) لسنة 2009 بإنشاء حكومة دبي الإلكترونية،
وعلى القانون رقم (8) لسنة 2010 بشأن دائرة الرقابة المالية وتعديلاته،

قررنا ما يلي:

التعريفات
المادة (1)

يكون للكلمات والعبارات التالية، حيثما وردت في هذا القرار، المعاني المبيّنة إزاء كل منها، ما لم يدل سياق النص على خلاف ذلك:

الإمارة: إمارة دبي.

الحكومة: حكومة دبي.

الجهات الحكومية:	الدوائر الحكومية والهيئات والمؤسسات العامة والمجالس والسلطات بما في ذلك سلطات المناطق الحرة، وأية جهة أخرى تابعة للحكومة.
الدائرة:	دائرة حكومة دبي الإلكترونية.
المعلومات:	المعلومات والبيانات والوثائق وأوعية المعلومات سواء كانت مطبوعة أو مكتوبة على الورق أو مخزنة إلكترونياً أو معالجة أو مرسلة بالبريد أو من خلال الوسائل الإلكترونية أو التي تظهر في التسجيلات المرئية أو المسموعة أو التي يُتلفظ بها في المحادثات المباشرة أو في أية وسيلة من وسائل الاتصال.
أنظمة المعلومات:	أي نظام محوسب أو يدوي تطبقه الجهات الحكومية بهدف إدارة ومعالجة المعلومات.
أمن المعلومات:	أي إجراء أو تدبير يتخذ لحماية أنظمة المعلومات أو المعلومات من الوصول إليها أو استخدامها أو الكشف عنها أو تعطيلها أو تعديلها أو تدميرها أو إلغائها أو حذفها بشكل غير مُصرّح به.
حوكمة أمن المعلومات:	مجموعة فرعية من حوكمة المؤسسات، تتكوّن من التوجيه الإستراتيجي والبناء التنظيمي والإجراءات الضرورية التي تكفل حماية مصادر المعلومات الحيوية وسريتها.
نظام أمن المعلومات:	الإطار العام لأمن المعلومات المعتمد من اللجنة.
اللجنة:	لجنة أمن المعلومات المشكّلة بمقتضى هذا القرار.

أهداف نظام أمن المعلومات

المادة (2)

يهدف نظام أمن المعلومات إلى تحقيق ما يلي:

1- إيجاد وتطوير إستراتيجية متكاملة، وسياسة موحدة، لأمن المعلومات وأنظمة المعلومات الخاصة بالحكومة وحمايتها من الاعتداء عليها أو من المخاطر التي تهددها باعتبارها ذات قيمة إستراتيجية وحيوية للإمارة.

2- إيجاد بيئة آمنة وموثوقة لتخزين وحفظ المعلومات الخاصة بالحكومة، واعتماد أفضل الوسائل الفعّالة التي تساعد على الحد من المخاطر المتعلقة بانتهاك أمن المعلومات.

3- تعزيز الوعي حول أهمية أمن المعلومات، من أجل ضمان ثقافة إلكترونية آمنة ومجتمع معلوماتي آمن.

4- تحديد أدوار ومسؤوليات الجهات الحكومية والموظفين العاملين لديها والمتعاملين معها، فيما يتعلق بأمن المعلومات بشكل واضح وعلى نحو يحول دون وقوع أي تضارب أو ازدواج في تلك الأدوار والمسؤوليات.

5- وضع الآليات التي تكفل الاستجابة للحوادث المتصلة بأمن المعلومات على نحو فعّال، وتحديد الممارسات والإرشادات التي تسهم في الحد من مخاطر تلك الحوادث.

6- ضمان أفضل أداء لأمن أنظمة المعلومات المطبقة لدى الجهات الحكومية بصورة تساعد هذه الجهات على القيام بمهامها المنوطة بها وتحقيق أهدافها الإستراتيجية بشكل آمن وفعّال.

نطاق تطبيق نظام أمن المعلومات

المادة (3)

أ- يطبق نظام أمن المعلومات على:

1- الجهات الحكومية والموظفين العاملين لديها.

