حكومة دبي
GOVERNMENT OF DUBAI

مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER

نظام أمن المعلومات

الإصدار 3.1

حكومة دبي
GOVERNMENT OF DUBAI

مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER

نظام أمن المعلومات

الإصدار 3.1

شكر وتقدير

شكر وتقدير

قام مركز دبي للأمن الإلكتروني بتحديث نظام أمن المعلومات الحكومية في دبي وفقاً لقانون دبي رقم 11 لسنة 2014 والقرار رقم 13 لسنة 2012 الصادر عن رئيس مجلس دبي التنفيذي حول تنظيم أمن المعلومات لحكومة دبي. و يشمل هذا النظام العديد من مجالات أمن المعلومات التي تتألف من ضوابط وضوابط فرعية محددة، ويتماشى بشكل وثيق مع المعايير الدولية الأخرى المتعلقة بأمن المعلومات والتي تعكس تأكيد حكومة دبي واعتمادها الممارسات المتعلقة بأمن المعلومات المدرجة في هذا المعيار. كما يتضمن النظام بنوداً خاصة تعكس خصوصية متطلبات حكومة دبي في مجال أمن المعلومات. و يود مركز دبي للأمن الإلكتروني أن يعرب عن شكره وتقديره لأعضاء الفريق الذين قاموا بالعمل على مراجعة هذا النظام في مركز دبي للأمن الإلكتروني ومختلف هيئات حكومة دبي التي تمت استشارتها خلال مراجعة التقرير. و قد أجرى مركز دبي للأمن الالكتروني المراجعة النهائية لهذا النظام وقام بالموافقة عليه.

يوسف الشيباني

الرئيس التنفيذي
مركز دبي للأمن الإلكتروني

جدول المحتويات

جدول المحتويات

1. المقدمة

تعتمد الأنشطة الإقتصادية والإجتماعية المعاصرة بشكل متزايد على معالجة المعلومات، ويستخدم الأفراد والمجتمعات ومؤسسات القطاعين العام والخاص هذه المعلومات كعنصر أساسي للتواصل فيما بينهم. وقد لعب التقدم المنجز في تكنولوجيا المعلومات والإتصال، بالإضافة الى الأنماط غير الإلكترونية القائمة حالياً، دوراً كبيراً على صعيد تعزيز نوعية الحياة ورفاهية المجتمعات التي باتت تعتمد الخدمات الإلكترونية أسلوباً بديلاً في العلاقات ما بين الأفراد والجهات الحكومية؛ بكونه اسلوباً يقلل التكاليف بشكل ملموس ويحد من الهدر في الوقت. وكذلك على صعيد الازدهار الاقتصادي الذي باتت التكنولوجيا عصبه الحيوي. وهكذا باتت التحديات التي تكمن في ضمان القدرة على الاستجابة والمرونة في التعامل مع المخاطر التي تهدد أمن المعلومات تكتسب أهمية متزايدة؛ إذ إن البيئة الآمنة لمعالجة المعلومات تعزز المنافع التي يجنيها المتعامل، كما تعزز أداء العمل والإنتاجية والأمن الوطني إلى حدٍ كبير. على النقيض من ذلك؛ تولد البيئة غير الآمنة إحتمال وقوع أضرار بالغة للمؤسسات بشكل قد يقوض ثقة المتعاملين والمقيمين إلى حدٍ بعيد. وتزداد المخاطر على وجه الخصوص لدى الجهات العاملة في أنشطة ذات طبيعة حيوية، مثل حوكمة القطاع العام وتوليد الطاقة الكهربائية والمعاملات المالية وخدمات الرعاية الصحية ... إلخ.

يشمل نظام أمن المعلومات لحكومة دبي الممارسات الأساسية المعتمدة في هذا المجال؛ وهو نظام صمم لضمان عدم المساس بالمعلومات الحكومية، ولتشجيع الموظفين في حكومة دبي على تبني أفضل الممارسات على هذا الصعيد، وكذلك للتأكد من وجود آليات فعالة للاستجابة للحوادث التي قد تمس هذه المعلومات. كما أن من أهداف هذا النظام تكوين ثقافة خاصة بأمن المعلومات لدي كافة الجهات التابعة لحكومة دبي؛ ثقافة كفيلة بتشجيع تلك الجهات على تضمينه كجزء أصيل من إستراتيجياتها: الحالية والمستقبلية.

2. الغرض

يهدف نظام أمن المعلومات إلى تزويد جميع الجهات التابعة لحكومة دبي بالمعايير التي من شأنها ضمان استمرارية إجراءات العمل الهامة وتقليل المخاطر والأضرار المتعلقة بأمن المعلومات، من خلال الحيلولة دون وقوع حوادث أمن المعلومات و/ أو الحد منها. كما يهدف أيضاً إلى المحافظة على مستوى مقبول من ضوابط تداول أصول المعلومات في الجهات التابعة لحكومة دبي؛ من حيث سريتها ومصداقيتها وتوافرها.

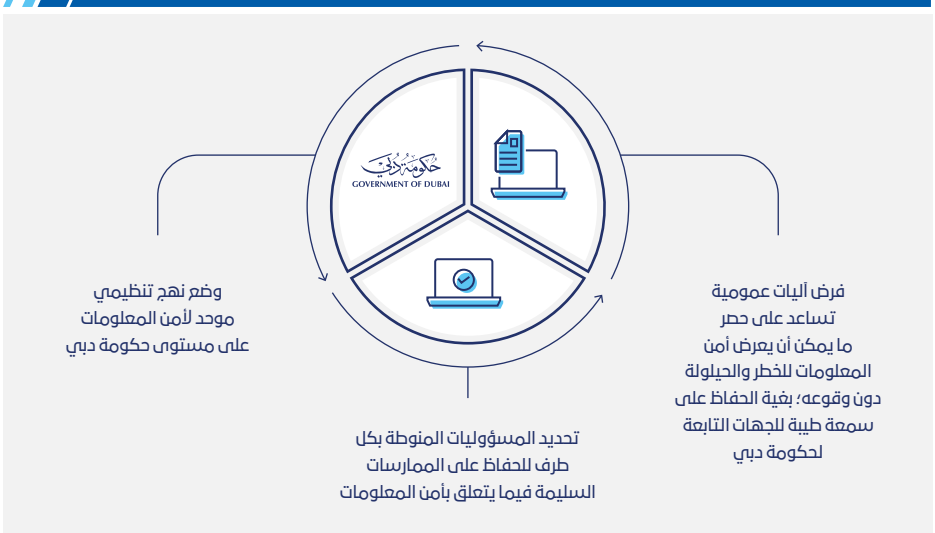
تتلخص أهداف نظام أمن المعلومات فيما يأتي:

أ. وضع نهج تنظيمي موحد لأمن المعلومات على مستوى حكومة دبي.

ب. فرض آليات عمومية تساعد على حصر ما يمكن ان يعرض أمن المعلومات للخطر والحيلولة دون وقوعه؛ بغية الحفاظ على سمعة طيبة للجهات التابعة لحكومة دبي.

ت. تحديد المسؤوليات المنوطة بكل طرف للحفاظ على الممارسات السليمة فيما يتعلق بأمن المعلومات.

أهداف نظام أمن المعلومات

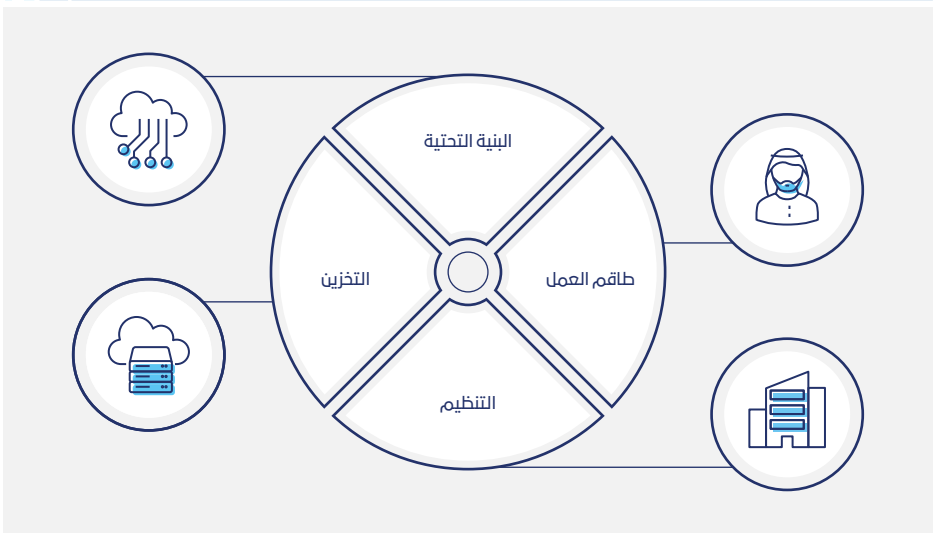


ويعد نظام أمن المعلومات إطاراً محايداً غير ذي صلة بأي تقنية، وليس من شأنه معالجة أي تطبيق تقني. وبناءً عليه فإن على الجهات التابعة لحكومة د بي ان تتناول النواحي الخاصة بالتقنية المعدة للتطبيق بما يعكس خصوصية نُظُمها الداخلية. كما سيتعين على تلك الجهات أن تضع مجموعة من السياسات والإجراءات التي تحكم سير عملياتها بما يتماشى مع هذا النظام. وتبعاً لذلك، لابد من وضع برامج أمن المعلومات/نظم إدارة أمن المعلومات وتطبيقها والحفاظ عليها لدى كل جهة تابعة لحكومة دبي.

3. نطاق العمل

يمثل نظام أمن المعلومات الحد الأدنى لمتطلبات ضوابط أمن المعلومات، وهي متطلبات قابلة للتطبيق في جميع الجهات التابعة لحكومة دبي؛ بما في ذلك، على سبيل المثال لا الحصر، الموظفون والاستشاريون والمقاولون والزوار غير العاملين بالحكومة والذين يتعاملون معها عبر قنوات متنوعة. علاوة على ذلك، ينطبق هذا النظام على أي معلومات حكومية بغض النظر عن نوعها ووسيطها (مثل المطبوعة الإلكترونية وغير الإلكترونية والشفوية والكتابية ... إلخ)، وعليه، يجب تطبيق هذا النظام في كامل الوحدات التنظيمية للجهات التابعة لحكومة دبي وألا يقتصر تطبيقها على الأقسام/الإدارات الخاصة بتقنية المعلومات فحسب.

المكونات وإجراءات العمل ومرافق معالجة المعلومات الهامة



يجب أن يأخذ نطاق عمل برنامج إدارة أمن المعلومات في الاعتبار جميع إجراءات العمل ومرافق معالجة المعلومات الهامة والمكونات، بما في ذلك:

أ. التخزين (نظم التخزين الإلكترونية سواء الافتراضية أو الفعلية، الوثائق الورقية ... إلخ)؛

ب. البنية التحتية (الأجهزة، التطبيقات، الشبكات ... إلخ)؛

ت. التنظيم (الإجراءات، السياسات ... إلخ)؛

ث. طاقم العمل (الإداريون، الموظفون، الزوار ... إلخ).

4. ملكية حكومة دبي للمعلومات

تمتلك حكومة دبي بشكل كامل كافة المعلومات التي جرت معالجتها من قبل كافة الجهات التابعة لها. ويمكن لكافة موظفي حكومة دبي تنفيذ أنشطة معالجة المعلومات على تنوعها وفقاً لما يتطلبه العمل، بل ويمكنهم التصرف بشكل مؤقت بالمعلومات نيابةً عن جهاتهم، شريطة أن يكون قد تم منحهم التفويضات الملائمة ذات الصلة. وتعمل الجهات التابعة لحكومة دبي على تحديد مثل هذه الصلاحيات المتعلقة بمعالجة المعلومات بالتوافق مع ما تتمتع به من التفويضات والقوانين واللوائح المعمول بها (بما يتماشى مع الضوابط 11.1 و 11.2). إن حماية المعلومات السرية ذات أولوية عالية من أجل الحفاظ على الحقوق الفردية وعلى الخصوصية.

لابد لأي عملية معالجة للمعلومات الشخصية والمعلومات المصنفة أن تكون مشروعة ومنصفة، وأن تكون وثيقة الصلة بالموضوع، دون أيما زيادة عن الأغراض التي أجريت من أجلها. وهذه الأغراض ينبغي أن تكون واضحة ومشروعة ومحددة قبل أوان جمع المعلومات. وتماشياً مع الضابط 6.5، يجوز للجهات التابعة لحكومة دبي أن تتقاسم المعلومات وتتبادلها مع جهات حكومية أخرى؛ وفق ما تراه مناسباً، وبما يتماشى مع القوانين واللوائح المعمول بها (وبما يتماشى مع الضوابط 11.1 و11.2)، وذلك لأغراض توفير الخدمات للجمهور وقطاع الأعمال (حتى لو لم يكن الكشف عن المعلومات متوقعاً في وقت جمعها)، أو لأغراض إدارتها الداخلية.

5. ملكية نظام أمن المعلومات وحق تعديله

تعود ملكية نظام أمن المعلومات إلى حكومة دبي، طبقاً للمادة (14) من قرار المجلس التنفيذي لحكومة دبي رقم (13) الصادر في العام 2012. وتحتفظ حكومة دبي بحق تعديل هذا النظام بما يتوافق مع احتياجات العمل المتغيرة ومع أولوياتها في الوقت المناسب؛ وفقاً لما ورد في القرار المذكور آنفاً.

6. الإلتزام بنظام أمن المعلومات

على كافة الجهات التابعة لحكومة دبي وموظفيها واستشاريها ومقاوليها وزوارها أن يكونوا على دراية بالعواقب المترتبة على عدم التقيد بالإرشادات المحددة في نظام أمن المعلومات.

إن الجهات التابعة لحكومة دبي التي تخفق في التقيد بهذه الإرشادات الموجودة في نظام أمن المعلومات تجازف بكشف معلومات مصنفة حساسة لأطراف غير

مخولة بالاطلاع عليها، أو توفر معلومات غير صحيحة للمتعاملين، أو تحول دون الوصول إلى معلومات حساسة.

وفي حالة تبين عدم إلتزام الجهات/الموظفين بهذه الإرشادات، فسيتم إلغاء حق أي منهم في الدخول إلى نظم المعلومات، وقد يخضعون لإجراءات تأديبية وفقاً للقوانين والسياسات المعمول بها حالياً في دولة الإمارات العربية المتحدة وفي حكومة دبي.

إن الامتثال للقوانين القائمة حالياً أو لأي تشريعات أخرى في المستقبل فيما يتعلق بأمن المعلومات له أسبقية على نظام أمن المعلومات نفسه.

7. قابلية التطبيق والإستثناءات من نظام أمن المعلومات

على الجهات التابعة لحكومة دبي مراجعة إمكانية تطبيق المجالات والضوابط الخاصة بنظام أمن المعلومات لتحديد تلك المجالات والضوابط التي يمكن تطبيقها فيها. يجب على الجهات الحكومية في دبي أن تلزم الموارد لتحقيق التنفيذ «المناسب»، مع مراعاة نتائج تقييم المخاطر، والحفاظ على أن تكون تكلفة تنفيذ الضوابط أقل من المخاطر المتوقعة أو قيمة المعلومات التي يتم حمايتها.

وإذا تطلب الأمر وجود استثناء من أي جزء من النظام، يجب على الشخص المخول من الإدارة العليا في الجهة التابعة لحكومة دبي الطالبة للاستثناء تقديم طلب مكتوب رسمي إلى مركز دبي للأمن الإلكتروني، على أن يتضمن هذا الطلب وصفاً للاستثناء وشرحاً لمبرراته وتقييماً للمخاطر التي قد تنجم عنه.

8. هيكل نظام أمن المعلومات

جرى تقسيم نظام أمن المعلومات إلى ثلاثة عشر مجالاً، كل مجال منها يأخذ بعين الإعتبار أحد المحاور الرئيسية لأمن المعلومات أو أكثر. وهي: الحوكمة، والتشغيل، والضمان (ضمان حسن التطبيق).

فالمجالات التابعة لمحور الحوكمة تحدد المستلزمات الأساسية المطلوبة لبناء أمن المعلومات وإدارتها. أما مجالات التشغيل فهي عبارة عن ضوابط فنية و/أو غير فنية يجوز لجهة ما استخدامها بناءً على نتائج الدراسة التي أجرتها لتقييم المخاطر. وأما مجالات الضمان فتعمل بما يضمن الجودة للجهة، حيث تؤكد أن العمل بالحل المنفذ يجري كما ينبغي له فعلاً أن يجري.

الجدول 1. مجالات نظام أمن المعلومات ومحاورها

المجالات	المحاور		
	الحوكمة	التشغيل	الضمان
المجال 1 – إدارة أمن المعلومات وحوكمتها	✓		
المجال 2 – إدارة المعلومات والأصول المتعلقة بها	✓	✓	
المجال 3 – إدارة المخاطر	✓	✓	
المجال 4 – إدارة الحوادث والمشاكل		✓	
المجال 5 – ضبط الدخول		✓	
المجال 6 – إدارة العمليات والنظم والإتصالات		✓	
المجال 7 – التخطيط لاستمرارية الأعمال والأنشطة	✓	✓	
المجال 8 – امتلاك وتطوير وإدارة نظم المعلومات		✓	
المجال 9 – حماية البيئة المحيطة بالمعلومات		✓	
المجال 10– دور ومسؤوليات الموارد البشرية	✓	✓	
المجال 11 – التنظيم التشريعي والرقابة	✓		✓
المجال 12 – ضمان أمن المعلومات وتقييم الأداء	✓		✓
المجال 13 – أمن السحابة الإلكترونية	✓	✓	

لقد جرت هيكلة نظام أمن المعلومات على النحو التالي:

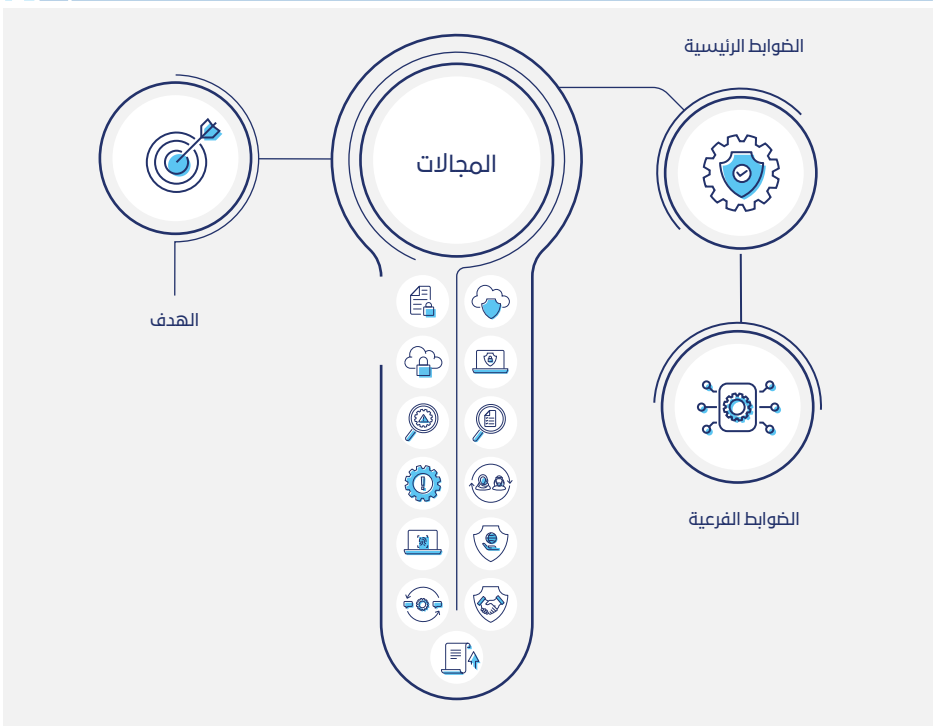
أ. المجالات: وتعبر عن إجراء رئيسي في أمن المعلومات؛

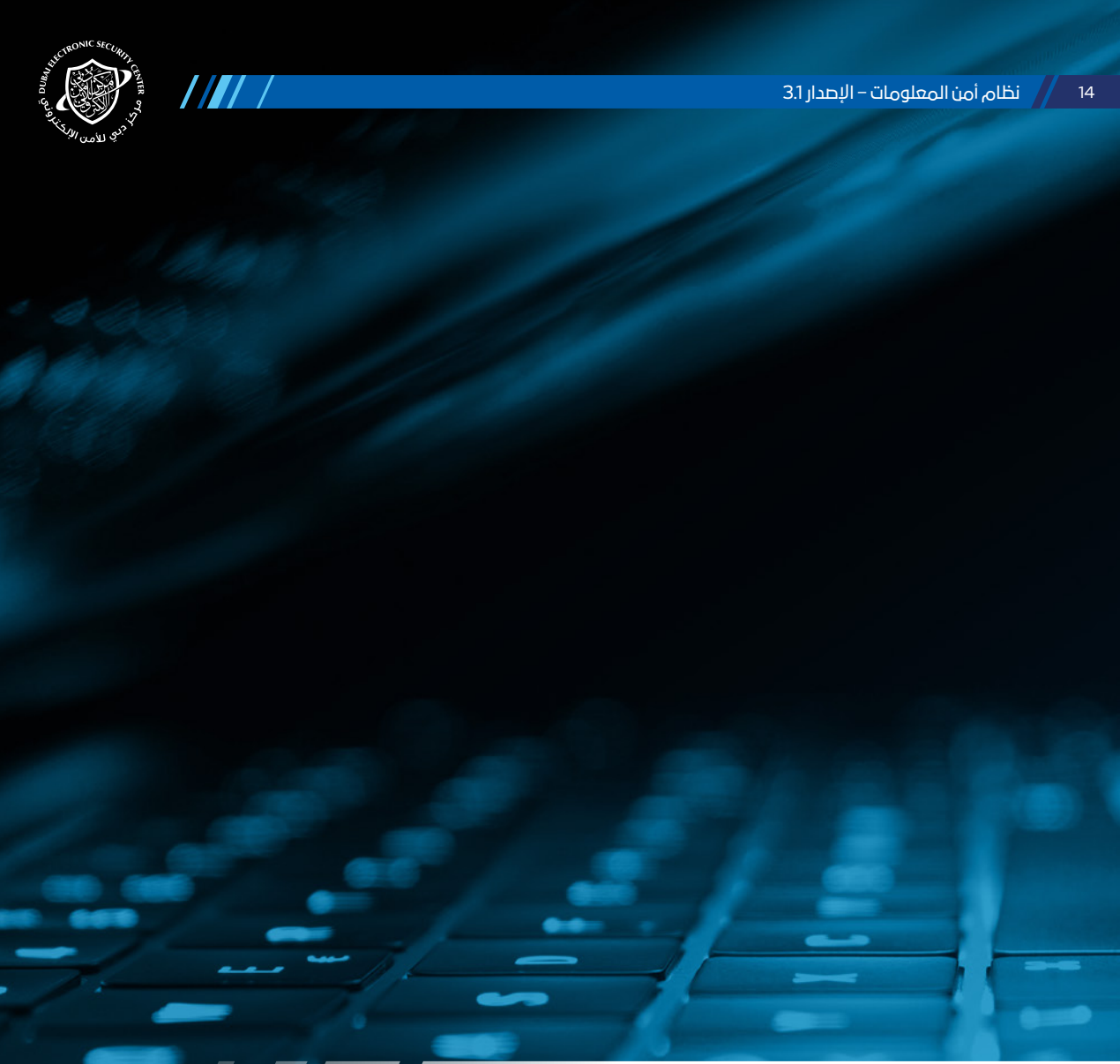
ب. الهدف: يعبر عما يتوقع تحقيقه من المجال؛

ت. الضوابط الرئيسية: تعبر عن ما ينبغي تطبيقه لتحقيق الهدف؛

ث. الضوابط الفرعية: تعبر عن الضوابط التفصيلية الفرعية للضوابط الرئيسية.