2- المعلومات الخاصة بالحكومة بغض النظر عن نوعها والوعاء الذي يحويها.

3- الأشخاص والجهات الذين تتطلب طبيعة الأنشطة التي يزاولونها الدخول إلى أنظمة المعلومات الخاصة بالجهات الحكومية.

ب- يُستثنى من تطبيق نظام أمن المعلومات الجهات الحكومية التي تقرر اللجنة عدم إخضاعها له إما بصورة كلية أو جزئية إذا كانت تكاليف تطبيقه لدى تلك الجهات تفوق مستوى المخاطر المتوقعة، أو تفوق أهمية المعلومات المراد حمايتها.

مكوّنات نظام أمن المعلومات

المادة (4)

يتكوّن نظام أمن المعلومات مما يلي:

أ- المجالات المرتبطة بأمن المعلومات، والتي تتوزع إلى ثلاثة محاور رئيسة تتعلق بحوكمة أمن المعلومات وعمليات تشغيلها وضمان حمايتها، ويكون لكل مجال هدف يسعى نظام أمن المعلومات إلى تحقيقه، وهذه المجالات والأهداف المتعلقة بها هي:

1- **إدارة وحوكمة أمن المعلومات**، ويهدف هذا المجال إلى تأكيد أهمية وجود مفهوم أمن المعلومات في برامج وإستراتيجيات الجهات الحكومية.

2- **إدارة المعلومات والأصول المتعلقة بها**، ويهدف هذا المجال إلى منع الدخول غير المُصرّح به إلى المعلومات التي تصنف بأنها سرية، والمحافظة على الأوعية التي تحوي المعلومات الخاصة بالجهات الحكومية.

3- **إدارة الحوادث والمشاكل**، ويهدف هذا المجال إلى ضمان معالجة حوادث ونقاط ضعف أمن المعلومات، والإبلاغ عنها بطريقة تسمح باتخاذ إجراءات تصحيحية في الوقت المناسب من قبل الجهات الحكومية.

4- **إدارة المخاطر**، ويهدف هذا المجال إلى وضع وتطوير خطة لمواجهة ومعالجة المخاطر المتعلقة بأمن المعلومات من خلال تحديد التهديدات المحتملة للمعلومات وأنظمة المعلومات الخاصة بالحكومة ونقاط ضعفها ومجالات تحسين مستوى حمايتها.

5- **ضبط الدخول**، ويهدف هذا المجال إلى حفظ وحماية سرية المعلومات وضمان بقائها صحيحة وسليمة ومتطابقة لدى الجهات الحكومية وذلك من خلال ضبط الدخول إلى هذه المعلومات.

6- **إدارة العمليات والنظم والاتصالات**، ويهدف هذا المجال إلى الحد من المخاطر المرتبطة بالعمليات اليومية لأنظمة المعلومات والتطبيقات والشبكات وأدوات الاتصال سواء المستخدمة لدى الجهات الحكومية أو المخصصة للمتعاملين معها.

7- **التخطيط لاستمرارية الأعمال والأنشطة**، ويهدف هذا المجال إلى التحقق من أن خدمات تقنية المعلومات وبنيتها التحتية قادرة على مقاومة المخاطر الناجمة عن

الأخطاء أو الحوادث أو الهجمات بغية توفير المعلومات والمحافظة على سير العمل لدى الجهات الحكومية.

8- **امتلاك وتطوير وإدارة نظم المعلومات**، ويهدف هذا المجال إلى دمج أمن المعلومات في دورة امتلاك أو تطوير أنظمة المعلومات لمنع التعديل غير المُصرّح به على هذه الأنظمة أو إساءة استخدام المعلومات الخاصة بالحكومة ووضع أسس البرمجة الآمنة.

9- **حماية البيئة المحيطة بالمعلومات**، ويهدف هذا المجال إلى منع الأضرار والتهديدات والعبث في المرافق الخاصة بمعالجة المعلومات ومصادرها لدى الجهات الحكومية.