هيكلة نظام أمن المعلومات





المجال 1
إدارة وحوكمة أمن المعلومات

المجال 1
إدارة و حوكمة أمن المعلومات

الهدف

التأكيد على أهمية وجود مفهوم أمن المعلومات في برامج و استراتيجيات الجهات الحكومية كجزء من. الحوكمة الشاملة، و ذلك من خلال توفير الآتي:

أ. مواءمة أمن المعلومات مع التوجه الاستراتيجي للجهة؛

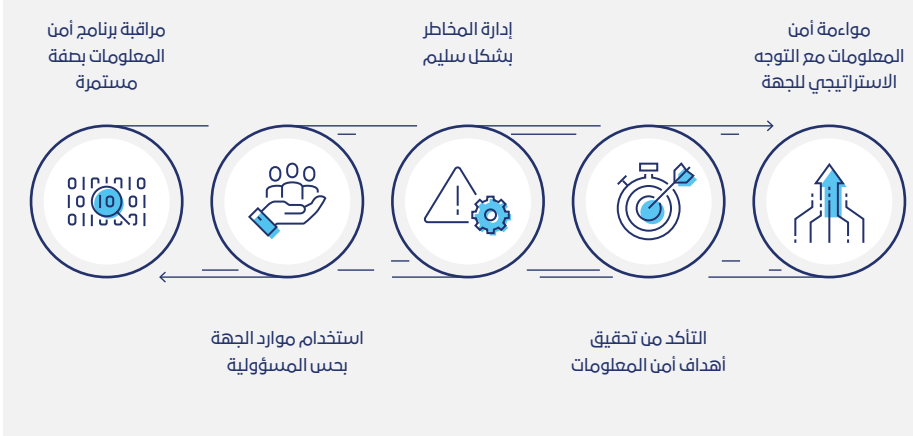
ب. التأكد من تحقيق أهداف أمن المعلومات؛

ت. إدارة المخاطر بشكل سليم؛

ث. استخدام موارد الجهة بحس المسؤولية؛

ج. مراقبة برنامج أمن المعلومات بصفة مستمرة.

أمن المعلومات في برامج واستراتيجيات الجهات الحكومية



الضابط الرئيسي – 1.1 أدوار أمن المعلومات و المسؤوليات المترتبة عليها:

تتلخص الغاية الرئيسية لتحديد أدوار أمن المعلومات و المسؤوليات المترتبة عليها في توضيح أدوار الأفراد، و تحديد مواضع المساءلة و المحافظة على فصل المهام، و إزالة أي تضارب في المصالح. و بالتالي، فمن أجل تطوير استراتيجية كاملة، و سياسة و برنامج متوافقين لأمن المعلومات في الجهة، ينبغي تحديد جميع الأدوار و المسؤوليات المتعلقة بأمن المعلومات و تعريفها بوضوح؛ و ذلك على النحو المقترح بشكل مبدئي و عام أدناه، أو بأي أسلوب آخر خاص بالجهة؛ بما لا يتعارض مع متطلبات هذا الضابط:

الضابط الفرعي – 1.1.1 مجلس الإدارة:

1.1.1.1. يتعين على مجلس الإدارة قبول مسؤولية أمن المعلومات و إبداء الالتزام بها؛

1.1.1.2. يكلف مجلس إدارة الجهة بمسؤولية الإشراف العام على إدارة برنامج أمن المعلومات و تنفيذه بشكل صحيح، و بمراجعة تقارير تقييم المخاطر.

الضابط الفرعي – 1.1.2 المدير العام/المدير التنفيذي:

1.1.2.1. يكلف المدير العام أو المدير التنفيذي، و الذي يكون تابعاً إدارياً لمجلس الإدارة، بالمسؤوليات الآتية:

أ. قبول المسؤولية العامة لأمن المعلومات و الإقرار بها؛

ب. فرض نظام لإدارة أمن المعلومات في الجهة؛

ت. فرض تطبيق سياسات أمن المعلومات في الجهة؛

ث. مراقبة التزام القطاعات بنظام إدارة أمن المعلومات و سياسات أمن المعلومات و متابعته؛

ج. فرض إجراءات المساءلة تجاه أمن المعلومات.

الضابط الفرعي – 1.1.3 اللجنة التوجيهية لأمن المعلومات:

1.1.3.1 يجب إنشاء لجنة توجيهية لأمن المعلومات يترأسها المدير العام أو نائبه (على ألا يكون مسؤولاً عن تنفيذ سياسات أمن المعلومات التقنية/

التشغيلية) و تضم رؤساء كل قطاع في الجهة. و على هذه اللجنة أن تتولى الأدوار و المسؤوليات الآتية:

أ. الإشراف على تنفيذ نظام إدارة أمن المعلومات و ضوابطه على مستوى الجهة، و التأكد من ذلك؛

ب. إجراء مراجعات دورية على تطبيق نظام أمن المعلومات، و أية ضوابط و أهداف لأمن المعلومات؛

ت. مراجعة و اعتماد سياسات و إجراءات أمن المعلومات بشكل دوري من أجل تنفيذها داخل الجهة؛

ث. تعزيز ثقافة أمن المعلومات في الجهة و نشرها؛

ج. التأكد من أن منهجية أمن المعلومات ذات الصلة هي جزء من جميع إجراءات العمل و أية مبادرات أو مشاريع جديدة في جميع إدارات أو وظائف الجهة؛

ح. متابعة و مراجعة نتائج التدقيق الداخلي و الخارجي من أجل فعالية تنفيذ نظام أمن المعلومات و ضمان اتخاذ الإجراءات التصحيحية اللازمة في الوقت المناسب؛

خ. مراجعة و اعتماد منهجية تقييم مخاطر أمن المعلومات و وضع معايير محددة لمخاطر أمن المعلومات المقبولة و مستويات التعرض لها؛

د. ضمان توفير الموارد الكافية لتطبيق نظام إدارة أمن المعلومات، و دعمه و تشغيله؛

ذ. وضع توصيات لكل من الإجراءات التصحيحية و الوقائية، اشتقاقاً من النهج المتبع لتقييم المخاطر؛

ر. مراجعة حوادث أمن المعلومات و الاستجابة لها؛

ز. التأكد من تنفيذ التوصيات الصادرة عن اجتماعات اللجنة؛

س. ضمان دمج متطلبات أمن المعلومات كجزء من المتطلبات التعاقدية في أنشطة إدارة المشاريع؛

ش. مراجعة و اعتماد خطط معالجة المخاطر و أي مخاطر متبقية بناء على تقييم المخاطر؛

الضابط الفرعي – 1.1.4 الإدارة العليا:

1.1.4.1 تكلف الإدارة العليا للجهة بالمسؤوليات الآتية:

أ. التأكد من أن كل موظف، أو موظفة، يتفهم مسؤولياته المتعلقة بأمن المعلومات بعد قراءة سياسة أمن المعلومات و يقر من خلال تسجيل رسمي أنه يفهم و يعتزم الامتثال لتلك المتطلبات؛

ب. تحديد الأهمية و مخاطر الأعمال المتعلقة بنظم المعلومات و الأصول الخاصة بها؛

ت. إجراء تقييم دوري لأصول المعلومات، و للمخاطر المرافقة لها؛

ث. إبلاغ نتائج تقييم المخاطر إلى أصحاب المصلحة المعنيين؛

ج. تحديد امتيازات الدخول المرتبطة بأصول المعلومات و نظم المعلومات التابعة لها، و مراجعتها بصفة دورية؛

ح. تطبيق سياسات و إجراءات أمن المعلومات لتستهدف تقليل منسوب المخاطر إلى مستويات مقبولة، بطريقة مجدية اقتصادياً؛

خ. ضمان تنفيذ اختبارات تقنية لأمن أنظمة المعلومات بصفة دورية؛

د. ضمان الإبلاغ عن أي دليل على وجود تهديد لأمن المعلومات أو أي نشاط مشبوه قد يؤدي إلى كشف أو تلف أو تدمير معلومات الجهة؛

ذ. الاستجابة لحوادث أمن المعلومات؛

ر. ضمان إدراج متطلبات أمن المعلومات في أنشطة/عقود مشاريع الإدارة المعنية.

الضابط الفرعي – 1.1.5 المسؤول عن أمن المعلومات:

1.1.5.1 تسند مسؤولية أمن المعلومات في الجهة الحكومية إلى فرد أو فريق متخصص، على أن يكون رئيس فريق حوكمة أمن المعلومات من مواطني دولة الإمارات العربية المتحدة، و يتمتع بالمؤهلات و الاستقلالية، و أن يتبع مباشرةً الإدارة العليا، و أن تتم مراعاة الفصل بين المهام و إزالة أي تضارب بالمصالح و يناط بصاحب هذه الوظيفة ما يأتي من مهام:

أ. تخطيط برنامج أمن المعلومات و تنفيذه و متابعته، ليأتي متكاملاً مع إجراءات الجهة ككل؛

ب. التنسيق مع الإدارة العليا لتحديد أصول المعلومات على مستوى الجهة و تطويرها و تأمين مناولتها و إدارتها؛

ت. تخطيط منهجية لتقييم مخاطر أمن المعلومات للجهة وتطويرها وتحديثها، مع تأكيد مراجعتها وتحديثها باستمرار بالتنسيق مع الإدارة العليا لدى الجهة؛

ث. ضمان تحديد الضوابط التشغيلية الملائمة وتنفيذها تبعاً لنتائج تقييم المخاطر؛

ج. تطوير السياسات و الإجراءات اللازمة تبعاً لنتائج تقييم المخاطر، بالتنسيق مع ملاك العمليات المعنيين؛

ح. ضمان امتثال الجهة لبرنامج أمن المعلومات، رفع تقارير حالة تنفيذ نظام أمن المعلومات للجنة التوجيهية لأمن المعلومات؛

خ. مساعدة الإدارة العليا و دعمها في تأدية مسؤولياتها تجاه أمن المعلومات؛

د. إعداد خطط التوعية و التدريب و التعليم الأمني المناسبة و تنفيذها بصفة دورية لموظفي الجهة و الأطراف الخارجية المعنية، بما في ذلك الشركاء و مزودي الخدمات و الاستشاريين... إلخ؛

ذ. ضمان الامتثال لسياسات و معايير مركز دبي للأمن الإلكتروني، و التأكد من مشاركة مزودي الخدمات المعتمدين من المركز في الأنشطة ذات الصلة؛

ر. تسهيل تطبيق نظام أمن المعلومات، على ألا تكون المهام ترتبط بشكل مباشر بالمسؤوليات التالية:

- تنفيذ الضوابط التشغيلية (ضوابط تكنولوجيا المعلومات أو الأمن السيبراني)؛
- إجراء عمليات تدقيق للتحقق من مدى فعالية تنفيذ نظام أمن المعلومات؛
- اتخاذ القرارات خلال اجتماعات اللجنة التوجيهية لأمن المعلومات.

الضابط الفرعي – 1.1.6 الموظفون:

1.1.6.1 تكلف الجهة جميع الموظفين مسؤولية الالتزام بسياسات/عمليات/برنامج أمن المعلومات، و إبلاغ إداراتهم المباشرة عن أية خروقات أمنية أو حوادث مريبة؛

1.1.6.2 يوافق و يقر موظفو الجهة و الأطراف الخارجية المعنية بالمسؤوليات المتعلقة بأمن المعلومات و التزامهم باتباع سياسات الاستخدام المقبول لمعلومات الجهة و أصول المعلومات.

الضابط الفرعي – 1.1.7 رواد أمن المعلومات:

1.1.7.1 تكلف الإدارة العليا مسؤولية تنسيق أنشطة أمن المعلومات لموظفين على دراية و وعي بالمتطلبات التنظيمية لأمن المعلومات، و ذلك بصفتهم رواد أو ممثلي أو منسقي أمن المعلومات، و يتولون المهام التالية:

أ. ضمان تنفيذ الضوابط المتعلقة بنظام أمن المعلومات في الإدارة المعنية بما يتماشى مع سياسات الجهة و إجراءاتها؛

ب. مساعدة ملاك العمليات/المعلومات و مدراء المشاريع في تلبية متطلبات أمن المعلومات و تقييم المخاطر و مؤشرات الأداء الرئيسية لأمن المعلومات و الإجراءات التصحيحية المتعلقة بالتدقيق و ما إلى ذلك؛

ت. المشاركة في إيجاد حلول للحوادث المتعلقة بأمن المعلومات و المتعلقة بالإدارة؛

ث. المساعدة في تقديم توعية دورية خاصة بأمن المعلومات لموظفي الإدارة المعنية.

الضابط الفرعي – 1.1.8 التدقيق الداخلي:

تقوم الجهة الحكومية بدبي بـ

1.1.8.1 تكليف مسؤوليات التدقيق على فعالية تنفيذ نظام أمن المعلومات إلى فريق أو إدارة مستقلة أو طرف خارجي؛

1.1.8.2 التأكد من الاختيار المناسب لفريق التدقيق أو المدققين لضمان الموضوعية و الحيادية أثناء عملية التدقيق؛

1.1.8.3 الحد من الوصول إلى أدوات عملية التدقيق و سجلاتها لتجنب أي حالات سوء استخدام أو اختراق.

الضابط الرئيسي – 1.2 سياسة أمن المعلومات:

الضابط الفرعي – 1.2.1 وثيقة سياسة أمن المعلومات:

تقوم الجهة الحكومية بدبي بـ

1.2.1.1 تطوير سياسة أمن المعلومات و نشرها و متابعتها على مستوى الجهة، مبينة المبادئ الأساسية لحماية جميع أصولها المعلوماتية، و التأكد من أن كافة المستخدمين في الجهة و الأطراف الخارجية ذات الصلة ملمين بالتهديدات الأمنية المحتملة و المخاطر المرتبطة بها في أثناء العمل؛

1.2.1.2 اعتماد سياسة أمن المعلومات من قبل الإدارة العليا، و نشرها و تعميمها على الموظفين و الأطراف الخارجية ذات الصلة.

الضابط الفرعي – 1.2.2 مواءمة سياسة أمن المعلومات مع التوجه الاستراتيجي للجهة:

تقوم الجهة الحكومية بدبي بـ

1.2.2.1 مواءمة سياسة أمن المعلومات مع الاستراتيجية الشاملة للجهة بما يسهل تحقيق أهداف هذه الجهة و غاياتها، و يدعم منظومة أعمالها، مع تلافي وضع أي عراقيل في طريق تنفيذها؛

1.2.2.2 تتولى الجهة الحكومية مواءمة سياسة أمن المعلومات لديها مع المعايير و الأطر و السياسات الصادرة من قبل مركز دبي للأمن الإلكتروني، بما يضمن فعالية الأمن السيبراني و المرونة السيبرانية و مواكبة أحدث المستجدات في مجال أمن المعلومات؛

1.2.2.3 تحديد سياسات الجهة التي تشير إلى أنه لا يوجد أي مستخدم أو جهاز موثوق من داخل أو خارج شبكة الجهة، بما يضمن التحقق المستمر بالاستناد إلى عوامل عديدة بما فيها موثوقية المستخدم و سلامة الجهاز و حساسية الموارد المطلوبة (مثل تطبيق نظام الثقة المنعدمة).

الضابط الفرعي – 1.2.3 مراجعة سياسة أمن المعلومات:

تقوم الجهة الحكومية بدبي بـ:

1.2.3.1 تحديد مسؤولية واضحة لمراجعة منتظمة لسياسة أمن المعلومات و التي يتعين إجراؤها مرة واحدة في السنة على الأقل، و/أو مع أية تغييرات قد تخضع لها الجهة؛

1.2.3.2 رفع أي تحديث لسياسة أمن المعلومات أو مراجعة لها إلى اللجنة التوجيهية لأمن المعلومات و إعداد بيان بالتغييرات لتقديمه إلى المدير التنفيذي/المدير العام للجهة.

الضابط الرئيسي – 1.3 السياسات التقنية و التشغيلية:

تقوم الجهة الحكومية بدبي بـ:

1.3.1 تطوير مجموعة من سياسات أمن المعلومات التقنية/التشغيلية التي تغطي تدابير الحماية الأمنية المطلوبة و ضوابطها تبعاً لنتائج تقييم المخاطر. و تشرح هذه السياسات المسؤولية الكلية لجميع المعنيين بحماية أصول المعلومات المتعلقة بإجراءات العمل ذات الصلة، و تعمل على نشرها و تحديثها بصفة دورية؛

1.3.2 تعزيز السياسات التقنية/التشغيلية للجهة، إذا ما اقتضت الضرورة، بمجموعة من الإجراءات و الإرشادات التي تغطي تفاصيل تطبيق تلك السياسات تبعا لنتائج تقييم المخاطر؛

1.3.3 تحرص الجهة على مراجعة السياسات المتعلقة بأمن المعلومات بصفة دورية (مرة واحدة سنوياً على الأقل) لضمان مواكبتها للتطورات و قدرتها على معالجة التهديدات المحتملة لأمن المعلومات و التهديدات السيبرانية، إلى جانب تقليل المخاطر المتعلقة بأصول المعلومات.

الضابط الرئيسي – 1.4 التوعية بأمن المعلومات و التدريب عليها:

تقوم الجهة الحكومية بدبي بـ:

1.4.1. تصميم برنامج توعية بأمن المعلومات (يكون موجه لفئات محددة على أساس المهام أو الأقسام، أو وفقاً لما تراه الجهة) و تطويره و تنفيذه على مدار العام، و يتكون البرنامج من أنشطة توعية مستهدفة في مجال أمن المعلومات تتماشى مع سياسات الجهة المتعلقة بأمن المعلومات؛

1.4.2 توفير التدريب و التوعية الأساسية في مجال أمن المعلومات بصفة دورية بجميع الموظفين في الجهة، و يغطي برنامج التدريب محاور تخص أمن المعلومات، بما يتماشى مع سياسات الجهة، كجزء من التدريب الأولى للمستخدمين الجدد، و عند تطبيق التغييرات في نظم المعلومات، و بصفة دورية وفقاً لاحتياجات الجهة؛

1.4.3 توفير تدريبات أمن المعلومات بصورة دورية و مناسبة للموظفين المشاركين في تشغيل برنامج/إدارة أمن المعلومات في مجالات العمل التي يتبعون لها؛

1.4.4 تصميم و صيانة مواد التوعية المتعلقة بأمن المعلومات و التي تعمل على تثقيف المستخدمين على سياسات أمن المعلومات و تغطي المخاطر الأمنية لإجراءات عمل الجهة و تركز على الحد من مخاطر الأعمال المحتملة؛

1.4.5 إجراء إستطلاعات دورية للتوعية الأمنية لقياس فعالية التدريب الأمني و مستوى الوعي لدى جميع موظفي الجهة و الأطراف الخارجية ذات الصلة، سعياً للحد من الأخطاء الشائعة أو حالات سوء الفهم في مفاهيم أمن المعلومات، و لتحسين برنامج التوعية الشاملة؛

1.4.6 توثيق سجلات الحضور لجميع الموظفين في برامج التوعية و التدريب في أمن المعلومات؛

1.4.7 تحديد الطرق أو التقنيات المناسبة للتدريب مثل القاعات الدراسية أو عبر الإنترنت أو عن طريق برنامج، بناءً على متطلبات الجهة المحددة؛

1.4.8 تستخدم الجهة موقعها الإلكتروني أو منصاتها العامة و برامجها و مبادراتها لنشر الوعي بالأمن السيبراني بين مجتمعها و الأطراف الخارجية.

الضابط الرئيسي – 1.5 إتفاقية المحافظة على السرية:

تقوم الجهة الحكومية بدبي بـ:

1.5.1 تطوير إتفاقية عدم الإفصاح و المحافظة على السرية، و التي يتم توقيعها من قبل جميع الموظفين أو الأطراف الخارجية، و إجراء مراجعة منتظمة لها. و تغطي الإتفاقية متطلبات الجهة لحماية معلوماتها من التسريب داخلياً أو خارجياً، و ذلك باستخدام مصطلحات قانونية قابلة للتطبيق، مع التأكيد على مفهوم «ضرورة الإطلاع»؛

1.5.2 تثقيف الموظفين و توعيتهم بسرية المعلومات الحكومية، و إيضاح كيف يمكن أن يؤثر تسريب المعلومات، كتابةً أو شفاهةً، في أداء الجهة.

الضابط الرئيسي – 1.6 علاقات الإتصال و استدامة أمن المعلومات:

تقوم الجهة الحكومية بدبي بـ

1.6.1 المحافظة على قنوات الاتصال المناسبة مع السلطات الرسمية ذات الصلة في مجال أمن المعلومات؛

1.6.2 تحديد قنوات الاتصال الرئيسية مع الجهات الأمنية و القضائية لغرض الاتصال بها في حالات حوادث أمن المعلومات و الانتهاكات ... و غيرها؛

1.6.3 المحافظة على قنوات الاتصال و/أو العضويات مع المجموعات ذات الاهتمام الخاص: المنتديات أو الجمعيات المهنية المتخصصة بأمن المعلومات؛ و ذلك من أجل مواكبة أحدث المستجدات في مجال أمن المعلومات.

الضابط الرئيسي – 1.7 ضمان علاقات آمنة مع الأطراف الخارجية:

تقوم الجهة الحكومية بدبي بـ

1.7.1 تحديد و تقييم المخاطر المتعلقة بالحوكمة و أمن المعلومات المتعلقة بعلاقاتها الخارجية كالعملاء و مزودي الخدمات و الاستشاريين، و متعاقدي التوظيف الخارجي، و مزودي الخدمات الحاسوبية السحابية ... إلخ، و تقييم مستواها؛

1.7.2 إختيار ضوابط و اجراءات أمن المعلومات المناسبة للسيطرة على المخاطر التي جرى تحديدها، وتطبيقها؛

1.7.3 وضع الاتفاقيات/العقود اللازمة لضمان أمن العلاقات مع الأطراف الخارجية، وتنفيذها؛ بما يتضمن الالتزام بمتطلبات أمن المعلومات والتي تغطي سرية المعلومات و مصداقيتها وتوافرها.

المجال 2
إدارة المعلومات والأصول المتعلقة بها

المجال 2
إدارة المعلومات والأصول المتعلقة بها

الهدف

تحديد أصول المعلومات وتصنيفها، وتحديد التدابير الملائمة لحفظها وتداولها السليم، وكذلك الاجراءات الآمنة لإتلافها والتخلص منها، بغرض حماية الجهة من الالتزامات القانونية ومن فقدان المعلومات ومن الاعتداءات ... وغيرها.