10- **دور ومسؤوليات الموارد البشرية**، ويهدف هذا المجال إلى تحديد أدوار ومسؤوليات موظفي الجهات الحكومية والمتعاملين معها المتعلقة بالمعلومات ومرافق المعالجة الخاصة بها، وذلك للحد من أية مخاطر أو انتهاكات مرتبطة بهذا الشأن.

11- **التنظيم التشريعي والرقابة**، ويهدف هذا المجال إلى تحديد التشريعات اللازمة في مجال تقنية المعلومات وتوعية الموظفين والمتعاملين بها لتفادي أية انتهاكات أو مخالفات لهذه التشريعات.

12- **ضمان أمن المعلومات وتقييم الأداء**، ويهدف هذا المجال إلى اختيار وتنفيذ وتطوير تدابير أمن المعلومات التي تساعد على صنع القرار داخل الجهات الحكومية وتحسين أدائها.

ب- الضوابط الرئيسة والفرعية التي يتم من خلالها تحقيق أهداف المجالات المبيّنة في الفقرة (أ) من هذه المادة.

ج- المصطلحات الفنية المتصلة بتقنية المعلومات ومعانيها بشكل واضح ودقيق.

التزامات الدائرة

المادة (5)

لغايات هذا القرار، تتولى الدائرة القيام بما يلي:

1- إعداد نظام أمن المعلومات وعرضه على اللجنة لاعتماده.

2- تزويد الجهات الحكومية بنظام أمن المعلومات المعتمد من اللجنة، وتقديم التوعية والإرشادات اللازمة لتطبيقه والعمل بمقتضاه.

3- وضع إستراتيجية فاعلة تقوم على تعزيز الشراكة والتعاون وتبادل المعلومات والخبرات بين الجهات الحكومية والقطاع الخاص في مجال أمن المعلومات.

4- وضع خطة طوارئ عامة على مستوى الحكومة والجهات الحكومية للمحافظة على أمن المعلومات ومراقبة تنفيذها، وإجراء التجارب العملية لاختبار نجاح هذه الخطة لضمان عدم تعرض المعلومات وأنظمة المعلومات للمخاطر والتهديدات المحتملة، ورفع التقارير اللازمة بهذا الشأن إلى اللجنة.

5- إخطار الجهات الحكومية بالحوادث الطارئة التي يمكن أن تؤثر على أمن المعلومات، وتزويد هذه الجهات بالتدابير والإجراءات التي تكفل التقليل من مستوى المخاطر المحتملة بهذا الشأن.

6- اتخاذ الإجراءات اللازمة لمواكبة الحلول العالمية المبتكرة في مجال أمن المعلومات، والاستفادة منها في بناء وتحديث وتطوير تقنية فعّالة لحماية المعلومات وأنظمة المعلومات الخاصة بالحكومة.

7- وضع وتصميم وتنفيذ برامج تدريبية متخصصة في مجال أمن المعلومات تواكب التطور التقني في هذا المجال وتفضي إلى تطبيق أفضل الممارسات اللازمة لحماية المعلومات والتصدي للمخاطر التي تهددها.

8- نشر ثقافة أمن المعلومات لدى موظفي الجهات الحكومية والمتعاملين معها، ووضع برامج التوعية والتثقيف المناسبة في هذا الشأن.

9- توفير الدعم الفني والإداري للجنة، ومتابعة تنفيذ القرارات والتوصيات الصادرة عنها.

10- التنسيق مع الجهات الحكومية بشأن سبل تطوير نظام أمن المعلومات، وتصويب أية ثغرات تعترض تطبيقه لدى تلك الجهات.

11- التنسيق مع الجهات الحكومية بشأن الإجراءات اللازمة لتنفيذ خطة الطوارئ العامة على مستوى الحكومة.

تشكيل اللجنة

المادة (6)

أ- تُشكّل بموجب هذا القرار لجنة تسمى "**لجنة أمن المعلومات**"، برئاسة مدير عام الدائرة وعضوية كل من:

1- ممثل عن شرطة دبي نائباً للرئيس.
2- ممثل عن الإدارة العامة لأمن الدولة.
3- ممثل عن الأمانة العامة للمجلس التنفيذي.
4- ثلاثة ممثلين عن جهات حكومية وخاصة يحددها مدير عام الدائرة.
5- ممثلين اثنين عن الدائرة يكون أحدهما مقرراً للجنة.