ضوابط إدارة المعلومات والأصول المتعلقة بها

الضابط الرئيسي – 2.1 إدارة أصول المعلومات:

تقوم الجهة الحكومية بدبي بـ:

2.1.1 تطوير ونشر والمحافظة على سياسة وإجراءات إدارة أصول المعلومات لدى الجهة أو عمل إطار لتحديد أصول المعلومات وإدارتها وحمايتها بما يتماشى مع القوانين واللوائح المعمول بها؛

2.1.2 تطوير سجل لجميع أصول المعلومات لدى الجهة وتوثيقه والحفاظ عليه بحيث يشمل أصول المعلومات الهامة والبيانات وما يتعلق بها من مرافق ومكونات لمعالجتها، مثل أصول البرمجيات، والموارد البشرية والأصول

الفعلية وغيرها، مع الأخذ بعين الاعتبار التفاصيل الأخرى، مثل تصنيف المعلومات والموقع الفعلي والتراخيص والقيمة العلمية، وغيرها من المعلومات الضرورية التي قد تبرز الحاجة إليها للحد من المخاطر والتعافي من الكوارث؛

2.1.3 مراجعة سجل أصول المعلومات على فترات منتظمة وتحديثه بصفة دورية.

الضابط الرئيسي – 2.2 ملكية أصول المعلومات وعهدتها:

تقوم الجهة الحكومية بدبي بـ:

2.2.1 وضع سياسة ملكية المعلومات وتطبيقها، بحيث يتم تعريف أصول المعلومات وربطها بمالك وأمين عهدة بعينه. تعد الإجراءات ذات الصلة بالعمل والخدمات والتطبيقات وأنظمة المعلومات أو مجموعة البيانات أمثلة على الأصول التي ينبغي تحديد ملكيتها و عهدتها؛

2.2.2 تحميل مالك أصول المعلومات مسؤولية التأكد من تصنيف المعلومات بالشكل السليم؛ تبعاً لحساسيتها؛

2.2.3 تحميل مالك أصول المعلومات مسؤولية تحديد القيود المفروضة على الدخول للمعلومات والتأكد من مراجعتها بصفة دورية تبعاً لمستوى تصنيفها، مع مراعة سياسة التحكم بالدخول المعمول بها في الجهة؛

2.2.4 تحميل أمين العهدة مسؤولية المحافظة على المهام التشغيلية اليومية المرتبطة بأصول المعلومات، مع الأخذ بعين الاعتبار السلطة الأعلى لمالك أصول المعلومات.

الضابط الرئيسي – 2.3 تصنيف أصول المعلومات:

تقوم الجهة الحكومية بدبي بـ:

2.3.1 وضع مخطط/إجراء لتصنيف المعلومات لدى الجهة وتطبيقه، وذلك استناداً إلى أهمية أصول المعلومات وقيمتها والمتطلبات القانونية ومتطلبات الحماية ... وغيرها، بما يتماشى مع القوانين واللوائح المعمول بها (نظام أمن المعلومات، الضابط 11.1 و 11.2)؛

2.3.2 تطوير سياسة تصنيف المعلومات والإجراءات ذات العلاقة، ونشرها و تحديثها بصفة دورية، بما يتماشى مع القوانين واللوائح المعمول بها (نظام أمن المعلومات، الضابط 11.1 و 11.2).

الضابط الرئيسي – 2.4 وضع المسميات لأصول المعلومات وتداولها:

تقوم الجهة الحكومية بدبي بـ:

2.4.1 وضع الضوابط الملائمة لوضع المسميات وتداول أصول المعلومات (الإلكترونية والفعلية)، وتنفيذها، تبعاً لمستوى التصنيف المحدد لها، مع الأخذ بعين الاعتبار متطلبات التداول وإجراءات الحفظ وحدود النشر ... وغيرها، لكل من هذه الأصول؛

2.4.2 تطوير إجراء لوضع مسميات أصول المعلومات ومتطلبات تداولها، ونشر هذا الإجراء وتحديثه بصفة دورية.

الضابط الرئيسي – 2.5 التخلص من المعلومات وأصول المعلومات:

تقوم الجهة الحكومية بدبي بـ:

2.5.1 تحديد تدابير الأمن والسلامة المطلوبة قبل التخلص من المعلومات أو أصولها، وتنفيذها، حسب قيمتها وأهميتها وحساسيتها؛

2.5.2 تطوير إجراء واضح لعملية التخلص من المعلومات وأصولها، ونشره وتحديثه بصفة دورية، كجزء من إجراءات وضع المسميات والتداول؛

2.5.3 حفظ سجلات المعلومات الحساسة والمصنفة التي تم إتلافها والتخلص منها، بما يتوافق مع نظام تصنيف المعلومات.

الضابط الرئيسي – 2.6 مسؤولية أصول المعلومات:

تقوم الجهة الحكومية بدبي بـ:

2.6.1 وضع سياسة الاستخدام المقبول التي تحكم استخدام المعلومات وأصولها، وكذلك توزيعها وتحديثها بصفة دورية، بما في ذلك استخدام الأجهزة الشخصية في محيط الجهة.

الضابط الرئيسي – 2.7 حماية المعلومات/البيانات:

تقوم الجهة الحكومية بدبي بـ:

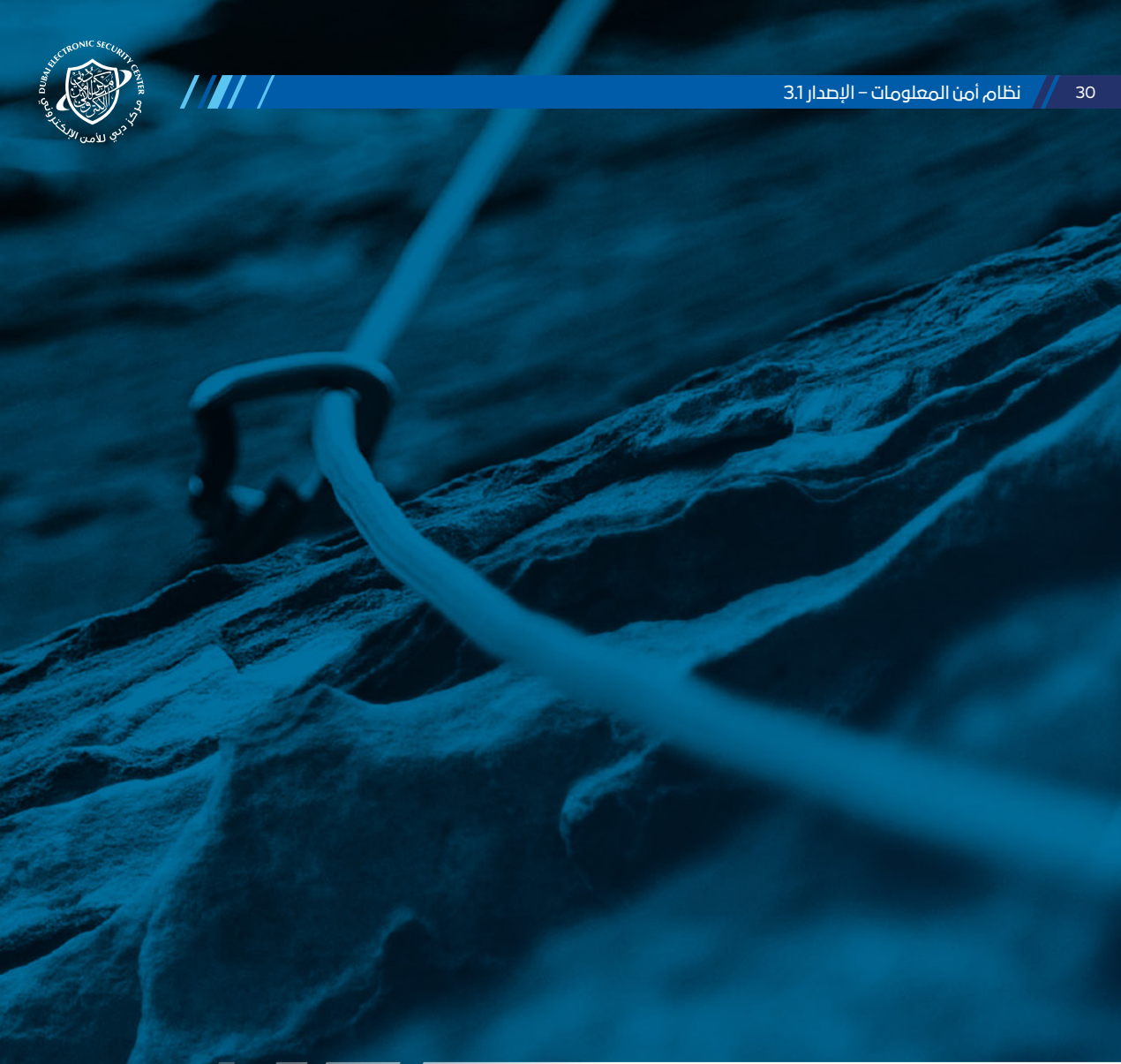
2.7.1 وضع إجراء لتحديد مخاطر الوصول إلى المعلومات أو البيانات الحساسة/المصنفة (البيانات غير المفتوحة و غير العامة) وفقاً لمتطلبات الامتثال المحددة للحماية والخصوصية، بما يتماشى مع القوانين واللوائح المعمول بها، مثل قانون بيانات دبي؛

2.7.2 ضمان عدم معالجة المعلومات أو البيانات الحساسة/المصنفة (البيانات غير المفتوحة و غير العامة) للجهة أو تخزينها أو مشاركتها خارج حدود دولة الإمارات العربية المتحدة إلا بعد اتخاذ تدابير الحماية والحصول على موافقة مسبقة من قبل الإدارة؛

2.7.3 وضع إجراء لإخفاء البيانات وتطبيق تقنيات البيانات الاصطناعية بما يتماشى مع سياسات الجهة ومتطلبات العمل والقوانين واللوائح المعمول بها؛

2.7.4 تطبيق تقنيات البيانات الاصطناعية المناسبة وإخفاء البيانات بناءً على نتائج تقييم المخاطر، حيث تشارك الجهة بياناتها الحساسة مع الأطراف الخارجية لأسباب تتعلق بمصالح العمل؛

2.7.5 تطبيق ضوابط مناسبة لحماية خصوصية البيانات عند تطبيق حلول تقنية متقدمة وأنظمة استجابة ذاتية، على سبيل المثال برنامج الدردشة شات جي بي تي ومنصات الذكاء الاصطناعي والاستجابة الصوتية التفاعلية، بما يتماشى مع تصنيف بيانات الجهة ونتائج تقييم المخاطر.



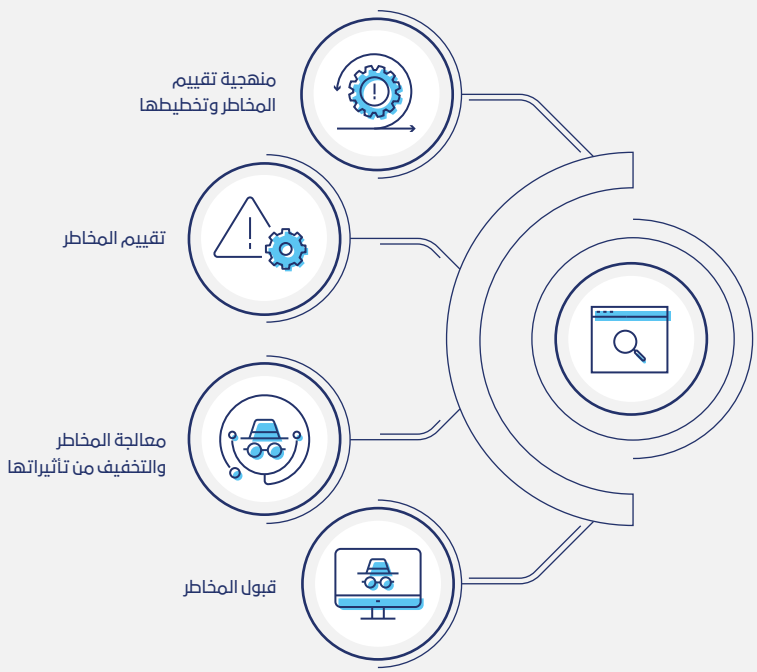
المجال 3
إدارة المخاطر

المجال 3
إدارة المخاطر

الهدف

تحديد المخاطر المرتبطة بالمعلومات وأصولها الحيوية ومعالجتها من خلال دراسة مفصلة لإجراءات العمل وتحديد التهديدات ونقاط الضعف ومن ثم تطبيق الخطط والضوابط المناسبة اللازمة.

ضوابط إدارة المخاطر



الضابط الرئيسي – 3.1 منهجية تقييم المخاطر وتخطيطها:

تقوم الجهة الحكومية بدبي بـ:

3.1.1 تطوير منهجية لتقييم المخاطر تتواءم مع متطلبات برنامج/إدارة أمن المعلومات لدى الجهة؛

3.1.2 وضع خطة دورية لإجراء تقييم المخاطر لدى الجهة ككل؛

3.1.3 وضع معايير للمخاطر المقبولة، كجزء من منهجية تقييم المخاطر؛

3.1.4 تحديد نطاق تقييم المخاطر ليشمل أصحاب المصلحة الرئيسيين بما في ذلك الأطراف الخارجية، فيما يتعلق بإجراءات العمل وأصول المعلومات الخاصة بها والتي سيتم تضمينها في التقييم؛

3.1.5 ضمان جمع بيانات التهديدات ونقاط الضعف المتعلقة بالمعلومات ونظم المعلومات، وتحليلها في إطار عملية تقييم مخاطر أمن المعلومات؛

3.1.6 تحديد وجمع وتحليل المعلومات الحساسة المتعلقة بالتهديدات في الجهة والأصول المتعلقة بها في إطار عملية جمع المعلومات الخاصة بالتهديدات؛

3.1.7 تطبيق خطط دورية لزيادة الوعي حول برنامج تقييم المخاطر بين كافة أقسام الجهة.

الضابط الرئيسي – 3.2 تقييم المخاطر:

تقوم الجهة الحكومية بدبي بـ

3.2.1 إجراء والحفاظ على تقييم مفصل للمخاطر وفقا لمنهجية تقييم المخاطر المعتمدة؛

3.2.2 تحليل المخاطر وترتيبها وفق الأولوية؛ قياساً لمدى خطورتها؛ من أجل وضع الخطط والضوابط لمعالجتها؛

3.2.3 تحديد المخاطر المقبولة تماشياً مع منهجية تقييم المخاطر التي تم وضعها؛

3.2.4 توثيق نتائج تقييم المخاطر و اعتماد المخاطر العالية رسمياً من قبل اللجنة التوجيهية لأمن المعلومات أو الإدارة العليا.

الضابط الرئيسي – 3.3 معالجة المخاطر والتخفيف من تأثيراتها:

تقوم الجهة الحكومية بدبي بـ

3.3.1 تحديد الخطط المناسبة لمعالجة المخاطر (التخفيف من الأثر – التجنب – التحويل ... وغيرها) التي تم تحديدها؛

3.3.2 تحديد واختيار الضوابط الأمنية التشغيلية المناسبة) موضحة تحت المجالات التشغيلية في هذه الوثيقة (للتخفيف من تأثيرات المخاطر المحددة؛

3.3.3 اعتماد الضوابط الأمنية التشغيلية المناسبة من قبل اللجنة التوجيهية لأمن المعلومات لإدارة المخاطر العالية؛

3.3.4 تطبيق ضوابط تخفيف تأثيرات المخاطر من قبل مالك الخطر؛

3.3.5 مراجعة الضوابط التي جرى تطبيقها لتخفيف تأثيرات المخاطر ومراقبة فعاليتها.

الضابط الرئيسي – 3.4 قبول المخاطر:

تقوم الجهة الحكومية بدبي بـ

3.4.1 توثيق المخاطر العالية أو المتبقية وغير المُعالجة، مع إيضاح مبررات عدم معالجتها، واعتمادها من اللجنة التوجيهية لأمن المعلومات/الإدارة العليا، وتوضيح خطة تفصيلية لمعالجة هذه المخاطر في وقت لاحق.

المجال 4
إدارة الحوادث والمشاكل

المجال 4
إدارة الحوادث والمشاكل

الهدف

وضع الإجراء العملي المناسب لتحديد حوادث أمن المعلومات والتعامل معها بفاعلية؛ بهدف الحد من آثارها السلبية في سير العمل لدى الجهة.

ضوابط إدارة الحوادث والمشاكل

الضابط الرئيسي – 4.1 تخطيط إدارة الحوادث:

تقوم الجهة الحكومية بدبي بـ

4.1.1 تطوير السياسة والإجراءات الرسمية لإدارة حوادث أمن المعلومات ونشرها وتحديثها بصفة دورية، بما في ذلك رفع التقارير عن الحوادث شديدة الخطورة إلى مركز دبي للأمن الإلكتروني والهيئات الخارجية الأخرى؛

4.1.2 وضع الآليات والتدابير المناسبة للاستجابة لحوادث أمن المعلومات في الجهة، وتشكيل فريق مؤهل ومعتمد لاستجابة الحوادث لدى الجهة، ويتبع المهام التالية:

أ. يتمتع بالمعرفة حول حوادث أمن المعلومات وإجراءاتها؛

ب. وضع خطة لإدارة الحوادث وتحديد الإجراءات المتعلقة بها؛

ت. الاستجابة للحوادث وإجراء التحقيقات المناسبة وتحديد مسبباتها الأساسية؛

ث. إبلاغ أصحاب المصلحة المعنيين بخطة العمل والتواصل معهم بشأن الإجراءات اللازمة؛

ج. الحفاظ على الأدلة المتعلقة بالحوادث؛

ح. تحديد وتسجيل الدروس المستفادة ومتطلبات تطوير عملية الاستجابة.

4.1.3 تحديد وتقديم ما يلزم من تدريبات ودورات توعوية دورية وشهادات معتمدة لفريق الاستجابة للحوادث لدى الجهة، وذلك من أجل التطوير المستمر حتى يتم التعامل مع حوادث أمن المعلومات بشكل فعال؛

4.1.4 تحديد الإجراءات اللازمة لإدارة الحوادث وتنفيذها وفق ما يلي:

أ. تقييم حوادث أمن المعلومات وترتيبها وفق الأولوية؛ قياساً لمدى خطورتها؛

ب. تكليف فريق مؤهل/معتمد من قبل مركز دبي للأمن الإلكتروني للاستجابة للحوادث في حال مشاركة جهات خارجية في التعامل مع الحوادث ؛

ت. إبلاغ مركز دبي للأمن الإلكتروني عن الحوادث ذات الخطورة العالية لإجراء التحقيقات الإضافية.

4.1.5 تطوير إجراءات عملية الاختبار اللازمة وتطبيقها للتحقق من فعالية عملية الاستجابة للحوادث وكفاءتها حيثما ينطبق ذلك، وتحديد ضوابط إضافية لتجنب وقوع حوادث مماثلة في المستقبل.

الضابط الرئيسي – 4.2 الإبلاغ عن حوادث أمن المعلومات والإجراءات التصعيدية:

تقوم الجهة الحكومية بدبي بـ:

4.2.1 تكليف جميع الموظفين وأي مستخدمين يتعاملون مع معلومات الجهة بأي وسيلة، مسؤولية إبلاغ الفريق المسؤول لدى الجهة بأسرع وقت ممكن عن أية حوادث لأمن المعلومات ونقاط الضعف الأمنية في الأنظمة أو الخدمات، سواء كانت ملحوظة أو في حالة الاشتباه بها؛

4.2.2 تطبيق إجراء تصعيدي خاص بحوادث أمن المعلومات التي يتم تصنيفها على أنها ذات خطورة عالية، كما تحدد السلطات الخارجية التي قد تسهم في إجراء التحقيقات الإضافية لهذه الحوادث إذا ما دعت الحالة إلى ذلك.

الضابط الرئيسي – 4.3 جمع الأدلة:

تقوم الجهة الحكومية بدبي بـ

4.3.1 تطبيق إجراءات لتحديد كافة الأدلة المتعلقة بحوادث أمن المعلومات وجمعها والحفاظ عليها.

الضابط الرئيسي – 4.4 قاعدة معرفية لحوادث أمن المعلومات:

تقوم الجهة الحكومية بدبي بـ

4.4.1 إنشاء قاعدة معرفية لجميع حوادث أمن المعلومات تحتوي على معلومات عن الحوادث السابقة وأنواعها وتكاليفها، وأي معلومات أخرى مناسبة؛

4.4.2 إنشاء قاعدة معرفية مركزية لجمع البيانات المتعلقة بحوادث أمن المعلومات واتجاهات الهجمات والتهديدات الجديدة ونقاط الضعف، وذلك من مصادر خارجية متعددة مثل تقارير الموردين والجهات الحكومية والتنبيهات الأمنية وغيرها، وتحليلها من أجل تحديد التدابير الوقائية.

4.5 إدارة المشكلات:

4.5.1 تتولى الجهة تحديد إجراءات إدارة المشكلات وتطبيقها، مع مراعاة ما يلي:

أ. رصد المشكلة؛

ب. تصنيف المشكلة وتحديد مدى أولويتها؛

ت. تشخيص المشكلة وإجراء التحقيقات اللازمة؛

ث. معالجة المشكلة؛

ج. تحديد الدروس المستفادة وتحسين عملية إدارة المشكلات.

المجال 5
ضبط الدخول

المجال 5
ضبط الدخول

الهدف

تأمين الدخول الافتراضي والفعلي لمعلومات وموارد ومرافق معالجة المعلومات الخاصة بالجهة وحمايتها طوال دورة حياتها.

أهداف ضبط الدخول

الضابط الرئيسي – 5.1 سياسة/إجراء إدارة ضبط الدخول:

تقوم الجهة الحكومية بدبي بـ:

5.1.1 تطوير سياسة ضبط الدخول التي تعالج جميع المتطلبات الأمنية اللازمة لتطبيقها بشكل فعال داخل الجهة، وتوزيعها وتحديثها بصفة دورية، بما في ذلك ضبط دخول الجهات الخارجية ومنحها إمكانية الدخول إلى

الموارد التي تعتبر ضرورية للغاية لأي مستخدم أو جهاز يعمل بأدنى حد من إمكانية الدخول، وذلك وفق منهجية الثقة المعدومة؛

5.1.2 تطوير إجراء لضبط الدخول يحدد الخطوات والإجراءات التفصيلية الواجب إتباعها لضبطه، تبعاً لمفهوم ضبط الدخول القائم على الأدوار؛

5.1.3 بناء قاعدة بيانات آمنة لجميع امتيازات دخول أنظمة المعلومات.

الضابط الرئيسي – 5.2 ضبط الدخول الافتراضي:

الضابط الفرعي – 5.2.1 ضبط دخول المستخدمين:

تقوم الجهة الحكومية بدبي بـ:

5.2.1.1 وضع إجراء عملي وتطبيقه: لتسجيل/إلغاء تسجيل المستخدمين، والتعديل أو تجميد أو سحب امتيازات دخول المستخدمين؛

5.2.1.2 تزويد كل مستخدم بمعرف مميز (هوية مستخدم) لاستخدامات العمل الفردية فقط؛

5.2.1.3 تطبيق معيار موحد لإنشاء معرفات المستخدمين على نطاق الجهة؛

5.2.1.4 تطبيق تقنية مناسبة للتحقق من هويات المستخدمين خلال عملية الدخول سواء كان في الموقع ذاته أو عن بعد؛

5.2.1.5 تطوير سياسة التحقق من هويات المستخدمين (مثل: إدارة كلمات السر التي تتناول بوضوح إجراء إنشاء وإسناد كلمات السر ومسؤوليتهم تجاه استخدامها والأسلوب الموصي به لهيكلتها، وغيره) ونشر هذه السياسة وتحديثها بصفة دورية؛

5.2.1.6 تحديد فئات المستخدمين الذين يحتاجون إلى امتيازات خاصة (بشكل دائم)، والتأكد من توافر ما يأتي:

أ. تفويض دخول موافق عليه وساري المفعول؛

ب. ضرورة وحاجة استخدام النظام؛

ت. سمات أخرى تتفق مع ما هو مطلوب من قبل الجهة أو مع مهام/وظائف الأعمال؛

ث. يقتصر استخدام حسابات الدخول ذات الامتيازات الخاصة على الأغراض التي أنشأت من أجلها.

5.2.1.7 حفظ سجلات جميع امتيازات الدخول للمستخدمين من الجهة والجهات الخارجية، ومراقبتها بشكل مستمر؛

5.2.1.8 الحد من عدد معرفات المستخدمين ذوي الامتيازات الخاصة أو العالية لتمنح للأفراد ذوي الحاجة الفعلية إلى مثل هذه الامتيازات، على أن تكون معتمدة على أساس أهداف العمل؛

5.2.1.9 تطبيق ضوابط الأمن والمراقبة المستقلة على استخدام ذوي المعرفات الخاصة أو الامتيازات العالية؛

5.2.1.10 وضع الإجراءات المناسبة لطلبات الحسابات المؤقتة وحساب الزوار وتطبيق الإلغاء التلقائي لهذه الحسابات؛

5.2.1.11 تخصيص امتيازات الدخول بناءً على معايير تحددها ضوابط الحد الأدنى من صلاحيات الدخول والفصل في المهام ومنح تصاريح دخول مشددة للمستخدمين – وليس بناءً على الثقة المفترضة (أي تطبيق منهجية الثقة المعدومة)؛

5.2.1.12 تطبيق إجراء لمراجعة صلاحيات دخول المستخدمين والأطراف الخارجية وإعادة اعتمادها بصفة دورية تبعاً لما تحدده الجهة.

الضابط الفرعي – 5.2.2 ضبط الدخول إلى الشبكة:

تقوم الجهة الحكومية بدبي بـ

5.2.2.1 تطوير سياسة ضبط الدخول إلى الشبكة بحيث تشمل تفاصيل الشبكات وأجهزتها التي يمكن الوصول إليها، وعملية التفويض الرسمية لمنح حق الوصول إلى الشبكة، وما إلى ذلك؛

5.2.2.2 وضع إجراء عملي لتفويض/تفعيل أو إنهاء أي روابط اتصال للشبكات لدى الجهة؛

5.2.2.3 تطبيق الأداة/الوسيلة المناسبة لضبط الدخول إلى الشبكة من أجل الكشف عن، والتعرف إلى، والتحقق من، أي معدات أو أجهزة تتصل بالشبكات؛

5.2.2.4 إدارة الدخول إلى منافذ التهيئة (Configuration Posts) الخاصة بمعدات/أجهزة الشبكات وضبطها؛

5.2.2.5 تطبيق ضوابط الفصل المناسبة على جميع أنواع الشبكات لدى الجهة (الداخلية،الخارجية، اللاسلكية، الاتصال الهاتفي الرقمي؛ عبر بروتوكول الإنترنت ... وما إلى ذلك)؛

5.2.2.6 تطبيق الضوابط الأمنية والتشغيلية المناسبة لأي اتصالات بشبكات خارجة عن نطاق التحكم المباشر للجهة.

الضابط الفرعي – 5.2.3 ضبط الدخول إلى أنظمة التشغيل:

تقوم الجهة الحكومية بدبي بـ

5.2.3.1 إدارة أنظمة التشغيل والتحكم بالدخول إليها من خلال إجراء آمن للدخول؛

5.2.3.2 تزويد كل مستخدم بمعرف مميز (هوية مستخدم) وتطبيق آلية مناسبة للتحقق من الهوية؛

5.2.3.3 الحد من استخدام معرفات الهوية العامة وحصرها للظروف الاستثنائية التي تكون مبررة عملياً، مع تطبيق آلية المساءلة المناسبة لمثل هذا الاستخدام؛

5.2.3.4 وضع نظام للتحقق من هوية المستخدمين على مستوى الجهة يتم من خلاله فرض ضوابط للتحقق؛

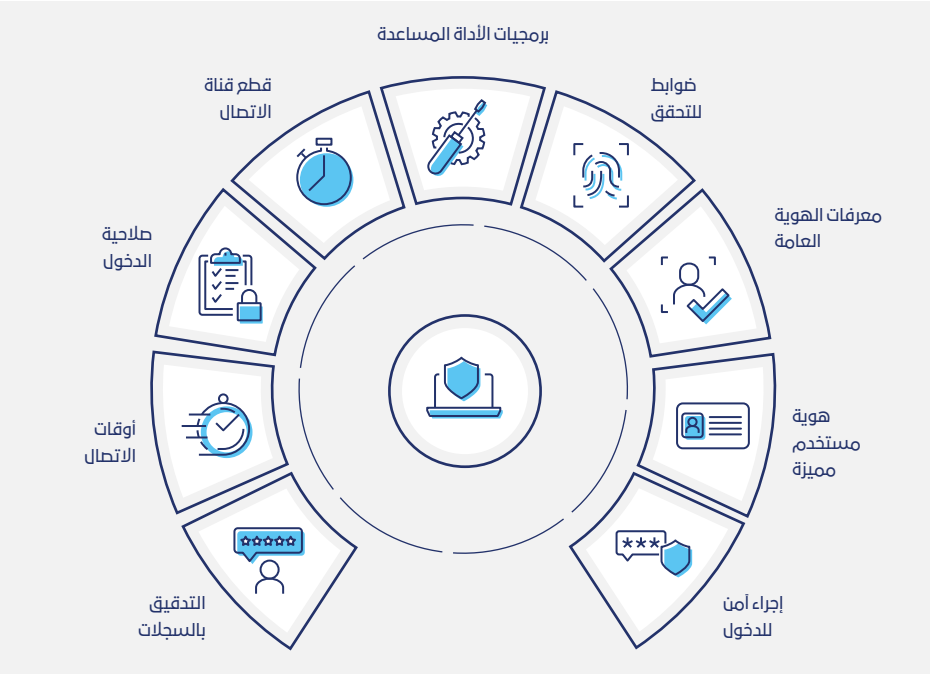
5.2.3.5 إدارة استخدام برمجيات الأداة المساعدة، وضبطه؛

5.2.3.6 تطبيق خاصية قطع قناة الاتصال بعد فترة من عدم النشاط منعاً للدخول غير المصرح به؛

5.2.3.7 تطبيق خاصية تعليق صلاحية الدخول؛

5.2.3.8 تقييد أوقات الاتصال لأنظمة المعلومات والتطبيقات الحساسة؛

5.2.3.9 حفظ سجلات التدقيق الخاصة بمعرفات إداريي الأنظمة ومحاولات دخولهم، ومراجعتها باستمرار.



الضابط الفرعي – 5.2.4 ضبط الدخول إلى التطبيقات:

تقوم الجهة الحكومية بدبي بـ:

5.2.4.1 توفير الدخول إلى التطبيقات بناءً على مسؤوليات الوظيفة والمبررات العملية بما يتوافق مع سياسة/إجراء التحكم بالدخول المتبع لدى الجهة؛

5.2.4.2 وضع ضوابط فعلية و/أو افتراضية لعزل بيئات أنظمة المعلومات و التطبيقات الحساسة للغاية.

الضابط الفرعي – 5.2.5 أمن الدخول عن بعد:

تقوم الجهة الحكومية بدبي بـ:

5.2.5.1 تطوير سياسة تعالج مسائل الدخول عن بعد إلى موارد الجهة ونشرها وتحديثها بشكل دوري، و التأكد من تطبيق ضوابط أمنية كافية بناءً على نتائج تقييم المخاطر لضمان حماية معلومات/بيانات الجهة من المستخدمين العاملين عن بُعد؛

5.2.5.2 تعزيز سياسة العمل عن بعد بإجراء يعالج متطلبات الاتصال عن بعد (مثل الشبكات الافتراضية الخاصة)، واستخدام الأجهزة الشخصية والاتصالات الآمنة ومسؤوليات المستخدم؛

5.2.5.3 فرض اعتماد رسمي و مصادقة مناسبة بشكل مسبق على اتصالات الدخول عن بعد؛

5.2.5.4 التأكد من تطبيق ضوابط أمنية كافية على أجهزة مستخدمي الشبكات الافتراضية الخاصة، مثل التحقق من الهوية والتشفير وبرمجيات مكافحة الفيروسات و جدار الحماية الأمني و مهلة إنهاء الاتصال وتصنيف المحتوى وغيرها؛

5.2.5.5 تزويد مستخدمي الدخول عن بعد بإمكانية الدخول إلى الخدمات المخولة للمستخدمين على وجه التحديد؛

5.2.5.6 مراقبة سجلات التدقيق الخاصة باتصالات دخول المستخدمين عن بعد وسجلات أنشطتهم ومراجعتها.

الضابط الفرعي – 5.2.6 الحوسبة المتحركة:

تقوم الجهة الحكومية بدبي بـ:

5.2.6.1 تطوير سياسة رسمية تحكم الاستخدام الملائم للحوسبة المتحركة ومرافق الاتصالات، ونشرها وتحديثها بصفة دورية؛

5.2.6.2 تطبيق التدابير الأمنية المناسبة للحماية من مخاطر استخدام الحوسبة المتحركة ومرافق الاتصالات، مثل:

أ. تطبيق أداة تشفير لحماية المعلومات الحساسة؛

ب. ضمان الاستخدام الآمن للأجهزة الحاسوبية المحمولة؛

ت. تطبيق الأدوات اللازمة لتعطيل أو مسح بيانات الأجهزة الحاسوبية المحمولة في حال فقدانها أو سرقتها؛

ث. وضع الإجراءات المناسبة للنسخ الاحتياطي لبيانات الأجهزة الحاسوبية المحمولة؛

ج. الحد أو تقييد استخدام الأجهزة الحاسوبية المحمولة للمستخدمين المرخص لهم مع وضع ضوابط أمنية كافية.

5.2.6.3 تطوير ونشر والحفاظ على سياسة وإجراءات للتعامل مع واستخدام الأجهزة الشخصية (إحضار الجهاز الخاص بك) والتي ليست مملوكة للجهة، وتطبيق المتطلبات الأمنية للجهة في التعامل مع أجهزة الحاسوب المحمولة المفقودة أو المسروقة، وتخزين بيانات الجهة على هذه الأجهزة، والاتصال بشبكة الجهة وأنظمتها، الخ؛

الضابط الفرعي – 5.2.7 إدارة الدخول اللاسلكي:

تقوم الجهة الحكومية بدبي بـ

5.2.7.1 تطوير سياسة رسمية لاستخدام الشبكة اللاسلكية ونشر هذه السياسة وتحديثها بصفة دورية؛

5.2.7.2 فرض تفويض رسمي مسبق للوصول اللاسلكي عبر الشبكة قبل إجراء أي اتصال؛

5.2.7.3 تطبيق ضوابط التحقق من الهوية المناسبة للدخول اللاسلكي؛

5.2.7.4 فرض الضوابط الأمنية المناسبة للدخول اللاسلكي على شبكة الجهة، ووضع قيود على هذا الاستخدام وإرشادات لتنفيذه؛

5.2.7.5 تزويد مستخدمي الاتصال اللاسلكي بصلاحية الدخول إلى الخدمات التي تم التصريح لهم باستخدامها على وجه التحديد؛

5.2.7.6 المراقبة المستمرة للدخول اللاسلكي غير المصرح به إلى الشبكة.

الضابط الرئيسي – 5.3 التحكم بالدخول الفعلي:

الضابط الفرعي – 5.3.1 سياسة الدخول الفعلي و إجراءاته:

تقوم الجهة الحكومية بدبي بـ

5.3.1.1 تطوير سياسة دخول فعلي رسمية وموثقة تعالج متطلبات الجهة لتنفيذ ضوابط الدخول الفعلي على المكاتب والغرف وغيرها من الأماكن ونشرها وتحديثها بصفة دورية؛

5.3.1.2 تعزيز سياسة الدخول الفعلي، عند الضرورة، بإجراء مفصل لكيفية تنفيذ ضوابط الحماية وتزويد المستخدمين بالوصف الكامل لعناصر الحماية على صعيد الأمن الفعلي؛

5.3.1.3 فرض تفويض رسمي مسبق للدخول الفعلي لأي من المرافق التي تحتوي موارد معالجة المعلومات.

الضابط الفرعي – 5.3.2 ضوابط الأمن الفعلي:

تقوم الجهة الحكومية بدبي بـ

5.3.2.1 فرض الحدود المناسبة للتحكم بالدخول الفعلي لدى جميع منافذ الدخول الفعلي للجهة؛

5.3.2.2 التحقق من المناطق المحمية وضمان الدخول إليها، فقط للموظفين المصرح لهم بذلك؛

5.3.2.3 ضبط الدخول إلى مرافق معالجة المعلومات والمناطق العامة ومراقبتها؛

5.3.2.4 حماية وسائل الدخول الفعلي، وفرض الضوابط الملائمة لحمايتها؛

5.3.2.5 حفظ قائمة جرد الموجودات لتشمل كافة أجهزة الدخول الفعلي التي تملكها الجهة؛

5.3.2.6 مراجعة سجلات الدخول الفعلي بشكل منتظم؛

5.3.2.7 تطبيق آلية لرصد تحركات الموظفين وغير الموظفين داخل الجهة.

الضابط الرئيسي – 5.4 ضبط الدخول العام و دخول الأطراف الخارجية:

تقوم الجهة الحكومية بدبي بـ

5.4.1 فرض التفويض الرسمي المسبق للدخول الافتراضي والفعلي المطلوب من قبل الأطراف الخارجية عبر تطبيق معايير «ضرورة الاطلاع»؛

5.4.2 مراقبة الدخول الافتراضي والفعلي المتاح للعامة وللأطراف الخارجية، وتسجيله؛

5.4.3 ضبط الدخول الفعلي إلى أي مناطق تضم نظم معلومات، وغيرها من المناطق مثل التوريد أو التحميل أو أي نقاط أخرى يجوز للعاملين غير المفوضين الدخول إليها، من خلال التحقق من هويات الزوار قبل السماح لهم بالدخول؛

5.4.4 منح التفويض، ومراقبة الدخول إلى/والخروج من مرافق مركز البيانات وضبطهما، والاحتفاظ بسجلات تلك المجريات؛

5.4.5 تطبيق آليات حماية وضبط الدخول الفعلي على الغير أو الأفراد الخارجيين الذين تتم الاستعانة بخدماتهم، وتحميلهم مسؤولية أي انتهاك أو مساس بسياسة أمن المعلومات الخاصة بالجهة.

الضابط الرئيسي – 5.5 التحكم بالوصول إلى المعلومات والوثائق:

تقوم الجهة الحكومية بدبي بـ

5.5.1 وضع ضوابط أمنية كافية للتعامل مع جميع الوثائق و السجلات الإلكترونية/ الورقية الحساسة لحمايتها من الضياع أو سوء الاستخدام أو التعديل غير المصرح به؛

5.5.2 تحديد الحقوق اللازمة للوصول إلى الوثائق/المعلومات المحمية؛

5.5.3 وضع سياسة واضحة بشأن التحكم بالوثائق، بالترافق مع تحديد واضح لمدة الأرشفة، وتعزيزها بالإجراءات والإرشادات المفصلة حول التنفيذ والاستخدام؛

5.5.4 إعتماد إجراء للتخلص من الوثائق، مع متطلبات التفويضات والمسؤوليات.

الضابط الرئيسي – 5.6 تدقيق ضبط الدخول ومراجعته:

تقوم الجهة الحكومية بدبي بـ

5.6.1 تطبيق سجلات التدقيق في نظم معالجة المعلومات، تبعاً للضرورة؛

5.6.2 تسجيل قوائم ضبط الدخول الافتراضي والفعلي وتحديثها ومراجعتها بصفة دورية.

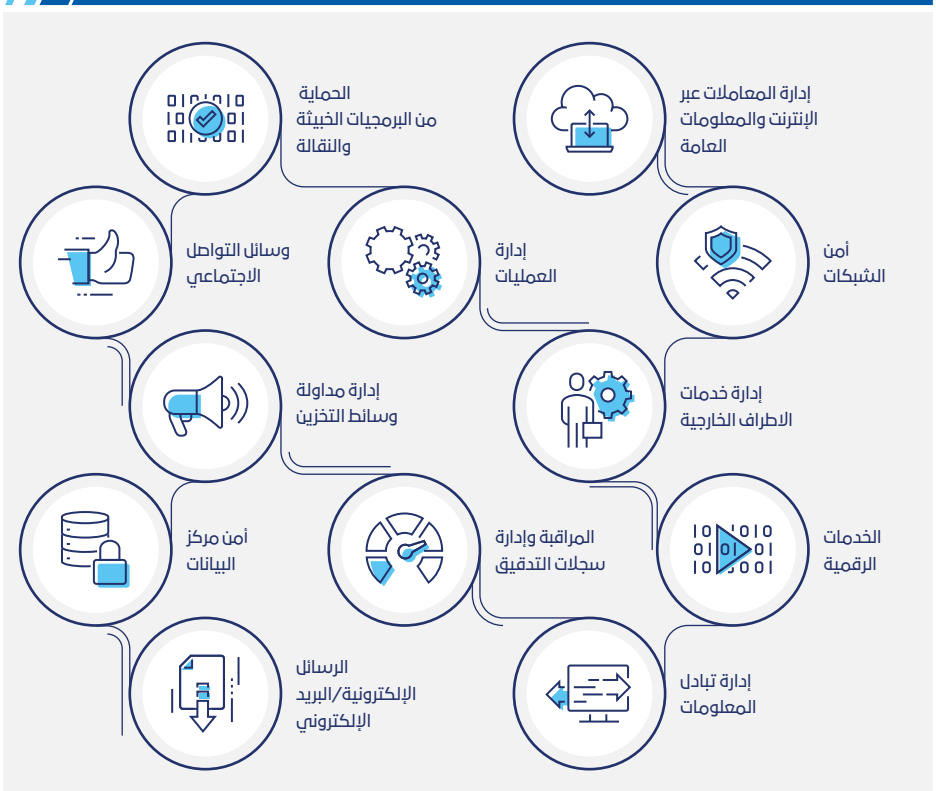
المجال 6
إدارة العمليات والنظم والإتصالات

المجال 6
إدارة العمليات والنظم والإتصالات

الهدف

الحد من المخاطر المرتبطة بالعمليات اليومية لأنظمة المعلومات والتطبيقات والشبكات وأدوات الاتصال، سواء المستخدمة في الجهة داخلياً و/أو مع طرف خارجي.

ضوابط إدارة العمليات والنظم والإتصالات



الضابط الرئيسي – 6.1 إدارة العمليات:

الضابط الفرعي – 6.1.1 إدارة السعة الخاصة بالتكنولوجيا والعمليات:

تقوم الجهة الحكومية بدبي بـ

6.1.1.1 التأكد من التخطيط والإعداد المسبق لتوفير السعة والموارد المناسبة لنظم معالجة المعلومات ومكوناتها التقنية، بما يتماشى مع اللوائح المعمول بها؛

6.1.1.2 إجراء مراجعة تخطيط سنوية لمتطلبات السعة الخاصة بموارد نظم معالجة المعلومات ومكوناتها التقنية.

الضابط الفرعي – 6.1.2 توثيق الإجراءات التشغيلية:

تقوم الجهة الحكومية بدبي بـ

6.1.2.1 تطوير مجموعة كاملة من وثائق الإجراءات التشغيلية لكافة نظم معالجة المعلومات، تبين تفاصيل المدخلات والمخرجات والتبعيات، وتحديثها بصفة دورية؛

6.1.2.2 توثيق كتيبات التهيئة الأساسية المحدثة لكافة نظم معالجة المعلومات، بما في ذلك حصر مفصل بكافة مكوناتها، وتحديثها بصفة دورية؛

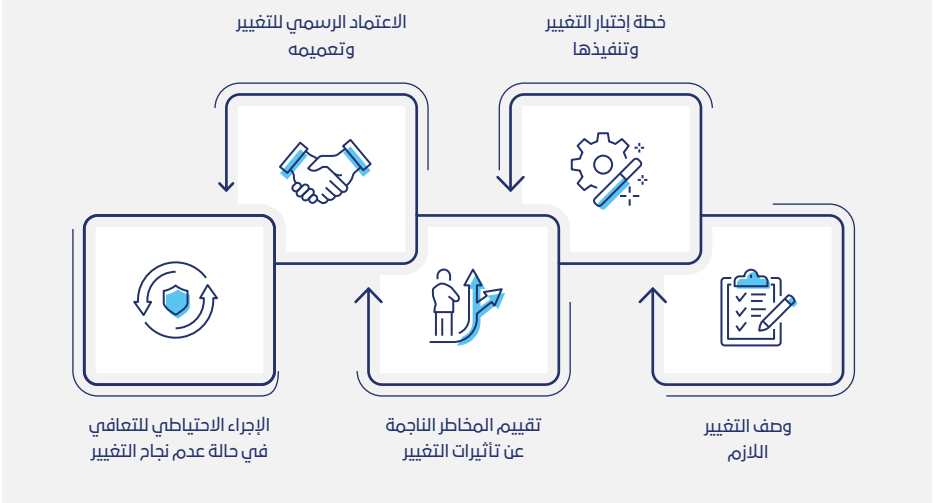
6.1.2.3 توثيق المعايير/الضوابط المتعلقة بالأمن السيبراني لتطبيقها عند شراء/تطوير الأنظمة أو التطبيقات؛

6.1.2.4 وضع ضوابط أمنية كافية على عملية توثيق الإجراءات التشغيلية لكافة نظم معالجة المعلومات الحساسة، وذلك من خلال تحديد قائمة توزيع واضحة للمستخدمين المصرح لهم باستخدامها، والتأكد من توافر هذه الإجراءات التشغيلية للمستخدمين المصرح لهم عند الحاجة.

الضابط الفرعي – 6.1.3 إدارة التغيير:

تقوم الجهة الحكومية بدبي بـ

تطبيق إجراء عملي لإدارة التغيير



6.1.3.1 تطوير سياسة إدارة تغيير موثقة رسمياً من شأنها أن تحدد إجراء إدارة التغيير الشاملة التي تستخدمها الجهة، والتي تبين أدوار أصحاب الأعمال المختلفة ومسؤولياتهم وكذلك نشرها وتحديثها بصفة دورية؛

6.1.3.2 تعزيز سياسة إدارة التغيير، تبعاً للحاجة، بإجراء تفصيلي لتسهيل تطبيق الإجراء الخاص بإدارة التغيير والتهيئة وتوفير الإرشادات لكافة المستخدمين؛

6.1.3.3 تطبيق إجراء عملي لإدارة التغيير يتوجب أن يحتوي، كحد أدنى، على التفاصيل الآتية:

أ. وصف التغيير اللازم؛

ب. خطة إختبار التغيير وتنفيذها؛

ت. تقييم المخاطر الناجمة عن تأثيرات التغيير؛

ث. الإجراء العملي للإعتماد الرسمي للتغيير وتعميمه على كافة أصحاب المصلحة؛

ج. الإجراء الاحتياطي للتعافي في حالة عدم نجاح التغيير.