ب- تتم تسمية ممثلي الجهات المشار إليها في الفقرة (أ) من هذه المادة من قبل مسؤولي تلك الجهات، ويُراعى عند تسمية هؤلاء الممثلين أن يكونوا من ذوي الخبرة في مجال أمن المعلومات.

اجتماعات اللجنة

المادة (7)

أ- تعقد اللجنة اجتماعاتها بدعوة من رئيسها أو نائبه في حال غيابه مرة واحدة كل ثلاثة أشهر على الأقل، وكلما دعت الحاجة، وتكون اجتماعاتها صحيحة بحضور أغلبية أعضائها على أن يكون من بينهم رئيس اللجنة أو نائبه.

ب- تُصدِر اللجنة توصياتها وقراراتها بالإجماع أو بأغلبية أصوات أعضائها الحاضرين، وفي حال تساوي الأصوات يرجح الجانب الذي منه رئيس الاجتماع.

ج- يكون للجنة الاستعانة بمن تراه مناسباً من ذوي الخبرة والاختصاص، دون أن يكون لهم صوت معدود في مداولاتها.

د- تدوّن اجتماعات اللجنة وقراراتها في محاضر خاصة يوقع عليها رئيس الاجتماع والأعضاء الحاضرون.

اختصاصات اللجنة

المادة (8)

تتولى اللجنة القيام بما يلي:

1- دراسة نظام أمن المعلومات المعد من قبل الدائرة، واعتماده خلال مهلة لا تزيد على ثلاثة أشهر من تاريخ إحالته إليها من الدائرة.

2- متابعة تنفيذ نظام أمن المعلومات لدى الجهات الحكومية، ومدى التزامها بتطبيقه، ورفع التقارير اللازمة بهذا الشأن إلى رئيس المجلس التنفيذي للإمارة.

3- إجراء مراجعة دورية لنظام أمن المعلومات، وتقييم مستواه ومدى كفاءته في حماية المعلومات وأنظمة المعلومات الخاصة بالحكومة، وتحديد جوانب التطوير والتحديث التي يمكن إدخالها عليه، وجوانب الضعف والقصور التي تشوبه، وإصدار القرارات والتوصيات اللازمة بهذا الشأن.

4- دراسة التقارير المرسلة إليها من الجهات الحكومية حول نتائج تقييم مستوى المخاطر المتعلقة بأمن المعلومات لدى هذه الجهات وإصدار القرارات المناسبة بهذا الشأن.

5- التأكد من وجود خطة طوارئ خاصة بأمن المعلومات لدى الجهات الحكومية، وإجراء التقييم الدوري لهذه الخطة، وإصدار القرارات والتوصيات اللازمة بشأنها.

6- اقتراح التشريعات والسياسات والخطط والبرامج اللازمة لضمان مزيد من الحماية للمعلومات وأنظمة المعلومات الخاصة بالحكومة.

7- اقتراح التدابير اللازمة لتعزيز التنسيق والتعاون بين الجهات الحكومية في مجال أمن المعلومات، وتوحيد جهود هذه الجهات لحماية البنية التحتية لتقنية المعلومات لديها.

التزامات الجهات الحكومية

المادة (9)

تلتزم الجهات الحكومية بما يلي:

1- تزويد اللجنة خلال مدة أقصاها ستة أشهر من تاريخ إرسال نظام أمن المعلومات إليها بوثيقة مواءمة تتضمن بيان مجالات النظام القابلة للتطبيق لديها، وكذلك بجدول زمني يبين خطط وآليات ومراحل تطبيق هذه المجالات.

2- وضع البرامج والأنظمة التقنية والسياسات والإجراءات التي تحكم عملياتها بما يضمن تطبيق نظام أمن المعلومات بصورة تتلاءم وتتواءم مع نوع المعلومات الموجودة لديها وطبيعتها وأهميتها ومدى حساسيتها وسريتها.

3- إطلاع الموظفين العاملين لديها والمتعاملين معها على نظام أمن المعلومات وتدريبهم على تطبيقه بما يحويه من مجالات وأهداف وضوابط، ومراقبة مدى التزامهم به.

4- اتخاذ تدابير الأمن والسلامة اللازمة لحماية المعلومات الموجودة لديها، بما في ذلك منع الدخول أو التعديل أو التغيير غير المُصرّح به لتلك المعلومات، وحمايتها من الفقدان أو التسرب أو التلف أو التدمير أو الإضرار بها بأية صورة كانت.

5- وضع خطة طوارئ داخلية تتوافق مع خطة الطوارئ العامة المعتمدة من الدائرة وذلك بهدف المحافظة على أمن المعلومات وأنظمة المعلومات المتوفرة لدى الجهة الحكومية، وإجراء تجارب عملية لاختبار هذه الخطة لضمان عدم تعرض تلك المعلومات والأنظمة للمخاطر والتهديدات المحتملة.

6- الاستجابة السريعة والفعّالة والمنظمة لأية حوادث قد تضر بالمعلومات وأنظمة المعلومات الخاصة بها، وإجراء التحقيق اللازم في هذه الحوادث، وإبلاغ الجهات المختصة واللجنة بذلك.

7- توفير التوعية الأساسية في مجال أمن المعلومات للموظفين العاملين لديها، الذين تتصل مهام عملهم بتقنية المعلومات، والتأكد من أن هؤلاء الموظفين يدركون مسؤولياتهم بشأن حماية أمن المعلومات، والتهديدات المحتملة لهذه المعلومات، والمخاطر والانتهاكات التي قد تتعرض لها.

8- إجراء مراجعة دورية لمجالات وضوابط نظام أمن المعلومات المطبقة لديها حسب تقييم مستوى المخاطر القائمة أو المحتملة، وذلك بهدف التحقق من مدى مواءمة هذه المجالات والضوابط مع طبيعة مهامها واختصاصاتها وقابليتها للتحديث ورفع التوصيات اللازمة بهذا الشأن إلى اللجنة.

9- تزويد اللجنة بتقارير دورية تتضمن نتائج تقييم مستوى المخاطر المتعلقة بأمن المعلومات لديها، والإجراءات المتخذة من قبلها في مجال تطبيق نظام أمن المعلومات.

التزامات دائرة الرقابة المالية

المادة (10)

تتولى دائرة الرقابة المالية مراقبة تطبيق الجهات الحكومية لنظام أمن المعلومات، وإعداد التقارير اللازمة بهذا الشأن وتزويد اللجنة بنسخة منها.

التزامات موظفي الجهات الحكومية

المادة (11)

يجب على موظفي الجهات الحكومية التقيد بما يلي:

1- الالتزام بتطبيق نظام أمن المعلومات بما يضمن حماية المعلومات وأنظمة المعلومات الخاصة بالجهة الحكومية التي يعملون لديها.

2- عدم الإفصاح عن أية معلومات سرية، سواء بطبيعتها أو بحكم التعليمات الصادرة بشأنها، ما لم يتم الحصول على إذن خطي مسبق بذلك من قبل المرجع المختص في الجهة الحكومية التي يعملون لديها.

3- المحافظة على أمن المعلومات، وعدم القيام بأي إجراء من شأنه أن يؤدي إلى تغيير تلك المعلومات أو تعديلها أو تدميرها أو إتلافها أو حذفها أو إلغائها أو فقدانها ما لم يكن ذلك صادراً عن موظف مختص مُصرّح له بذلك.

4- إخطار رؤسائهم المباشرين والجهات المختصة عن أية تهديدات أو اختراقات أو انتهاكات أو حوادث يمكن أن تؤدي إلى كشف المعلومات المتوفرة لدى الجهة الحكومية التي يعملون لديها أو تغييرها أو تعديلها أو تدميرها أو إتلافها أو حذفها أو إلغائها أو فقدانها.