الضابط الفرعي – 6.1.4 الفصل في الواجبات:

تقوم الجهة الحكومية بدبي بـ

6.1.4.1 فصل الواجبات والمسؤوليات، عند الضرورة، من خلال توزيع المهام الخاصة بعمل معين بين عدة مستخدمين، وبطريقة من شأنها أن تقلل من الأخطاء والاحتيال والتعديل غير المصرح به، أو من إساءة استخدام أصول الجهة.

الضابط الفرعي – 6.1.5 الفصل في المرافق التشغيلية:

تقوم الجهة الحكومية بدبي بـ

6.1.5.1 فصل مرافق التطوير والاختبار والإنتاج لتقليل الخطر الذي قد يؤثر في أنظمة الإنتاج نتيجة الدخول أو التغيير غير المصرح بهما، مقصوداً كان أو غير مقصود؛

6.1.5.2 تخصيص بيئة حاسوبية آمنة لمرافق أنظمة المعلومات المهمة والحساسة.

الضابط الفرعي – 6.1.6 تطبيق أنظمة المعلومات:

تقوم الجهة الحكومية بدبي بـ

6.1.6.1 تطوير سياسة وإجراءات رسمية لاقتناء، وتطبيق وترقية نظم المعلومات التي تفي بمتطلبات الجهة لضمان تنفيذ ضوابط الحماية قبل قبول أو تطبيق هذه الأنظمة؛

6.1.6.2 تحديد معايير قبول تطبيق أنظمة المعلومات الجديدة والترقيات، وفرض عملية مصادقة واعتماد رسمية يتم فيها تحديد المتطلبات الأمنية؛

6.1.6.3 إجراء الاختبارات الأمنية المناسبة على أنظمة المعلومات، عند تطويرها وقبل الموافقة عليها وإطلاقها، مع ضمان فحصها بصورة دورية.

الضابط الفرعي – 6.1.7 التقنيات الافتراضية:

تقوم الجهة الحكومية بدبي بـ

6.1.7.1 استخدام تقنيات افتراضية (virtualization techniques) عند الضرورة، بما يتوافق مع الضوابط الأمنية المناسبة التي من شأنها، عند استخدامها بالشكل السليم، المساعدة في خفض معدل احتمال وقوع الهجمات الأمنية الناجحة؛

الضابط الرئيسي – 6.2 إدارة خدمات الاطراف الخارجية:

تقوم الجهة الحكومية بدبي بـ

6.2.1 تطوير اتفاقية رسمية مع الاطراف الخارجية من مزودي الخدمات، تأخذ بالاعتبار ضرورة التقيد بالمتطلبات الأمنية الخاصة بمعلومات الجهة، وتحديثها بصفة دورية؛

6.2.2 وضع التدابير المناسبة التي من خلالها يتم التأكد من تنفيذ واتباع الأطراف الخارجية الضوابط الأمنية وتعاريف الخدمات ومستوى تقديمها؛ كما تم الاتفاق عليها في الاتفاقيات التعاقدية؛

6.2.3 مراقبة الخدمات وكل ما يتعلق بها من منجزات مزودة من الأطراف الخارجية، ومراجعتها ومراقبتها بشكل منتظم؛

6.2.4 وضع التدابير المناسبة لإدارة وتقييم المخاطر المتعلقة بالتغييرات على خدمات الاطراف الخارجية. أمثلة على هذه التغييرات قد تكون:

أ. تطبيق الجهة ضوابط أمنية جديدة أو تحسينية؛

ب. قيام الجهة بتحسين سياساتها/إجراءاتها؛

ت. استخدام تكنولوجيا أو مورد جديد.

الضابط الرئيسي – 6.3 الحماية من البرمجيات الخبيثة والنقالة:

تقوم الجهة الحكومية بدبي بـ

6.3.1 تطوير سياسة رسمية تغطي إحتياجات ضوابط الحماية، والكشف عن البرمجيات الخبيثة وضوابط التعافي منها، وتوزيعها وتحديثها بصفة دورية؛

6.3.2 القيام بالتوعية المنتظمة عن أهمية حماية بنية الجهة التحتية من هجمات البرمجيات الخبيثة على مستوى الجهة كافة؛

6.3.3 تطبيق نظام/برنامج مناسب على مستوى الجهة، يتم من خلاله مسح البرمجيات الخبيثة والكشف عنها وإزالتها؛

6.3.4 المحافظة على آليات حماية محدثة ضد البرمجيات الخبيثة، وتحديث هذه الآليات باستمرار من خلال إصدارات جديدة؛

6.3.5 القيام بإجراء مسح دوري لكافة أنظمة المعلومات ومسح فوري للملفات التي يتم تحميلها من مصادر خارجية أو فتحها أو تشغيلها، وذلك وفقا لما تحدده السياسات المطبقة؛

6.3.6 أتمتة وتهيئة وتحديث وتشغيل أنظمة مكافحة البرمجيات الخبيثة بين جميع المستخدمين والموظفين؛

6.3.7 إنشاء قنوات اتصال استعلامية مناسبة للحصول على أحدث تفاصيل البرمجيات الخبيثة الجديدة عليها؛

6.3.8 وضع تطبيق خطط/إجراءات الاستمرارية المناسبة للتعافي من هجمات البرمجيات الخبيثة؛

6.3.9 تحديد تقنيات برمجيات الأجهزة النقالة: المقبولة وغير المقبولة؛

6.3.10 وضع قيود استخدام رسمية وإرشادات تنفيذ على تقنيات برمجيات الأجهزة النقالة المقبولة؛

6.3.11 فرض تفويض ومراقبة ورقابة رسمية على استخدام تقنيات برمجيات الأجهزة النقالة.

الضابط الرئيسي – 6.4 أمن الشبكات

تقوم الجهة الحكومية بدبي بـ:

6.4.1 تطبيق إجراء رسمي للتحكم بالترابط بين شبكة الجهة وأنظمة المعلومات الحساسة التي تملكها وأي شبكة أو أنظمة معلومات أخرى خارج حدودها الرسمية؛ مبينة أدوار ومسؤوليات حماية التوصيات وجميع المسائل الضرورية الأخرى، مثل مدة الاتصال ومنافذها ودخول المستخدمين؛

6.4.2 تطوير وتطبيق اتفاقيات خدمة الشبكة بحيث تضمن احتواءها على جميع متطلبات ضوابط الأمن ومستوى الخدمة ومتطلبات ادارتها؛

6.4.3 تفعيل مزامنة الساعة في كافة أجهزة الشبكة وفقاً للمرجع المتفق عليه، مثل التوقيت العالمي (UTC)؛ تسهيلاً للتحليل القضائي ولمراقبة دقتها باستمرار؛

6.4.4 مراقبة توصيلات نظام المعلومات باستمرار، والتحقق دوماً من تنفيذ المتطلبات الأمنية؛

6.4.5 تطبيق ضوابط آمنة لمسارات الشبكة؛

6.4.6 توفير مستوى حماية كاف لسرية المعلومات المرسلة ومصداقيتها وتوافرها، ومنع الوصول غير المصرح به إلى المعلومات أو البيانات أثناء العبور (سواء داخل الجهة أو إلى الشبكة الخارجية)؛

6.4.7 إنهاء الاتصال بالشبكة لأي نشاط، طبقاً للفترة الزمنية غير الفاعلة التي تحددها الجهة؛

6.4.8 تطبيق الإجراءات اللازمة لضمان مستوى مناسب/عالٍ من توافر الشبكة؛

6.4.9 تهيئة أجهزة مرور الشبكة تبعاً للحاجة؛ طبقاً للقاعدة العامة «رفض الكل» وقبول تمرير ما هو مبرر بشكل كافٍ، مع المحافظة على سجلات التدقيق لجميع التغييرات وفقاً لسياسة إدارة التغيير الخاصة بالجهة؛

6.4.10 تطوير توثيق كامل عن أجهزة الشبكة وتوصيلاتها ومكوناتها وتعديات بروتوكول الإنترنت، والاحتفاظ بها، مع التأكد من تطبيق حماية أمنية عالية وضوابط على الوثائق؛

6.4.11 تطبيق إجراءات تسجيل ورقابة مناسبة للتمكن من تسجيل الأنشطة الأمنية في الشبكة؛

6.4.12 يتوجب على الجهة تحديد الحد الأدنى من متطلبات الأمان والامتثال ومستويات الخدمة لجميع خدمات الشبكة أو الخدمات الأمنية، وتضمين هذه المتطلبات الواردة في عقد أو اتفاقية الخدمات المدارة أو المقدمة من طرف خارجي؛

6.4.13 التأكد من المراقبة المستمرة للمستخدمين والأجهزة على شبكة الجهة،

والتركيز على الحد من المخاطر المتعلقة بالتهديدات والبرمجيات الضارة وغيرها، وتحسين مستوى الأمان ومنع اختراق البيانات على الشبكة.

الضابط الرئيسي – 6.5 إدارة تبادل المعلومات:

الضابط الفرعي – 6.5.1 تبادل المعلومات:

تقوم الجهة الحكومية بدبي بـ:

6.5.1.1 تطوير سياسة وإجراءات رسمية تحكم تبادل المعلومات داخلياً في الجهة أو خارجياً مع جهات خارجية، وفي كافة أنواع قنوات الاتصال، استناداً إلى أهمية المعلومات وتماشياً مع القوانين واللوائح ذات الصلة؛

6.5.1.2 تطوير اتفاقيات تبادل معلومات رسمية بحيث تشمل متطلبات الحماية وعدم الإفصاح بشأن تبادل أية معلومات تتعلق بالحكومة بين الجهة وأي طرف خارجي، وتحديثها بصفة دورية؛

6.5.1.3 تطبيق ضوابط أمنية كافية على عملية تبادل المعلومات، وبشكل خاص على الوسائط الفعلية المنقولة والتي تحتوي على معلومات، مثل وضع المسميات وتحديد المسؤوليات... إلخ.

الضابط الرئيسي – 6.6 الرسائل الإلكترونية/البريد الإلكتروني:

تقوم الجهة الحكومية بدبي بـ:

6.6.1 تطوير سياسة رسمية للتواصل الإلكتروني تحكم استخدام كافة أدوات إرسال الرسائل الإلكترونية/البريد الإلكتروني المقدمة للمستخدمين؛ والتي تبين المخاطر المترتبة عليها، وكذلك نشرها وتحديثها بصفة دورية؛

6.6.2 تطبيق آليات للتأكيد على سرية ومصداقية الرسائل الإلكترونية/البريد الإلكتروني والتوافر المناسب لها؛

6.6.3 وضع نص «عدم تحمل المسؤولية» الإلزامي للرسائل الإلكترونية/البريد الإلكتروني؛

6.6.4 تطبيق سياسة أرشفة واستبقاء للرسائل الإلكترونية/البريد الإلكتروني؛

6.6.5 تطبيق آليات تحقق هوية متقدمة للدخول إلى الرسائل الإلكترونية/البريد الإلكتروني من شبكات غير موثوقة وشبكات عامة؛

6.6.6 نشر آليات تشفير متقدمة تدعم عدم التنصل/الإنكار (على سبيل المثال، توقيعات رقمية) عندما يتم تبادل معلومات حكومية مهمة وحساسة.

الضابط الرئيسي – 6.7 إدارة المعاملات عبر الإنترنت والمعلومات العامة:

الضابط الفرعي – 6.7.1 ضوابط المعاملات عبر الإنترنت:

تقوم الجهة الحكومية بدبي بـ:

6.7.1.1 وضع وتنفيذ الضوابط المناسبة لضمان السرية والمصداقية والتوافر لأي معلومات أو خدمات مرتبطة بالمعاملات عبر الإنترنت، لحمايتها من عمليات الاحتيال أو التعديل غير المصرح به أو الكشف عنها، إلخ؛

6.7.1.2 تطوير وتنفيذ الاتفاقيات المطلوبة مع أي طرف مشارك في إدارة خدمات المعاملات عبر الانترنت وضمان إدراج الشروط التجارية وتفاصيل التفويض/ السماح والمسؤوليات ... إلخ.

الضابط الفرعي – 6.7.2 المعلومات العامة:

تقوم الجهة الحكومية بدبي بـ:

6.7.2.1 حماية صحة المعلومات المتاحة عبر القنوات العامة التي يمكن الدخول إليها من قبل الجمهور، مثل مواقع الشبكة العالمية ووسائل الإعلام التحريرية المرتبطة بها ... إلخ، واستخدام الضوابط الأمنية الخاصة بالمعلومات، مثل ضوابط التحقق والدخول المناسبة، استناداً إلى طبيعة متطلبات الأعمال و الالتزامات القانونية السائدة؛

6.7.2.2 التأكد من قيام الوحدة الإدارية المفوضة بالتأكد من تقيد المعلومات التي ينشرها الموظفون بالقوانين والقواعد واللوائح المعمول بها، والمصادقة على نشرها.

الضابط الرئيسي – 6.8 إدارة مداولة وسائط التخزين:

تقوم الجهة الحكومية بدبي بـ:

6.8.1 وضع وتنفيذ إجراءات الأمن والحماية المناسبة على جميع أنواع وسائط التخزين التي تحتوي على المعلومات، من حيث التداول أو التخزين أو الاستخدام ... إلخ.

الضابط الرئيسي – 6.9 المراقبة وإدارة سجلات التدقيق:

تقوم الجهة الحكومية بدبي بـ

6.9.1 تفعيل سجلات التدقيق على جميع أنظمة معالجة المعلومات أو التطبيقات ومراجعتها بشكل دائم، مع ضمان تطبيق إجراءات مناسبة للاحتفاظ بها؛

6.9.2 وضع متطلبات المراقبة المناسبة لجميع أنظمة المعلومات/التطبيقات تبعاً لأهميتها؛

6.9.3 تسجيل المهام التي نفذها إداريو النظم ومشغلوها، وضمان مراجعتها باستمرار عن طريق وحدة مستقلة؛

6.9.4 تفعيل إجراء تسجيل الأخطاء أو الأعطال في كافة مستويات النظم، بما في ذلك الشبكة والتطبيقات والأجهزة الخادمة وقواعد البيانات؛

6.9.5 وضع آلية مناسبة لتحليل سجلات التدقيق، وتنفيذها، واتخاذ الإجراءات المناسبة تجاه الأخطاء؛

6.9.6 حماية أنظمة التسجيل وملفاتها، حيثما كان ذلك مطلوباً، من التغييرات غير المصرح بها؛ بما في ذلك التعديات والإلغاءات وإعادة تسميتها في محتويات سجلات التدقيق والتواريخ وأختام التوقيت؛

6.9.7 تحديد مدة زمنية مناسبة للاحتفاظ بمعلومات سجلات التدقيق تبعاً لكل من احتياجات الأعمال وحساسية المعلومات؛

6.9.8 تفعيل تزامن التوقيت لجميع أنظمة معالجة المعلومات/التطبيقات مع مصدر دقيق للوقت.

الضابط الرئيسي – 6.10 أمن مركز البيانات:

6.10.1 تحديد سياسة أمن مركز البيانات بناءً على تقييم المخاطر لتطبيق إجراءات الأمان والحماية الافتراضية والفعلية والبيئية، وذلك لتعزيز أمان مركز بيانات الجهة والجوانب ذات الصلة؛

6.10.2 تطبيق آلية المصادقة متعددة العوامل في إطار عملية ضبط الدخول إلى مركز البيانات، ليتطلب استخدام عاملين مختلفين أو أكثر للمصادقة/الدخول؛

6.10.3 الاحتفاظ بقائمة للأفراد المصرح لهم بدخول مركز البيانات افتراضياً وفعلياً مع سجلات الاعتماد المتعلقة بها متضمنةً المبررات التي تخولهم للدخول؛

6.10.4 الاحتفاظ بسجلات تسجيل حركة دخول الأشخاص إلى مركز البيانات وخروجهم مع تحديد التاريخ والوقت والغرض من الزيارة وغيرها، والحرص على مراجعة/تدقيق قوائم وسجلات الدخول الفعلي والافتراضي بصفة دورية؛

6.10.5 اعتماد التغييرات والأنشطة المتعلقة بأصول مركز البيانات وتوثيقها بشكل رسمي، والحرص على تعيين فريق مستقل لمراجعة هذه السجلات بصفة دورية؛

6.10.6 تجهيز مراكز البيانات بكاميرات مراقبة لمتابعة الأنشطة التي تجري فيها وتسجيلها، مع الاحتفاظ بهذه السجلات وفقاً لشروط سياسة الاحتفاظ الخاصة بالجهة؛

6.10.7 تحديد الإجراءات اللازمة لشرح عملية التعامل مع حالات الطوارئ داخل مركز البيانات.

الضابط الرئيسي – 6.11 الخدمات الرقمية:

6.11.1 تحديد الخدمات الرقمية الخاصة بالجهة والتخطيط لها وتنفيذها وفقاً للوائح والقوانين المعمول بها؛

6.11.2 التأكد من إتاحة الخدمات الرقمية المعتمدة على القنوات الرقمية، بما يفي بمتطلبات أمن المعلومات واستمرارية العمل؛

6.11.3 إجراء عمليات تدقيق دورية لضمان امتثال الجهة لعوامل الأمان والخصوصية وحماية البيانات المتعلقة بالخدمات الرقمية.

الضابط الرئيسي – 6.12 وسائل التواصل الاجتماعي:

6.12.1 وضع وتطبيق سياسة الاستخدام الآمن لوسائل التواصل الاجتماعي وإدارتها، مع مراعاة المخاطر المتعلقة باستخدامها واللوائح والقوانين المعمول بها؛

6.12.2 تعزيز سياسة وسائل التواصل الاجتماعي بإجراء مفصل يتضمن ما يلي:

أ. إنشاء حسابات وسائل التواصل الاجتماعي وإدارتها وضمان أمانها والإشراف عليها؛

ب. مشاركة المعلومات وإدارة المحتوى؛

ت. حماية الخصوصية؛

ث. المراقبة وإدارة السجلات؛

ج. إدارة الحوادث.

المجال 7
التخطيط لاستمرارية الأعمال والأنشطة

المجال 7
التخطيط لاستمرارية الأعمال والأنشطة

الهدف

أ. ضمان توافر المعلومات والخدمات وإجراءات العمل المهمة ضمن الجهة الحكومية؛

ب. ضمان توافر خدمات تقنية المعلومات على النحو المطلوب؛

ت. ضمان الحد الأدنى من تأثر الأعمال في حالة تعطل أو تغيير خدمة ما؛

ث. التأكد من أن خدمات تقنية المعلومات وبنيتها التحتية قادرتان على المقاومة والتعافي في حالات الفشل الناجمة عن الأخطاء أو الهجمات المخطط لها أو الكوارث.

ضوابط التخطيط لاستمرارية الأعمال و الأنشطة

الضابط الرئيسي – 7.1 تحليل التأثير في العمل:

تقوم الجهة الحكومية بدبي بـ

7.1.1 تحديد منهجية تحليل التأثير على الأعمال والتي تغطي جميع العمليات والخدمات الحرجة وأنظمة المعلومات ذات الصلة وتطبيقها دورياً بما يتواءم مع توجيهات البنية التحتية للمعلومات الأساسية وتوجيهات تطوير خطة المرونة السيبرانية الصادرة من مركز دبي للأمن الإلكتروني؛

7.1.2 إجراء تحليل التأثير على الأعمال بصفة دورية وفق الإجراءات المحددة من أجل تعريف وتحديد تأثير احتمالات الفشل التشغيلي؛

7.1.3 تتولى الإدارة العليا مسؤولية تحليل التأثير على الأعمال بمشاركة جميع القطاعات ذات الصلة؛

7.1.4 تحديد إطار عمل المرونة السيبرانية/مراكز العمليات الأمنية وتطبيقه بشكل يضمن تعزيز مستوى الأمن السيبراني، مع التركيز على تحديد أساليب الهجمات وأنماط المخاطر السيبرانية لتعزيز إمكانية التعافي من أي هجوم سيبراني.

الضابط الرئيسي – 7.2 خطة استمرارية العمل:

تقوم الجهة الحكومية بدبي بـ

7.2.1 تنظيم مسؤولية خطة استمرارية العمل وتكليف لجنة من الإدارة العليا ومالكي الأعمال بذلك، وتبيانها؛ بوضع مسؤوليات معرفة وواضحة؛

7.2.2 تطوير خطة استمرارية العمل وضمان تطبيقها واختبارها وإعادة تقييمها بصفة دورية، وتغطي ما يلي:

أ. يجب أن تستند الخطة إلى تحليل التأثير على الأعمال وتقييم المخاطر؛

ب. يجب أن تشمل الخطة، في الحد الأدنى، الهدف والنطاق ومعايير التشغيل وإجراء التطبيق والعلاقة التكاملية ضمن الجهة وخارجها ومتطلبات الموارد وحماية المعلومات وأصول المعلومات عند حدوث المشكلات وغيرها؛

ت. يجب أن تتضمن الخطة متطلبات جميع خدمات تقنية المعلومات والعمل الأساسية من حيث المرونة والقدرة على التعافي واتخاذ الحلول البديلة؛

ث. يجب أن تغطي الخطة إرشادات الاستخدام والأدوار والمسؤوليات والإجراءات وعمليات التواصل وسيناريوهات الاختبار ومنهجيته.

7.2.3 تصميم عملية استمرارية العمل بطريقة تقلل من أثر التعطيل الكبير في وظائفه وعملياته الرئيسية.

الضابط الرئيسي – 7.3 التعافي من الكوارث:

تقوم الجهة الحكومية بدبي بـ

7.3.1 تحديد أنظمة العمل والتطبيقات الأكثر أهمية، طبقاً لتقييم المخاطر الذي تجريه الجهة؛

7.3.2 إعداد خطة مناسبة لتعافي أنظمة العمل المهمة والمحددة وفقاً لما تتطلبه عمليات الجهة؛

7.3.3 تحديد نوعية خطة التعافي بحيث تكون قابلة للتطبيق وتفي بالمتطلبات؛

7.3.4 ممارسة خطة التعافي المقررة وإجراء فحص دوري لها؛

7.3.5 إنشاء مواقع التعافي من الكوارث إذا ما أدى تعطل أنظمة معلومات الجهة وتطبيقاتها إلى خسارة كبيرة للحكومة، وذلك بناء على دراسة جدوى.

الضابط الرئيسي – 7.4 استراتيجيات النسخ الاحتياطي والتخزين:

الضابط الفرعي – 7.4.1 سياسة التخزين والنسخ الاحتياطي، وإجراءاتها:

تقوم الجهة الحكومية بدبي بـ

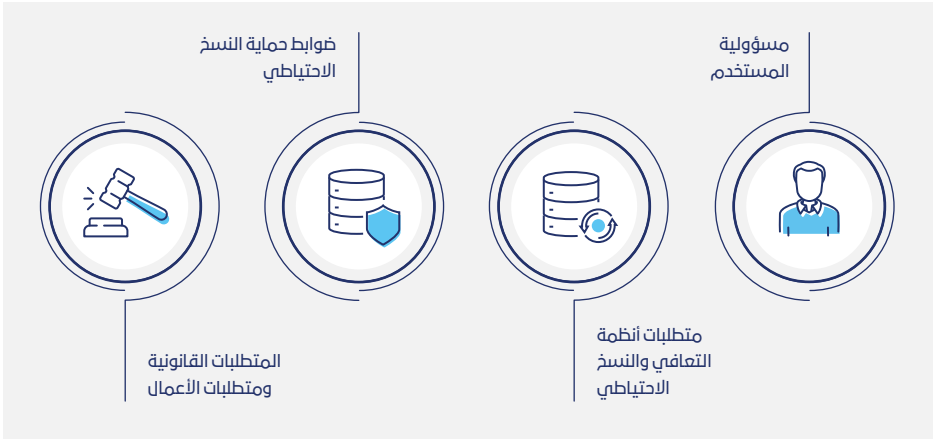
7.4.1.1 تطوير ونشر سياسة رسمية موثقة للنسخ الاحتياطي والتخزين واستبقاء المعلومات وتحديثها دورياً، على أن تشمل ما يأتي:

أ. مسؤولية المستخدم؛

ب. متطلبات أنظمة التعافي والنسخ الاحتياطي؛

ت. ضوابط حماية النسخ الاحتياطي؛

ث. المتطلبات القانونية ومتطلبات الأعمال (على سبيل المثال: نقطة التعافي المستهدفة، زمن التعافي المستهدف ... وغيرها).



7.4.1.2 استكمال سياسة النسخ الاحتياطية بوضع إجراء مفصل لمواصفات الاحتفاظ بالنسخ الاحتياطية والتخزين، وتطبيقها إذا لزم الأمر؛

الضابط الفرعي – 7.4.2 حماية مكتبة وسائط التخزين ومواردها:

تقوم الجهة الحكومية بدبي بـ

7.4.2.1 تطوير سياسة و إجراءات رسمية موثقة بشأن حماية مكتبة وسائط التخزين ونشرها وتحديثها بصفة دورية، بما يشمل التخلص من الوسائط أو إعادة استخدامها؛

7.4.2.2 تقييد الدخول إلى مكتبات وسائط وموارد التخزين ومراقبته المستمرة؛

7.4.2.3 وضع المسميات بوضوح على كافة وسائط وموارد التخزين، وتبيين قوائم التوزيع وضوابط التعامل والتصنيف الأمني الخاص بالتطبيق وفقاً لسياسة تصنيف الأصول؛

7.4.2.4 تخصيص أماكن مناسبة، مزودة بتدابير أمنية وبيئية وضوابط كافية لتخزين وسائط النسخ الاحتياطية، سواء داخل الموقع/خارج الموقع، وعلى النحو الذي تحدده الجهة؛

7.4.2.5 إعداد اتفاقيات وضوابط أمنية ملائمة في حالة اشتراك طرف خارجي في التعامل مع مكتبة وسائط التخزين التابعة للجهة؛

7.4.2.6 حماية كافة وسائط النسخ الاحتياطية الفعلية في أثناء عملية نقلها ومراقبتها؛

7.4.2.7 تشفير وسائط النسخ الاحتياطية والأرشيفات، في حال كان مثل هذا الإجراء مناسباً وذا جدوى تقنية؛

7.4.2.8 الحفاظ على المسؤولية تجاه وسائط النسخ الاحتياطية المنقولة خارج حدود مناطق سيطرة الجهة، وحصرها بالموظفين المفوضين.

الضابط الفرعي – 7.4.3 فحص استرجاع النسخ الاحتياطي:

تقوم الجهة الحكومية بدبي بـ

7.4.3.1 تخطيط عملية فحص دوري واسترجاع لكافة وسائط النسخ الاحتياطية والتخزين وتنفيذ هذه العملية.

الضابط الرئيسي – 7.5 فحص تخطيط استمرارية العمل ومراجعته:

7.5.1 تحديث خطة استمرارية العمل وخطة التعافي من الكوارث والنسخ الاحتياطي والاسترجاع، واختبارها بصفة دورية والحفاظ على سجلات الاختبارات؛

7.5.2 تحديد أنشطة التدريب السيبراني للأنظمة الأساسية وتنفيذها بصفة دورية لاختبار مدى فعالية خطط المرونة الخاصة بها.

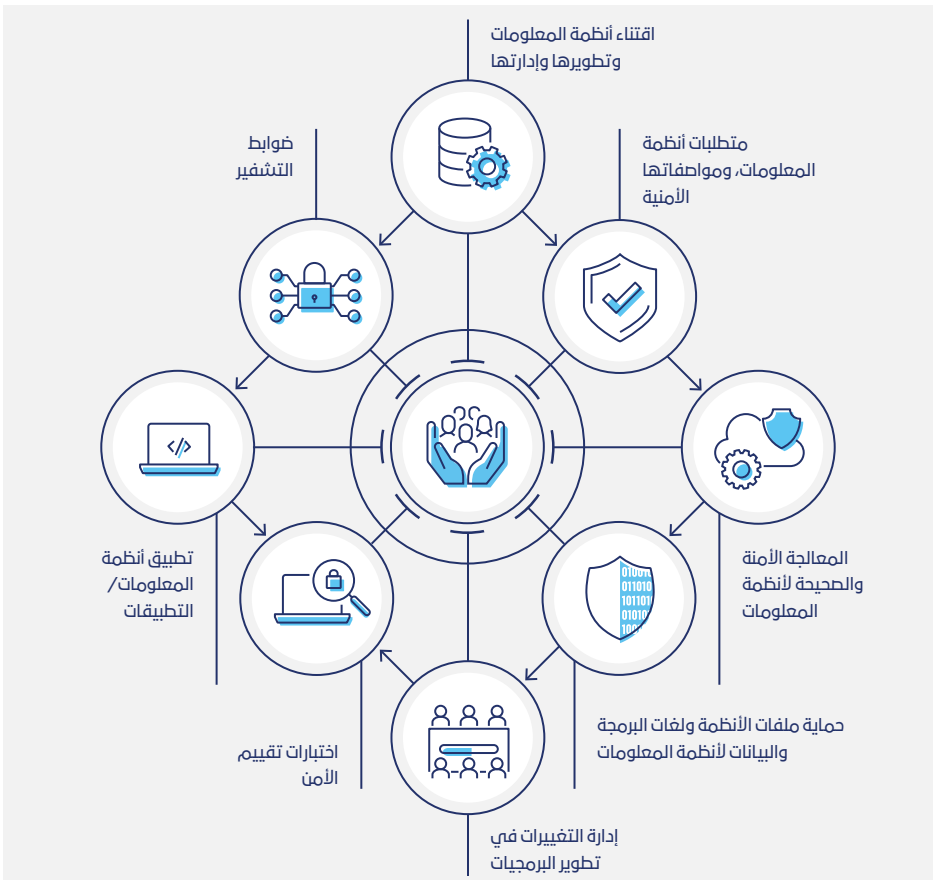
المجال 8
امتلاك وتطوير وإدارة نظم المعلومات

المجال 8
امتلاك وتطوير وإدارة نظم المعلومات

الهدف

إدراج أمن المعلومات في دورة إقتناء/تطوير النظم لمنع التعديل غير المصرح به على هذه الأنظمة أو إساءة استخدام المعلومات الخاصة بالحكومة، ووضع أسس البرمجة الآمنة.

ضوابط امتلاك وتطوير وإدارة نظم المعلومات



الضابط الرئيسي – 8.1 اقتناء أنظمة المعلومات وتطويرها وإدارتها:

الضابط الفرعي – 8.1.1 سياسة وإجراءات اقتناء أنظمة المعلومات وتطويرها وإدارتها:

تقوم الجهة الحكومية بدبي بـ:

8.1.1.1 تطوير السياسة والإجراءات الرسمية الموثقة لاقتناء وتطوير وإدارة نظم المعلومات، بحيث تتناول متطلبات الجهة لضمان أمن التطبيقات المطورة داخلياً أو من قبل أي طرف خارجي، مع تحديثها بصفة دورية ونشرها، بما في ذلك تطبيقات الهاتف المحمول؛

8.1.1.2. تطوير منهجية الأمان عن طريق التصميم، وتطبيقها لضمان إنشاء النظم وجميع مكوناتها بحيث تتضمن السياسات ذات الصلة الصادرة عن مركز دبي للأمن الإلكتروني، مع تطبيق منهجية استباقية تعتمد على تعزيز الأمان والخصوصية منذ البداية.

الضابط الفرعي – 8.1.2 تطوير التطبيقات

تقوم الجهة الحكومية بدبي بـ:

8.1.2.1 وضع منهجية لتطوير التطبيقات أو النظم تتضمن ضوابط أمنية كافية في جميع مراحل دورة حياة تطوير البرمجيات، مع الأخذ في الاعتبار متطلبات الأمن المحددة (على سبيل المثال الفنية، التقنية، والضمان الخ) في كل مرحلة من مراحل تطوير البرمجيات؛

8.1.2.2 تحديد وتوزيع والحفاظ على إجراء رسمي للنشر الآمن والتوزيع والتخصيص وإيقاف تشغيل تطبيقات أجهزة الحوسبة المحمولة وواجهات التطبيقات (بما في ذلك مكونات الطرف الثالث)، من خلال تحديثات/فحوصات منتظمة لضمان مستوى كاف من الأمن؛

8.1.2.3. حماية المعلومات والبيانات التي تم التعامل معها ومعالجتها من قبل التطبيقات على الشبكات العامة من الأنشطة الاحتيالية أو التعديلات غير المصرح بها أو الإفصاح، ومنع أي عملية غير مكتملة.

الضابط الرئيسي – 8.2 متطلبات أنظمة المعلومات، ومواصفاتها الأمنية:

تقوم الجهة الحكومية بدبي بـ

8.2.1 تحديد متطلبات أمن المعلومات وتوثيقها في جميع دراسات الجدوى وطلبات العروض وطلبات الأعمال المتعلقة بالأنظمة المراد إقتناؤها أو التي سيتم تطويرها داخلياً، لضمان دمج الضوابط الأمنية المناسبة وتخفيض التكاليف المرتبطة بهذه الضوابط؛

8.2.2 إعتماد وثائق تصميم أنظمة المعلومات التي تتناول الاحتياجات الأمنية التي تغطي جميع المنصات ذات الصلة (على سبيل المثال أنظمة التشغيل، المتصفحات، أجهزة الحوسبة المحمولة، الخ)؛

8.2.3 تطوير معايير البرمجة الآمنة الخاصة بتطوير وبرمجة أنظمة المعلومات/تطبيقات الهاتف المحمول/تطبيقات الإنترنت؛

8.2.4 تصميم الهيكل الأمني لتطوير أنظمة المعلومات وتطبيقها بما في ذلك أمن الشبكات، وأمن الإرسال ... الخ؛

8.2.5 تطبيق إجراء عملي مناسب لإدارة التهيئة خلال مرحلة تصميم أنظمة المعلومات، وتطويرها وتطبيقها وتشغيلها.

الضابط الرئيسي – 8.3 المعالجة الآمنة والصحيحة لأنظمة المعلومات:

تقوم الجهة الحكومية بدبي بـ

8.3.1 إجراء الاختبارات المناسبة للتحقق من صحة ضوابط إدخلال البيانات في أنظمة المعلومات أو التطبيقات؛

8.3.2 تحديد متطلبات لمصداقية الرسائل والمعلومات التي تجري معالجتها في أنظمة المعلومات/التطبيقات، وضمان تطبيق الضوابط المناسبة لحماية مصداقيتها؛

8.3.3 تضمين ضوابط التحقق من صحة المعلومات في الأنظمة/التطبيقات أثناء معالجتها، للكشف والحد عن أي قصور في مصداقية المعلومات المعالجة؛

8.3.4 إجراء الاختبارات المناسبة للتحقق من صحة ضوابط مخرجات البيانات من أنظمة المعلومات/التطبيقات.

الضابط الرئيسي – 8.4 حماية ملفات الأنظمة ولغات البرمجة والبيانات لأنظمة المعلومات:

تقوم الجهة الحكومية بدبي بـ:

8.4.1 تطبيق إجراءات تقييدية على تثبيت وصيانة أية برامج في البيئات التشغيلية لأنظمة المعلومات؛

8.4.2 تطبيق ضوابط الحماية المناسبة لاستخدام بيانات الاختبار؛

8.4.3 تطبيق الإجراءات المناسبة للتحكم بالوصول إلى النص المصدري للبرامج وأنظمة المعلومات/التطبيقات.

الضابط الرئيسي 8.5 إدارة التغييرات في تطوير البرمجيات:

تقوم الجهة الحكومية بدبي بـ:

8.5.1 تطبيق الضوابط المناسبة لإدارة التغيير في عمليات تطوير البرمجيات سواء أجريت داخلياً أو عن طريق الاستعانة بمصادر خارجية؛

8.5.2 إجراء الاختبارات والتحقق من الحالة التشغيلية لجميع أنظمة المعلومات/التطبيقات بعد تنفيذ أي تغيير عليها؛

8.5.3 تطبيق الضوابط المناسبة للحد من مخاطر تغيير البرمجيات؛

8.5.4 تطبيق الضوابط المناسبة لمنع تسرب المعلومات في جميع بيئات أنظمة المعلومات/التطبيقات؛

8.5.5 تطبيق ضوابط الأمن المناسبة على البرمجيات/التطبيقات التي يتم تطويرها عن طريق الاستعانة بمصادر خارجية تغطي جميع مراحل المشروع بما في ذلك إدارة شيفرة المصدر، صيانة التطبيقات ... إلخ.

الضابط الرئيسي – 8.6 اختبارات تقييم الأمن:

تقوم الجهة الحكومية بدبي بـ:

8.6.1 إجراء المراجعات الأمنية التقنية/عمليات التدقيق الأمني وإجراءات تحديد نقاط الضعف لتقييم البنية التحتية التقنية وأمان أنظمة المعلومات/التطبيقات بصفة دورية وتحديد قدرتها على مواجهة أحدث التهديدات ونقاط الضعف؛

8.6.2 إجراء المراجعات الدورية للنصوص المصدرية لجميع أنظمة المعلومات/التطبيقات المطورة داخلياً أو من قبل الغير.

الضابط الرئيسي – 8.7 تطبيق أنظمة المعلومات/التطبيقات:

تقوم الجهة الحكومية بدبي بـ

8.7.1 إطلاق أنظمة المعلومات/التطبيقات في البيئات التشغيلية بعد اختبارها بنجاح، وإصلاح حالات الخلل الخطرة والمخاطر العالية المحددة؛

8.7.2 تطبيق عملية موافقة أمنية للتأكد من التنفيذ المناسب للضوابط الأمنية على جميع أنظمة المعلومات/التطبيقات قبل إطلاقها.

الضابط الرئيسي – 8.8 ضوابط التشفير:

تقوم الجهة الحكومية بدبي بـ

8.8.1 تطوير سياسة لاستخدام التشفير وإدارة مفاتيحه، ونشرها وتحديثها بصفة دورية (على سبيل المثال أثناء تطوير وصيانة نظم المعلومات/التطبيقات وما إلى ذلك)؛

8.8.2 تطبيق آليات مناسبة للتشفير وإدارة مفاتيحه؛ وفقاً لحاجة الجهة؛

8.8.3 تطبيق ضوابط الأمن والحماية المناسبة على جميع مفاتيح التشفير المستخدمة لدى الجهة.

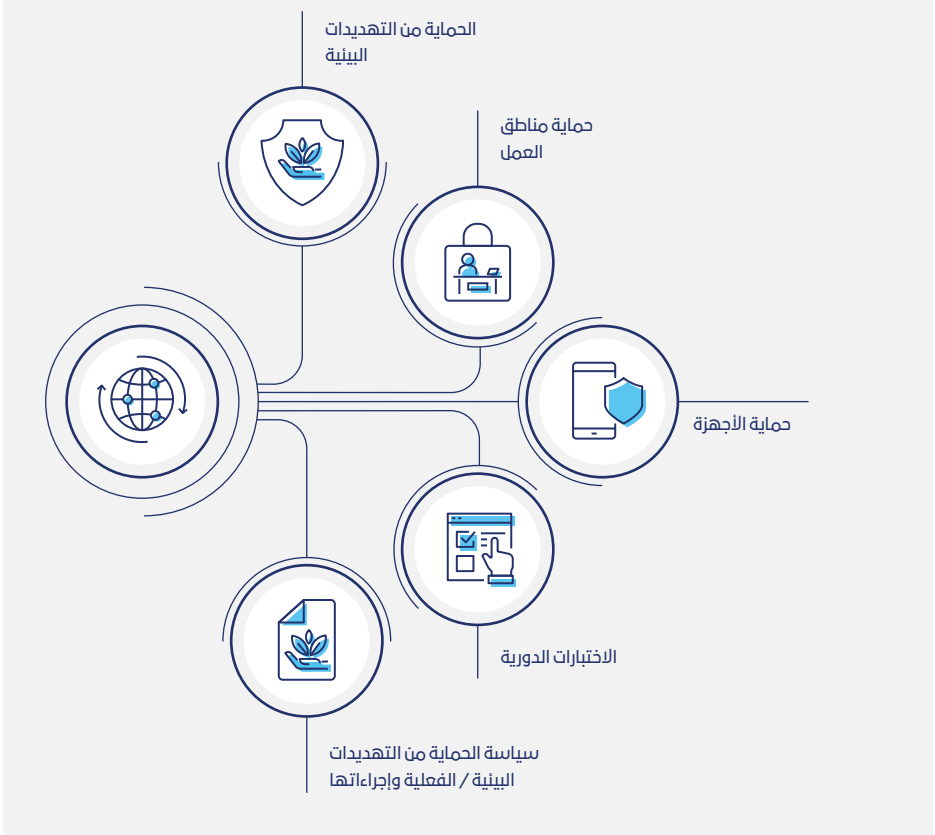
المجال 9
الأمان البيئي والمادي

المجال 9
الأمان البيئي والمادي

الهدف

التأكد من منع الأضرار الفعلية والبيئية والتهديدات والعبث في أماكن العمل والمرافق الخاصة بمعالجة المعلومات ومصادرها.

ضوابط حماية البيئة المحيطة بالمعلومات



الضابط الرئيسي – 9.1 سياسة الحماية من التهديدات البيئية/الفعلية وإجراءاتها:

تقوم الجهة الحكومية بدبي بـ:

9.1.1 تطوير سياسة رسمية وموثقة للحماية من التهديدات البيئية، تتناول متطلبات الجهة؛ لوضع ضوابط الحماية البيئية، وكذلك نشرها وحفظها؛

9.1.2 تعزيز سياسة الحماية من التهديدات البيئية من خلال إجراء رسمي موثق لتيسير تنفيذ هذه السياسة.

الضابط الرئيسي – 9.2 الحماية من التهديدات البيئية:

تقوم الجهة الحكومية بدبي بـ:

9.2.1 تطبيق ضوابط كافية للحماية من التهديدات البيئية، مثل الحرائق والفيضانات والزلازل ...إلخ؛

9.2.2 التحكم بمستوى الرطوبة ودرجة الحرارة السائدة في مرافق معالجة المعلومات، ومراقبتها باستمرار؛

9.2.3 تطبيق الأنظمة المناسبة لإخماد الحرائق والكشف عنها؛

9.2.4 تطبيق الضوابط المناسبة لمراقبة تسرب المياه في مواقع مرافق معالجة المعلومات.

الضابط الرئيسي – 9.3 حماية مناطق العمل:

تقوم الجهة الحكومية بدبي بـ:

9.3.1 تطبيق آليات مناسبة للأمن الفعلي لكل من المكاتب ومراكز البيانات ومناطق العمل الأخرى، تبعاً لأهمية تلك المناطق؛

9.3.2 تزويد الموظفين بالتوجيهات والتوعية المناسبة لضوابط الحماية المطبقة في مناطق العمل؛

9.3.3 تطوير سياسة تأمين المكاتب والشاشات التي تتناول مسؤولية المستخدمين في تأمين المكاتب ومناطق العمل وأجهزة الكمبيوتر وتوزيعها وحفظها؛

9.3.4 تطبيق ضوابط الأمن المناسبة على مناطق التوريد والتحميل.

الضابط الرئيسي – 9.4 حماية الأجهزة:

تقوم الجهة الحكومية بدبي بـ

9.4.1 وضع الأجهزة ذات الصلة بأنظمة المعلومات في مواقع آمنة ومحمية؛

9.4.2 حماية أجهزة وكابلات كهرباء مرافق معالجة المعلومات من الأخرار؛

9.4.3 توفير إمداد الطاقة غير المتقطع (UPS)لحالات إنقطاع تيار الكهرباء الرئيسي؛

9.4.4 تطبيق إجراءات الصيانة المناسبة لجميع مرافق معالجة المعلومات؛

9.4.5 تطبيق ضوابط الحماية المناسبة على الأجهزة ومرافق معالجة المعلومات الكائنة خارج موقع العمل بما في ذلك نقلها وتخزينها ومناولتها؛

9.4.6 تطبيق ضوابط الحماية المناسبة عند التخلص من الأجهزة والمعدات ومرافق معالجة المعلومات أو إعادة استخدامها.

الضابط الرئيسي – 9.5 الاختبارات الدورية:

تقوم الجهة الحكومية بدبي بـ

9.5.1 إجراء الاختبارات المناسبة وعمليات التقييم بصفة دورية على جميع ضوابط الحماية الفعلية والبيئية المطبقة، بما يشمل مراكز البيانات والسجلات المحفوظة.

المجال 10
دور ومسؤوليات الموارد البشرية

المجال 10
دور ومسؤوليات الموارد البشرية

الهدف

تحديد أدوار موظفي الجهات الحكومية والمتعاملين معها ومسؤولياتهم المتعلقة بالمعلومات ومرافق المعالجة الخاصة بها، والتأكد من أنهم على علم بالتزاماتهم تجاه أمن المعلومات؛ للحد من أية مخاطر أو انتهاكات مرتبطة بهذا الشأن.

خوابط دور مسؤوليات الموارد البشرية

الضابط الرئيسي – 10.1 الضوابط الأمنية قبل التوظيف:

تقوم الجهة الحكومية بدبي بـ

10.1.1 تحديد أدوار ومسؤوليات الموظفين والمتعاقدين والموظفين الذين جرت الاستعانة بهم من مصادر خارجية، لتتوافق مع سياسة الجهة العامة لأمن المعلومات؛

10.1.2 توثيق الأدوار والمسؤوليات الأمنية في الوصف الوظيفي والأهداف لجميع الموظفين والمتعاقدين وللموظفين الذين جرت الاستعانة بهم من مصادر خارجية؛

10.1.3 إجراء التدقيق الأمني المناسب والتحقق من خلفية جميع المرشحين للعمل وموظفي الأطراف الخارجية المعنيين، وفقاً للقوانين والسياسات المتبعة في حكومة دبي؛

10.1.4 التأكد من تحديد جميع الالتزامات الأمنية في عقود عمل الموظفين والمتعاقدين والموظفين الذين جرت الاستعانة بهم من مصادر خارجية، والتأكد من قراءة المتقدمين للعمل الذين تمت الموافقة على تعيينهم، هذه الالتزامات وموافقتهم عليها؛

10.1.5 تضمين الوعي حول أمن المعلومات كجزء من البرامج التوجيهية للموظفين الجدد والمتعاقدين والموظفين الذين تمت الاستعانة بهم من مصادر خارجية.