5- عدم استخدام أو استغلال المعلومات في غير الأغراض المحددة أو المخصصة لها.

6- عدم السماح لغير المخولين بالدخول إلى أنظمة المعلومات المطبقة لدى الجهات الحكومية التي يعملون لديها.

التدابير والإجراءات

المادة (12)

يكون عرضة للمساءلة التأديبية كل موظف من موظفي الجهات الحكومية يخالف تدابير الأمن والسلامة المعتمدة لدى هذه الجهات بشأن حماية أمن المعلومات بصورة تؤدي إلى تغييرها أو تعديلها أو تدميرها أو إتلافها أو حذفها أو إلغائها أو فقدانها، وذلك مع عدم الإخلال بمسؤوليته المدنية أو الجزائية عند الاقتضاء.

التزامات المتعاملين مع الجهات الحكومية

المادة (13)

على الأشخاص والجهات الذين تتطلب طبيعة الأنشطة التي يزاولونها الدخول إلى أنظمة المعلومات المطبقة لدى الجهات الحكومية، التقيد بالالتزامات التالية، وذلك تحت طائلة المسؤولية المقررة بموجب التشريعات السارية:

1- مراعاة التعليمات الصادرة عن الجهات الحكومية بشأن أمن المعلومات.

2- عدم القيام بأي فعل يكون من شأنه أن يؤدي إلى تغيير المعلومات الخاصة بالحكومة أو تعديلها أو تدميرها أو إتلافها أو حذفها أو إلغائها أو فقدانها.

3- عدم القيام بأي فعل من شأنه أن يؤدي إلى تعطيل أنظمة المعلومات الخاصة بالحكومة بصورة تصبح معها غير صالحة أو غير قادرة على القيام بوظائفها.

4- عدم استعمال أو استغلال المعلومات الخاصة بالحكومة لغير الأغراض المحددة لها.

5- عدم نسخ أو نشر أية معلومات خاصة بالحكومة إلا بعد الحصول على الموافقة الخطية المسبقة من الجهة الحكومية المعنيّة.

6- عدم السماح لغير المخولين بالدخول إلى أنظمة المعلومات المطبقة لدى الجهات الحكومية التي يتعاملون معها.

ملكية نظام أمن المعلومات

المادة (14)

يعتبر نظام أمن المعلومات وكافة مكوّناته من البيانات والمعلومات والبرامج ملكاً للحكومة، ولهذه الأخيرة وحدها صلاحية التصرف به بأية صورة من الصور.

تعديل نظام أمن المعلومات

المادة (15)

يكون لمدير عام الدائرة، وبناء على توصية اللجنة، تعديل أي من مجالات نظام أمن المعلومات وأهدافه وضوابط الوصول إلى هذه الأهداف بصورة تحقق غايات النظام المذكور وإخطار الجهات الحكومية التي تطبقه بذلك التعديل وذلك بعد اعتماده من اللجنة.

مهلة إعداد نظام أمن المعلومات

المادة (16)

على الدائرة، خلال مهلة لا تزيد على ثلاثة أشهر من تاريخ العمل بهذا القرار، إعداد نظام أمن المعلومات وعرضه على اللجنة لاعتماده، وإرساله بعد الاعتماد إلى الجهات الحكومية لتطبيقه والعمل بمقتضاه.

اللوائح التنفيذية

المادة (17)

يُصدر مدير عام الدائرة اللوائح والتعليمات اللازمة لتنفيذ أحكام هذا القرار.

الإلغاءات

المادة (18)

يُلغى أي نص ورد في أي قرار آخر إلى المدى الذي يتعارض فيه وأحكام هذا القرار.

النشر والسريان

المادة (19)

يُنشر هذا القرار في الجريدة الرسمية، ويُعمل به من تاريخ نشره.

حمدان بن محمد بن راشد آل مكتوم

ولي عهد دبي

رئيس المجلس التنفيذي

صدر في دبي بتاريخ 11 إبريل 2012م

الموافـــق 19 جمادى الأولى 1433هـ