الضابط الرئيسي – 10.2 الضوابط الأمنية أثناء العمل:

تقوم الجهة الحكومية بدبي بـ:

10.2.1 تكليف الإدارة العليا مسؤولية فرض امتثال على من يتبع لهم من الموظفين والمتعاقدين والموظفين الذين تمت الاستعانة بهم من مصادر خارجية لسياسات واجراءات الجهة المتعلقة بأمن المعلومات؛

10.2.2 تحديد وتطبيق إجراءات تأديبية واضحة ومحددة للموظفين والمتعاقدين وغيرهم من موظفي الأطراف خارجية في حال انتهاكهم لسياسات أمن المعلومات وإجراءاتها، والاحتفاظ بسجلات الاختراقات الأمنية؛

10.2.3 ضمان تزويد جميع الموظفين والمتعاقدين والموظفين الذين تمت الاستعانة بهم من مصادر خارجية ببرامج وعي أمن المعلومات بشكل منتظم.

الضابط الرئيسي – 10.3 الضوابط الأمنية عند إنهاء الخدمة أو تغيير العمل:

تقوم الجهة الحكومية بدبي بـ:

10.3.1 تطبيق الضوابط الأمنية المناسبة على عملية إنهاء الخدمة أو تغيير العمل؛

10.3.2 إبلاغ الموظف بمتطلبات إنهاء الخدمة؛ بما يتوافق مع اتفاقيات السرية وعقود العمل؛

10.3.3 تطبيق إجراء إعادة الموظف أصول الجهة الحكومية عند إنهاء خدمته؛

10.3.4 تطبيق إجراء إلغاء أو تغيير صلاحية وامتيازات الدخول للموظف، عند إنهاء خدمته أو تغيير عمله.

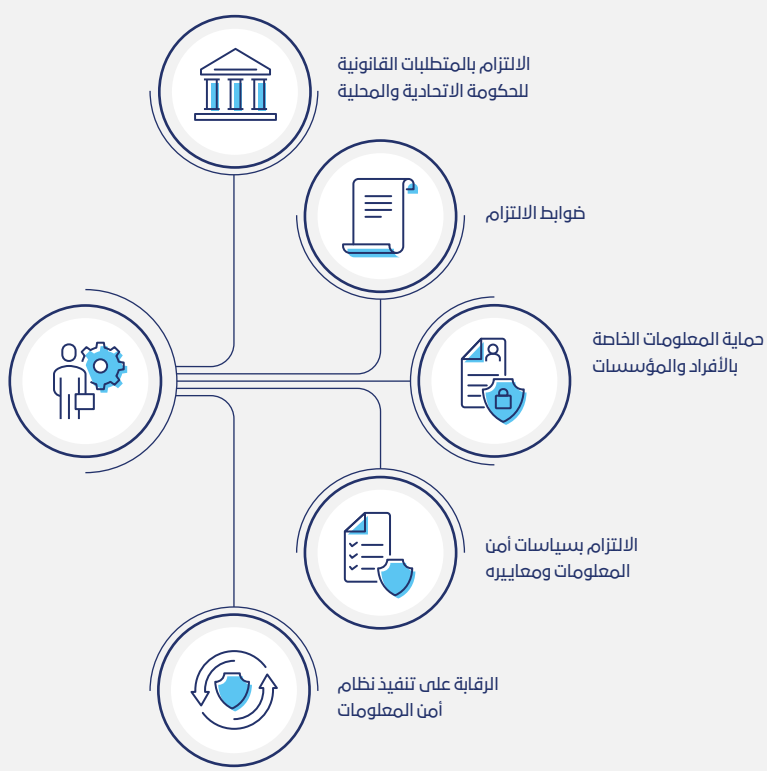
المجال 11
النظام التشريعي والرقابة

المجال 11
النظام التشريعي والرقابة

الهدف

تحديد التشريعات في مجال أمن المعلومات ومتطلبات الالتزام والرقابة بوضوح، من أجل ضمان فعالية تطبيق الضوابط الأمنية وتفادي أية انتهاكات لأية قوانين أو سياسات أو ضوابط.

ضوابط النظام التشريعي والرقابة



الضابط الرئيسي – 11.1 الالتزام بالمتطلبات القانونية للحكومة الاتحادية والمحلية:

تقوم الجهة الحكومية بدبي بـ

11.1.1 ضمان الالتزام بالقوانين والأنظمة الآتية:

- **أ.** مرسوم بقانون اتحادي رقم (46) لسنة 2021 بشأن المعاملات الإلكترونية وخدمات الثقة؛
- **ب.** قانون رقم (21) لسنة 2022 بشأن المعاملات والتجارة الالكترونية؛
- **ت.** قرار المجلس التنفيذي رقم (13) لسنة 2012 بشأن أمن المعلومات في حكومة دبي؛
- **ث.** قانون إدارة الموارد البشرية لحكومة دبي رقم (8) لسنة 2018 وتعديلاته؛
- **ج.** القانون رقم (11) لسنة 2014 بإنشاء مركز دبي للأمن الالكتروني؛
- **ح.** القانون رقم (26) لسنة 2015 بشأن تنظيم نشر وتبادل البيانات في إمارة دبي؛
- **خ.** قانون تنظيم تقديم الخدمات الرقميّة في إمارة دبي رقم (9) لسنة 2022؛
- **د.** المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية؛
- **ذ.** أية قوانين أو قرارات تتعلق بأمن المعلومات أو تتعلق بنطاق خدمات الجهة وتنسجم مع استراتيجيات الحكومة والخطط ذات الصلة.

الضابط الرئيسي – 11.2 ضوابط الالتزام:

تقوم الجهة الحكومية بدبي بـ

11.2.1 تحديد القوانين والأنظمة التي تنطبق على الجهة الحكومية وتنسجم مع نشاطها؛

11.2.2 تطوير ونشر سياسة رسمية لحفظ حقوق الملكية الفكرية وتحديد الالتزامات القانونية المتعلقة باستخدام أصول المعلومات (كالبرامج والأجهزة ... إلخ.) وحفظها؛

11.2.3 ضمان الالتزام بحفظ حقوق الملكية الفكرية واتفاقيات ترخيص البرامج؛

11.2.4 منع الموظفين من استخدام أو توزيع أي نسخ غير مرخصة لمواد أو برمجيات أو تطبيقات مرخصة/خاضعة لحقوق طبع ونشر؛

11.2.5 تطبيق ضوابط الحماية المناسبة لحفظ معلومات وسجلات الجهة الحكومية وتخزينها والتخلص منها.

الضابط الرئيسي – 11.3 حماية المعلومات الخاصة بالأفراد والمؤسسات:

تقوم الجهة الحكومية بدبي بـ

11.3.1 تطوير ونشر سياسة خصوصية تتماشى مع القوانين واللوائح المعمول بها، وتلبي المتطلبات القانونية اللازمة لمنع إساءة استخدام المعلومات الشخصية/الخاصة لموظفي الجهة وعملائها؛

11.3.2 تطوير إجراء مفصل لتدابير الحماية اللازمة لمعالجة البيانات والمعلومات الخاصة، وكذلك نشره وتحديثه بصفة دورية؛

11.3.3 إجراء دورات توعية مستمرة حول متطلبات حماية البيانات والمعلومات الشخصية للموظفين المعنيين بتلك المسؤولية؛

11.3.4 تقييد عمليات الدخول إلى البيانات الخاصة والشخصية وتقليلها ومراقبتها، مع تطبيق الضوابط المناسبة التي تحكم عمليات جمع البيانات الشخصية ومعالجتها ونقلها، والتي يجب أن تجرى بناءً على أساس «ضرورة الإطلاع» على المعلومات؛

11.3.5 وضع تدابير الحماية المناسبة لمنع تسرب البيانات وتطبيقها، بما في ذلك وضع إجراءات المساءلة اللازمة لحماية المعلومات والأجهزة والنُظم الأساسية وغيرها؛

11.3.6 حماية البيانات السرية والحساسة، بما في ذلك البيانات الشخصية، باستخدام تقنيات حماية مناسبة مثل أدوات إخفاء البيانات وإخفاء البيانات بهوية مستعارة وغيرها، وذلك بما يتماشى مع منهجية تصنيف المعلومات الخاصة بالجهة.

الضابط الرئيسي – 11.4 الالتزام بسياسات ومعايير أمن المعلومات:

تقوم الجهة الحكومية بدبي بـ

11.4.1 إجراء المراجعات الدورية للتحقق من مدى الالتزام بتنفيذ سياسات وإجراءات أمن المعلومات؛

11.4.2 إجراء المراجعات التقنية/عمليات التدقيق الأمنية لأنظمة المعلومات بصفة دورية (مثل تحديد مواطن الضعف واختبار الاختراق)، لضمان أمان الأنظمة الأساسية للجهة والتحقق من امتثالها للسياسات والمعايير/الضوابط الأمنية؛

11.4.3 إعداد التقارير للإدارة العليا بصفة دورية لعرض مستوى المرونة السيبرانية للجهة وتفاصيل الإجراءات التصحيحية لنتائج المراجعة الفنية.

الضابط الرئيسي – 11.5 الرقابة على تنفيذ نظام أمن المعلومات:

تقوم الجهة الحكومية بدبي بـ

11.5.1 تخطيط عمليات التدقيق وتنفيذها بصفة دورية على مستوى الجهة (مرة واحدة في السنة على الأقل)، لضمان تلبية الجهة لجميع متطلبات نظام أمن المعلومات، بما في ذلك متطلبات السياسات والأطر والمعايير الصادرة عن مركز دبي للأمن الإلكتروني؛

11.5.2 تقديم تقارير عن نتائج/توصيات التدقيق إلى الإدارة العليا/اللجنة التوجيهية لأمن المعلومات لاستعراض الإجراءات التصحيحية المناسبة؛

11.5.3 متابعة المهام ذات الصلة بصفة دورية لضمان اتخاذ الإجراءات التصحيحية المناسبة في الوقت المناسب بناءً على نتائج التدقيق.

المجال 12

ضمان أمن المعلومات وتقييم الأداء

المجال 12
ضمان أمن المعلومات وتقييم الأداء

الهدف

اختيار مقاييس أمن المعلومات التي تساعد في عملية صنع القرار وتحسين الأداء، وتنفيذ هذه العملية وتطويرها، من خلال الآتي:

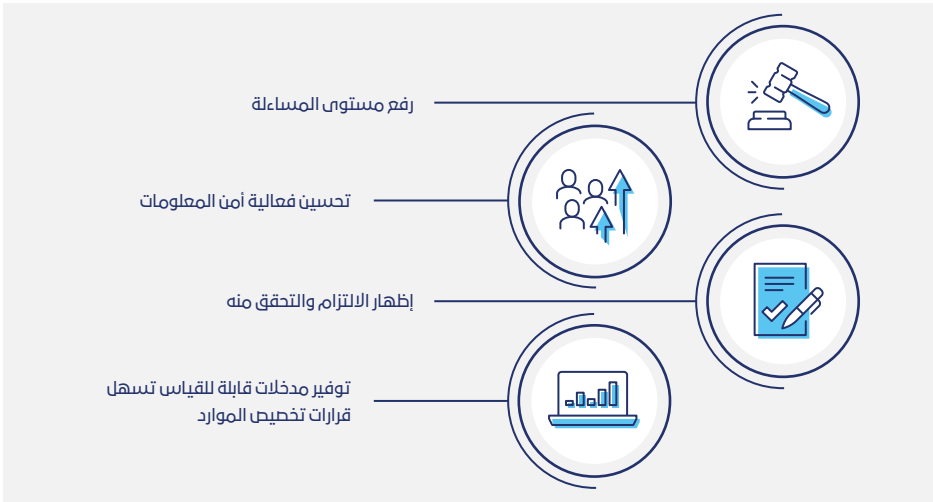
أ. رفع مستوى المساءلة؛

ب. تحسين فعالية أمن المعلومات؛

ت. إظهار الالتزام والتحقق منه؛

ث. توفير مدخلات قابلة للقياس تسهل قرارات تخصيص الموارد.

اختيار مقاييس أمن المعلومات التي تساعد في عملية صنع القرار وتحسين الأداء



الضابط الرئيسي – 12.1 مؤشرات الأداء الرئيسية لأمن المعلومات:

تقوم الجهة الحكومية بدبي بـ

12.1.1 تطوير مجموعة من مؤشرات الأداء الرئيسية لأمن المعلومات، وتحديدها وتنفيذها والتي:

أ. تدعم عمليات التخطيط الاستراتيجي والتشغيلي بحيث تضمن تنفيذ مهمة الجهة؛

ب. يتم إدراجها في التقارير السنوية حول فعالية ضوابط أمن المعلومات؛

ت. تكون معرفة للمساعدة في مراقبة الالتزام بمتطلبات نظام أمن المعلومات؛

ث. تتم مراجعتها بشكل منتظم واستخدامها لدعم السياسات وتخصيص الموارد واتخاذ القرارات المتعلقة بالميزانية، وتقييم حالة برنامج أمن المعلومات والمخاطر التشغيلية؛

ج. يجري استخدامها لمعالجة المشكلات وأوجه القصور واتخاذ الإجراءات التصحيحية، مثل تعديل السياسات والإجراءات، أو تقديم دورات تدريبية حول أمن المعلومات للموظفين؛

ح. يتم تحديدها انطلاقاً من كافة الادارات المعنية بالجهة الحكومية، مثل وحدة عمليات تكنولوجيا المعلومات وفريق الاستجابة للحوادث، والموارد البشرية وفريق الأمن الفعلي، أو غير ذلك، باستخدام مصادر بيانات مختلفة، مثل تقييم المخاطر، واختبار الاختراق، والرقابة المستمرة؛

خ. تحتوي على معلومات قابلة للقياس لأغراض المقارنة، مع استخدام صيغ للتحليل ولتعقب التغييرات باستخدام النقطة المرجعية ذاتها. ويمكن استخدام النسبة المئوية أو المتوسط الحسابي أو الأرقام المطلقة، تبعاً للنشاط الذي يجري قياسه؛

د. يتم قياسها بناءً على إجراءات عمل ثابتة ومتكررة لأمن المعلومات؛

12.1.2 دمج المقاييس ومؤشرات الأداء الرئيسية لأمن المعلومات في جميع إجراءات العمل لدى الجهة الحكومية، ويكلف المسؤولون في الجهة الحكومية مسؤولية تحقيق تلك القياسات؛

12.1.3 اعتماد مقاييس ومؤشرات الأداء الرئيسية لأمن المعلومات من قبل الإدارة العليا للجهة الحكومية؛

12.1.4 إجراء مراجعات دورية حول نتائج قياسات أمن المعلومات من أجل ضمان التحسين المستمر لبرنامج أمن المعلومات داخل الجهة؛

12.1.5 تسجيل الإجراءات والأحداث التي قد يكون لها تأثير في فعالية نظام أمن المعلومات أو أدائه.

الضابط الرئيسي – 12.2 لوحة مقاييس أمن المعلومات:

تقوم الجهة الحكومية بدبي بـ

12.2.1 اعتماد منصة متكاملة، كما هو ضروري، أو دمج المؤشرات ضمن أداة قياس الأداء المعتمدة لدى الجهة، والتي:

أ. تحدد حالة المرونة السيبرانية للجهة ونتائج التدقيق المحددة والإجراءات التصحيحية المعمول بها، إلى جانب تحديد المخاطر العالية والمتبقية؛

ب. تجمع كل مؤشرات الأداء الرئيسية لأمن المعلومات لمراجعتها ومراقبتها من قبل الإدارة العليا والأطراف المعنيين المسؤولين بصفة دورية، وذلك بهدف تسهيل عملية صنع القرار والتخطيط الشامل لبرنامج أمن المعلومات.

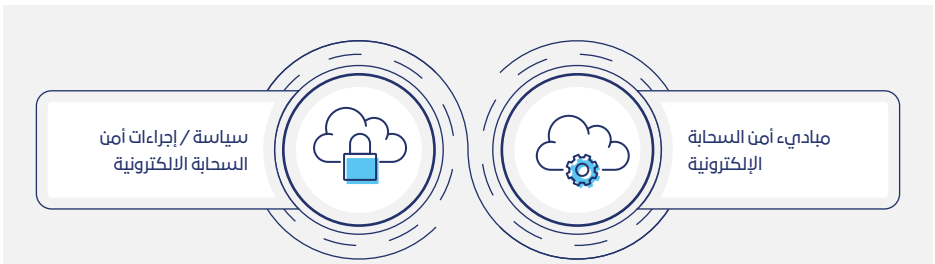
المجال 13
أمن السحابة الإلكترونية

المجال 13
أمن السحابة الإلكترونية

الهدف

وضع ضوابط لتخفيف المخاطر المرتبطة بالحوسبة السحابية واستخدام خدمات السحابة الالكترونية.

ضوابط أمن السحابة الإلكترونية



الضابط الرئيسي: 13.1 سياسة/إجراءات أمن السحابة الالكترونية:

تقوم الجهة الحكومية بدبي بـ

13.1.1 تطوير سياسة رسمية خاصة بأمن السحابة الإلكترونية ونشرها والحفاظ عليها لتلبية متطلبات الجهة فيما يتعلق بعملية إدارة السحابة ككل، والتي تتضمن إجراء اختيار خدمات السحابة الإلكترونية وإدارتها وتسجيل الخروج منها، وتحديد الأدوار والمسؤوليات الخاصة بأصحاب المصلحة المعنيين؛

13.1.2 تطوير ونشر والحفاظ على إجراءات الأمن الخاصة بالسحابة الالكترونية والتي تعمل على توفير تفاصيل التنفيذ لإنشاء وإدارة بيئة آمنة لخدمات السحابة الإلكترونية؛

13.1.3 القيام بمراجعات دورية للسياسات والإجراءات الأمنية السحابية أو إذا حدثت تغييرات كبيرة لضمان استمرار الملاءمة والكفاية والفعالية؛

13.1.4 تطبيق إدارة مخاطر أمن السحابة الإلكترونية، والتي تتضمن متطلبات الجهة حول استخدام نموذج الحوسبة السحابية مثل البرمجيات المقدمة كخدمة والمنصة كخدمة والبنية التحتية كخدمة وما إلى ذلك، بما يشمل إدارة

الهوية والدخول والأمن السيبراني وحماية البيانات والجوانب التنظيمية وما إلى ذلك.

الضابط الرئيسي – 13.2 مباديء أمن السحابة الالكترونية:

الضابط الفرعي – 13.2.1 موقع البيانات:

تقوم الجهة الحكومية بدبي بـ

13.2.1.1 منع التعامل مع البيانات المصنفة وتخزينها عند مقدم خدمة السحابة الالكترونية، خارج نطاق الولاية القانونية أو الحدود الجغرافية لدولة الإمارات العربية المتحدة، بما في ذلك أغراض النسخ الاحتياطي أو التعافي من الكوارث.

الضابط الفرعي – 13.2.2 تصنيف البيانات والتعامل معها:

تقوم الجهة الحكومية بدبي بـ

13.2.2.1 تحديد الضوابط الأمنية المطلوبة إلى مزود الخدمة السحابية للتعامل مع البيانات وفقاً للقوانين واللوائح المعمول بها (بما يتماشى مع الضوابط 11.1 و11.2 من نظام أمن المعلومات).

الضابط الفرعي – 13.2.3 نموذج البناء والتنفيذ:

تقوم الجهة الحكومية بدبي بـ

13.2.3.1 ضمان تنفيذ الضوابط الأمنية السحابية الكافية من قبل مزود الخدمة السحابية وفقاً لنموذج البناء والتنفيذ المعتمد من قبل الجهة.

الضابط الفرعي – 13.2.4 إتفاقيات الخدمة:

تقوم الجهة الحكومية بدبي بـ

13.2.4.1 ضمان من خلال اتفاق رسمي بأن مزود الخدمة السحابية ليس لديه أي حقوق ملكية على البيانات المخزنة بغض النظر عن شكل أو وسيط التخزين؛

13.2.4.2 تطويـر اتفاقية رسمية مع مزود الخدمة السحابية المعتمد/المؤهل من قبل مركز دبي للأمن الإلكتروني، والتي تتضمن متطلبات أمن المعلومات التالية كحد أدنى:

أ. مخاطر أمن المعلومات وطرق الحد منها؛

ب. حماية البيانات وتخزينها؛

ت. التعامل مع حوادث أمن المعلومات؛

ث. التغيير، التعافي والإستعادة؛

ج. موقع البيانات؛

ح. تشفير البيانات.

متطلبات الاتفاق رسمي مع مزود الخدمة السحابية

الضابط الفرعي – 13.2.5 قابلية نقل البيانات والاستمرارية:

تقوم الجهة الحكومية بدبي بـ

13.2.5.1 التأكد بأن مزود الخدمة السحابية لديه المعايير والعمليات الملائمة لدعم قابلية البيانات للنقل والترحيل كلما قررت الجهة نقل بياناتها وتجنب الاعتماد على منهجية البائع الواحد؛

13.2.5.2 ضمان تنفيذ الضوابط الأمنية السحابية المناسبة من قبل مزود الخدمة السحابية، وتحديد متطلبات الجهة الخاصة بإجراء اختبارات دورية لخطط الاستمرارية والتعافي من الكوارث وعرض النتائج على الجهة.

الضابط الفرعي – 13.2.6 الإمتثال والمراقبة:

تقوم الجهة الحكومية بدبي بـ

13.2.6.1 إجراء مراجعات أو تدقيقات دورية للتحقق من التزام مزود الخدمة السحابية بسياسات الأمن المعمول بها وبالمتطلبات التعاقدية.

موجز بالمؤسسات والأبحاث التي تم الاستعانة بها

10. موجز بالمؤسسات والأبحاث التي تم الاستعانة بها

عن معايير أمن المعلومات القائمة حالياً وقوانينه وأطره خلال إعداد نظام أمن المعلومات لحكومة دبي ومراجعته. وقد جرى تحديد وثائق أمن المعلومات ذات الصلة بالموضوع والاستعانة بها، مأخوذة من المؤسسات الآتية، على سبيل المثال لا الحصر:

- The International Organization for Standardization (ISO)؛
- British Standards Institute (BSI)؛
- National Institute of Standards and Technology (NIST)؛
- Information Security Forum؛
- Payment Card Industry (PCI) Standards Council؛
- Information Technology Governance Institute (ITGI)؛
- Information Systems Audit and Control Association (ISACA)؛
- Organization for Economic Cooperation and Development (OECD).

ومن هذا المنطلق، قد تم النظر في إصدارات مختلفة من العديد من المعايير واللوائح والأطر المتعلقة بأمن المعلومات للحفاظ على نظام أمن المعلومات، بما في ذلك على سبيل المثال لا الحصر:

- ISO/IEC (The International Organization for Standardization/The International Electrotechnical Commission) standards؛
- BSI (The British Standards Institute) standards؛
- PCI (The Payment Card Industry) council standards؛
- COBIT (Control Objectives for Information and Related Technology) framework؛

- ITIL (Information Technology Infrastructure Library) framework؛
- SOX (Sarbanes–Oxley Act)؛
- COSO (Committee of Sponsoring Organizations of the Treadway Commission) framework.

إلى جانب ذلك، جرت معاينة العديد من المواقع الحكومية الرسمية من بلدان عديدة من خلال عملية بحث بهدف جمع السياسات والممارسات المتعلقة بأمن المعلومات، والمتاحة للجمهور حالياً. ومن ثم، تم وضع نظام أمن المعلومات في حكومة دبي رسمياً بموجب القرار رقم 13 لعام 2012 استناداً إلى أنظمة وأطر وسياسات وممارسات رائدة في مجال أمن المعلومات. وعلاوةً على ذلك، واستناداً إلى قانون دبي رقم 11 لسنة 2014، تولى مركز دبي للأمن الإلكتروني مسؤولية الحفاظ على نظام أمن المعلومات وتحديثه باستمرار من أجل تضمين أحدث ممارسات أمن المعلومات ومتطلبات الرقابة ذات الصلة.

الملحق
التعريفات

المصادقة متعددة العوامل
تستخدم العملية عاملين أو أكثر لقبول المصادقة، وتتضمن العوامل: 1– بيانات شخصية مثل كلمة المرور أو رقم التعريف الشخصي؛ و2– مقتنيات شخصية مثل أداة لتحديد الهوية أو رمز خاص؛ و3– الخصائص البيولوجية مثل المصادقة الحيوية.

مالك الخطر
شخص أو جهة يتمتع بالسلطة والمسؤولية لضمان إدارة المخاطر بشكل مناسب. كما يتحمل مسؤولية إدارة التهديدات ونقاط الضعف التي يمكن استغلالها، ويجب أن يكون عمله مرتبطاً بالتعامل مع المخاطر ولديه الصلاحية لتنفيذ التدابير التصحيحية اللازمة.

إدارة المشاكل
هي عملية تركز على منع الحوادث أو الحد من تأثيرها، حيث تُعد المشاكل السبب الأساسي لوقوع الحوادث، التي تسعى بدورها إدارة المشاكل لمنع وقوع الحوادث.

ضبط الدخول
هي آلية تمكن الأشخاص المخولين من الدخول إلى مصادر الجهة (الفعلية أو المنطقية)، في حين يمنع الأشخاص غير المخولين من القيام بذلك.

إمتيازات الدخول
ويقصد بها مستوى الدخول الممنوح لأحد المستخدمين للقيام بعمله/بعملها.

المساءلة
وتعني أن الأشخاص مسؤولون عن أفعالهم. ويمكن تحقيق ذلك من خلال عمليتي المراجعة وعدم التنصل من المسؤولية.

الاقتناء
عملية محددة عبر سلسلة من المراحل التي قد تشمل وضع المفاهيم والبدء والتصميم والتقييم والتطوير والاختبار والإنتاج والتعديل والتصرف بالخدمات والأنظمة.

الأصول
الأصول هي المصادر الاقتصادية، وهي أي شيء ملموس أو غير ملموس يمكن امتلاكه أو السيطرة عليه لإنتاج قيمة معينة يجري الاحتفاظ بها للحصول على قيمة اقتصادية إيجابية.

الضمان
هو ضمان ممارسة المعلومات وإدارة المخاطر المتعلقة باستخدامها وتجهيزها وتخزينها، ونقل المعلومات أو البيانات والنظم والعمليات المستخدمة لهذه الأغراض.

سجلات التدقيق
هو سجل زمني أو مجموعة من السجلات ذات الصلة، أو وجهة ومصدر السجلات التي توفر أدلة وثائقية من سلسلة من الأنشطة التي أثرت في أي وقت في عملية محددة، أو إجراء، أو حدث.

التحقق من الهوية
عملية التحقق من صحة ادعاء هوية معينة، وعادة ما يكون التحقق واحداً أو أكثر، من الاجراءات الآتية: شيء تعرفه (كلمة السر)، شيء تملكه (بطاقة الهوية)، أو أي شيء يدل عليك (بصمات الأصابع).

التفويض
يحدد التفويض ما يمكن لشخص ما القيام به على النظام. ويتفعل التفويض مباشرة بعد تحديد الهوية والتحقق منها.

التوافر
جزء من ثالوث أمن المعلومات؛ يشير التوافر إلى انه ينبغي أن تكون المعلومات متاحة عند الحاجة إليها.

التوعية
هي المعرفة وموقف الأفراد مما يخص حماية الأصول الفعلية، خاصة أصول المعلومات لتلك الجهة. وتطلب العديد من الجهات تدريباً رسمياً للتوعية الأمنية (بما في ذلك التعامل مع التهديدات المتعلقة بالهندسة الاجتماعية) لجميع العاملين عند التحاقهم بالعمل لديها. وبعد ذلك يجري هذا الأمر بصفة دورية، عادة ما يكون سنوياً.

أفضل الممارسات
الممارسة الأفضل هي الأسلوب أو الطريقة أو العملية أو النشاط أو الحافز أو المكافأة التي يقدر أنها ستكون أكثر فعالية في تحقيق نتيجة معينة من أي أسلوب أو طريقة أو عملية أخرى، عند تطبيقها على حالة أو ظرف من الظروف.

خطة استمرارية العمل
عملية موثقة تتيح للجهات الاستجابة لحالات اضطراب الأعمال والتعافي منها وفقاً لمستوى محدد مسبقاً من العمليات التشغيلية والعودة إليها واستئنافها وضمان استمرارية الوظائف الأساسية للأعمال.

الأثر في العمل
ويعرف الأثر في العمل بأنه عواقب الأضرار الناجمة عن حدث ما. ويتناول تحليل هذا الأثر تحديد إن كان مقبولا من قبل الجهة المعنية أم لا.

تحليل التأثير في العمل
هو العملية المستخدمة في تحديد أثر انقطاع الخدمات على كل وحدة عمل والجهة ككل. يمكن من خلال التحليل تقديم معلومات عن الآثار المترتبة على المدى القصير والطويل حين وقوع كارثة مثل فقدان المال والسمعة والخدمات المقدمة.

اجلب جهازك الخاص
جلب الجهاز الخاص بك، (ويسمى أيضا باسم جلب التكنولوجيا الخاصة بك، وجلب الهاتف الخاص بك، وجلب الكمبيوتر الشخصي الخاص بك) – يخضع لسياسة السماح للموظفين بجلب الأجهزة المملوكة شخصيا (اجهزة الكمبيوتر المحمولة، والأجهزة اللوحية، والهواتف الذكية) إلى مكان عملهم، واستخدام تلك الأجهزة للوصول إلى المعلومات الخاصة بالشركة والتطبيقات.

عملية المصادقة والاعتماد الرسمية
هو إجراء منهجي لتقييم الأنظمة ووصفها واختبارها والتصريح بها، قبل تشغيل نظام منها أو بعده. أما المصادقة فهي تقييم شامل لضوابط الأمن الإدارية والتشغيلية والفنية لنظام معلومات يجري العمل به لدعم إعتماد الأمن ولتحديد مدى التطبيق الصحيح للضوابط واستخدامها على الوجه المقصود منها؛ سعياً لتحقيق النتائج المرجوة فيما يتعلق بتلبية المتطلبات الأمنية للنظام. وأما الاعتماد فهو القرار الرسمي للإدارة المقدم من قبل مسؤول ذي منصب رفيع للموافقة على تشغيل نظام المعلومات والقبول صراحة بتعريض عمليات الجهة للمخاطرة (بما في ذلك المهمة أو الوظائف أو الصورة أو السمعة)، أو تعريض الأصول أو الأفراد للمخاطرة، استناداً إلى تطبيق مجموعة متفق عليها من الضوابط الأمنية.

إدارة التغيير
هي العملية الرسمية لتوجيه التغييرات في بيئة معالجة المعلومات، ومراقبتها. وتتمثل أهداف إدارة التغيير في الحد من المخاطر الناجمة عن التغييرات التي تطرأ على معالجة المعلومات وعلى بيئتها وتحسين استقرار وموثوقية بيئة المعالجة حال إجراء التغييرات. وتضمن عملية إدارة التغيير أن: هذا التغيير قد طلب إجراؤه وموافق عليه ومخطط له وجرى اختباره ونفذ ضمن برنامج، وأنه قد جرى الإبلاغ عنه وتنفيذه وتوثيقه ومراجعته بعد إحداثه.

البيانات الحساسة / المصنفة
هي أصول / مواد المعلومات أو البيانات (غير المفتوحة وغير العامة) التي تعتبرها الجهة أنها حساسة أو سرية والتي يتعين حماية سريتها أو نزاهتها أو توفرها. ويقتصر الوصول إلى هذه المعلومات على الأشخاص أو العمليات أو الأطراف الأخرى.

التصنيف
هو تعيين فئات للأصول بناءً على معايير محددة مسبقاً. ويستخدم مصطلح التصنيف في مجال أمن المعلومات لتصنيف أصولها من حيث عامل الحساسية؛ لحمايتها من الدخول أو الاستخدام أو الإعلان أو الكشف عنها أو التعطيل أو التعديل أو التخريب غير المصرح بأي منها.

الحوسبة السحابية
تمثل الحوسبة السحابية شكلاً من أشكال مصادر تقنية المعلومات والاتصالات ونموذج التسليم الذي يتيح إمكانية الوصول بسهولة عند الطلب إلى مجموعة مشتركة من موارد الكمبيوتر القابلة للتشكيل (مثل الشبكات والخوادم والتخزين والتطبيقات والخدمات) والتي يمكن توفيرها وإصدارها بسرعة.

أمن السحابة الالكترونية
يشير إلى مجموعة واسعة من السياسات والتقنيات والضوابط التي تم نشرها لحماية البيانات والتطبيقات والبنية التحتية المرتبطة بالحوسبة السحابية. ويتألف من جميع التدابير والممارسات والمبادئ التوجيهية التي يجب تنفيذها لتمكين بنية سحابية آمنة وحماية بيئة الحوسبة السحابية (SaaS, PaaS, IaaS)، إلخ.

مقدم الخدمة السحابية
الجهة التي توفر المنصات السحابية، والبنية التحتية، والتطبيقات، وخدمات الأمن أو التخزين لجهة/منظمة أخرى، وعادة يكون ذلك مقابل رسوم.

الموارد المختصة
محترف أمن المعلومات. وهو مورد مختص لديه القابلية والقدرة على تقديم التدريب والتوعية لموظفي الجهة والمستخدمين الآخرين لدعم برنامج أمن المعلومات للجهة.

الامتثال/الالتزام
ويقصد به التقيد بمعيار أو نظام ما (دولي أو داخلي)، وإظهار الالتزام به.

السرية
وهي أحد أطراف ثالوث أمن المعلومات؛ وتعني السرية وعدم الإفصاح عن بعض أصول المعلومات إلا لشخص مصرح له، وذلك تبعاً لمستوى تصنيف هذه الأصول.

إدارة التهيئة
وهي عملية إدارة خدمة تقنية المعلومات التي تتعقب كافة عناصر التهيئة الفردية (أصول تقنية المعلومات) في أحد أنظمتها، والتي قد تكون على مستوى جهاز حاسوب رئيسي أو على مستوى إدارة تقنية المعلومات بأكملها.

تضارب المصالح
الحالة التي قد يحصل فيها الشخص في جهة ما على منفعة شخصية أو مهنية من الإجراءات أو القرارات المتخذة بصفته الرسمية.

أصول المعلومات الهامة
الأصول التي لديها معلومات الأعمال الهامة والضرورية لتحقيق الأهداف والعمليات ذات الصلة. ويمكن أن تكون موجودة في أشكال كثيرة ولها قيمة تستحق حماية ما هو ضروري لأعمال الجهة ويمكن أن تتسبب في حدوث آثار ضارة كبيرة في حالة انقطاعها أو إذا تم تعديلها/فقدها/إتلافها أو الكشف عنها لأطراف أو عمليات غير مصرح بها.

التشفير
وهو مفهوم يتألف من جزأين: الأول هو عملية تحويل معلومات قابلة للاستخدام على نحو يجعلها غير قابلة للاستخدام من قبل أي شخص غير مخول؛ وتسمى هذه العملية «تشفير». والجزء الثاني هو إمكانية تحويل المعلومات التي جرى تشفيرها (جعلها غير قابلة للاستخدام) واستعادتها؛ بإجراء عملية فك التشفير إلى شكلها الأصلي القابل للاستخدام من قبل مستخدم مخول يملك مفتاح التشفير.

أمين العهدة
ويعرف أمين العهدة بأنه الفرد أو الجهة التي وافقت على تحمل مسؤولية الحفاظ على أصول المعلومات.

قابلية نقل البيانات
هو مفهوم لحماية المستخدمين من تخزين البيانات الخاصة بهم في منصات مغلقة، وبالتالي إغلاقها. وتشير قابلية النقل إلى القدرة على نقل البيانات بين برامج التطبيقات المختلفة أو بيئات الحوسبة أو الخدمات السحابية أو مقدمي الخدمات.

الكوارث
وهي أحداث مأساوية ناتجة عن المخاطر الطبيعية أو التي تكون من صنع الإنسان (والخطر هو موقف ما يشكل مستوى معيناً من التهديدات على الحياة أو الصحة أو الممتلكات أو البيئة)، وتؤثر سلباً في المجتمع أو البيئة.

جهات/جهة حكومة دبي
أي جهة أو سلطة أو مجلس أو مؤسسة أو قسم، وغيرها من حكومة دبي، جرى تأسيسها وتتبع لحكومة دبي قانوناً.

الدليل
وهو كل شيء يستخدم في تحديد أو إظهار حقيقة التسلل أو الإخلال بنظام المعلومات.

الأطراف الخارجية
فرد أو جهة تتعامل مع الجهة الحكومية خلال علاقة تجارية، وتتمتع بإمكانية الوصول إلى معلومات الجهة الحكومية أوأصول المعلومات لديها. وقد تتضمن الأطراف الخارجية، مزودي الخدمات والموردين والعملاء والشركاء والتحالفات والمتعاقدين وما إلى ذلك، وقد تشمل أيضاً الأطراف التعاقدية وغير التعاقدية على السواء.

إطار العمل
وهو مجموعة من المباديء التوجيهية والعمليات المنظمة التي تعالج مسألة معقدة. ويحدد إطار العمل السياسات والممارسات اللازمة لتوفير التوجيه العام بشأن المسائل التي تؤثر في أمن المعلومات.

الاحتيال
وهو الخداع المتعمد لتحقيق مكاسب شخصية أو إلحاق الضرر بفرد أو جهة أخرى.

الحوكمة
تعد حوكمة أمن المعلومات مجموعة فرعية من حوكمة المؤسسات، وهو توفر التوجيه الاستراتيجي وتكفل تحقيق الأهداف وإدارة المخاطر على نحو رشيد، وترصد نجاح أو فشل برنامج أمن المؤسسة.

الحوادث
يمكن إعتبار الحادث على أنه انتهاك، أو تهديد وشيك بانتهاك، سياسات أمن الحاسوب أو سياسات الاستخدام المقبول أو ممارسات الأمن القياسية.

المعلومات
وهي تصف أي معلومات تتعلق بالحوكمة، ويمكن أن تتمثل في أشكال عديدة: كأن تكون مطبوعة أو مكتوبة على الورق، أو مخزنة إلكترونياً أو تلك المرسلة بالبريد أو باستخدام الوسائل الالكترونية، أو التي تظهر في الأفلام، أو التي يتلفظ بها في المحادثات.

مالك أصول المعلومات
يحدد مصطلح «المالك» الفرد أو الجهة التي قد وافقت الإدارة على تحميلها مسؤولية ضبط إنتاج الأصول وتطويرها وصيانتها واستخدامها وأمنها. لكن هذا المصطلح لا يعني أن الشخص له أي حقوق فعلية لملكية الأصول. وإذ يجوز تفويض المهام الروتينية لأمين العهدة، كمثال، للعناية بالأصول على أساس يومي، غير أن المسؤولية تقع على عاتق المالك.

تبادل المعلومات
هي عملية إعطاء وتلقي المعلومات/البيانات أو إنتقال/نقل المعلومات المصنفة (الإلكترونية أو المادية) داخليا في الجهة، أو خارجيا مع أي طرف خارجي.

أمن المعلومات
وهي عملية حماية المعلومات في أي شكل من الأشكال كانت؛ سواء شفهية أو مكتوبة أو معالجة أو الكترونية ... وغيرها، من مخاطر الوصول إليها أو استخدامها أو الكشف عنها أو تعطيلها أو تعديلها أو تخريبها بشكل غير المصرح به؛ بهدف ضمان استمرارية الأعمال والتقليل من المخاطر التجارية إلى الحد الأدنى وتعظيم العوائد على الإستثمارات وفرص الأعمال التجارية.

أنظمة المعلومات
ويقصد بها أي نظام محوسب يستخدم لإدارة ومعالجة أي معلومات تتعلق بالحكومة ضمن جهة واحدة أو عبر جهات متعددة.

معالجة المعلومات
هي أي نشاط يتم القيام به على المعلومات، بما في ذلك، على سبيل المثال لا الحصر، الإنشاء أو التعديل أو الحذف أو التخزين، أو النقل، أو النسخ، أو التشفير، أو فك التشفير ... إلخ.

مرافق معالجة المعلومات
ويعرف مرفق معالجة المعلومات بأنه أي نظام أو خدمة أو بنية تحتية، أو أي موقع فعلي يضم هذه الأشياء، وقد يكون المرفق نشاطاً أو مكاناً؛ وقد يكون ملموساً أو غير ملموس.

المصداقية
جزء من أحد أطراف ثالوث أمن المعلومات؛ وتعني أن البيانات لم يتم تعديلها، سواء عن قصد أو غير قصد، من غير الحصول على إذن.

جرد الموجودات
هي قائمة بالسلع والمواد التي تملكها الجهة – ويمكن أن يكون تسجيل قوائم الجرد على شكل سجل للأصول.

تسريب المعلومات
هو السماح بتسرب معلومات حساسة أو سرية لتصبح معروفة من قبل شخص غير مخول له استعراضها.

ضبط الدخول الإفتراضي
ويقصد به مجموعة من السياسات والإجراءات والهيكل التنظيمي للجهة وضوابط الدخول الإلكترونية (التقنية) المصممة لتمكين الوصول الآمن إلى برامج وملفات بيانات الحاسوب، وكذلك إلى الشبكة.

هجمات البرمجيات الخبيثة
محاولة للتسلل إلى نظام كمبيوتر من غير الحصول على موافقة مسبقة؛ بقصد جعل النظام غير متوافر، أو بقصد سرقة المعلومات أو استخدامها لمهاجمة أجهزة الحاسوب الأخرى بالاعتماد على برامج مؤذية أو شيفرات خبيثة (وهذا يشمل فيروسات الحاسوب والديدان وأحصنة طروادة وبرامج التجسس وبرامج الإعلانات الضارة وبرمجيات الجريمة والجذور الخفية، وغيرها من البرامج الضارة أو غير المرغوب فيها).

مكتب وسائط التخزين
مستودع تقني آمن تخزن فيه الإصدارات المصرح بها لنسخ البرامج والأقراص المدمجة وشرائط التخزين لحمايتها.

مفهوم «ضرورة الاطلاع»
وهو عملية إدارية تثبت أن فرداً معيناً يطلب الوصول إلى معلومات خاصة محددة لأداء واجباته المعينة.

مسارات الشبكة
عملية إختيار أفضل الطرق لانتقال المعلومات عبر شبكة معينة.

أجهزة مرور الشبكة
الأجهزة المستخدمة لتوصيل أجهزة الكمبيوتر أو الأجهزة الالكترونية الأخرى معاً للتواصل، مثل: الموزع، المودم، أو جهاز التوجيه.

عدم التنصل
عدم التنصل يعني ضماناً أنه لا يمكن لأحد الأطراف الذين لهم علاقة بمعاملة ما أن ينكر أنه قد تسلم المعاملة، كما لا يستطيع أن ينكر الطرف الآخر أنه قد أرسل معاملة ما. ومثال على عدم التنصل هو استخدام التوقيع الرقمي.

المعاملات عبر الإنترنت
برامج الجهة والبيانات والمعلومات الأخرى المتاحة أو التي يسمح بالوصول إليها باستخدام نظام متاح للجمهور، وعادة ما يكون ذلك عن طريق إستخدام الإنترنت.

ضوابط الدخول الفعلي
تعمل ضوابط الدخول الفعلي على مراقبة بيئة مكان العمل ومرافق الحاسوب وضبطها، وكذلك على مراقبة الدخول إلى هذه المرافق والخروج منها، وضبطها. ومثال على ذلك: الأبواب والأقفال والتدفئة وتكييف الهواء والدخان وأجهزة إنذار الحريق وأنظمة إخماد الحريق والكاميرات والحواجز والسياج وحراس الأمن وأقفال الأسلاك، وغيرها. ويعد فصل الشبكة ومكان العمل إلى مناطق وظيفية هو أيضاً أحد الضوابط الفعلية.

السياسة
وثيقة ذات صلة بأمن المعلومات تكتب وتحدث بصفة دورية، هدفها تقديم بيانات إدارية تتعلق بإجراء عملي رئيسي لأمن المعلومات من خلال وضع القواعد للسلوك

المتوقع من قبل المستخدمين ومسؤولي الأنظمة والإدارة وأفراد الأمن؛ ومن خلالها يتم تفويض موظفي الأمن بالمراقبة والتحقق من إجراء التحقيقات، وكذلك التعريف والموافقة على اتخاذ الإجراءات ضد أي انتهاك، وتحديد الخط القاعدي الموافق عليه من قبل الجهة بما يخص الأمن. كما تساعد في تقليل المخاطر، وتتبع الامتثال للأنظمة والتشريعات.

الخصوصية
هي قدرة الفرد أو المجموعة على وضع حد من أن تصبح المعلومات عن أنفسهم معروفة لأشخاص آخرين غير الذين يختارونهم لإعطاء هذه المعلومات.

العملية/الإجراء
وهو وثيقة ذات صلة بأمن المعلومات ترفق مع السياسة، وتكتب لتقديم الإرشادات خطوة بخطوة حول «كيفية» تنفيذ بيانات السياسة.

نقطة التعافي المستهدفة
هو الحد الأقصى المسموح للفترة التي يمكن أن تضيع فيها البيانات من خدمات تكنولوجيا المعلومات بسبب وقوع حادث كبير.

زمن التعافي المستهدف
مدة الوقت التي يجب خلالها استعادة العمل بعد وقوع كارثة (أو تعطيل)، تجنباً لعواقب غير مقبولة مرتبطة بانقطاع استمرارية العمل.

المخاطر المتبقية
المخاطر المتبقية بعد معالجة المخاطر أو تنفيذ استجابة المخاطر، كما وافقت عليها الإدارة.

المخاطر
وهي الأضرار المحتملة القابلة للقياس، والتي قد تنشأ عن أحداث مستقبلية.

قبول المخاطر
يصف قبول المخاطر قراراً مدروساً لقبول نتائج واحتمالات وقوع مخاطر معينة.

تحليل المخاطر
يمثل تحليل المخاطر آلية لتحديد وتقييم العوامل التي قد تعرض نجاح مشروع معين للخطر أو تمنع تحقيق هدف ما. وتساعد هذه الآلية في تحديد التدابير الوقائية

اللازمة للحد من معدل احتمال حصول هذه العوامل، وكذلك تحديد التدابير المضادة للتعامل بنجاح مع هذه المخاطر عند نشوئها تفادياً للآثار السلبية المحتملة على الجهة.

تقييم المخاطر

وهي خطوة من خطوات عملية إدارة المخاطر تحدد القيمتين؛ النوعية والكمية للمخاطر، في ما يتصل بتهديد معروف. ويتطلب تقييم المخاطر الكمية إجراء عمليات حسابية لعنصرين من عناصر المخاطر؛ وهما حجم الخسارة المحتملة ومعدل احتمال حدوث الخسارة.

إدارة المخاطر

هي عملية تحليل للمخاطر ودرجة التعرض لها من خلال تحديد الأولويات وتقييمها، متبوعاً بالمراقبة وتطبيق الضوابط لتنفيذ المعالجة الأفضل للتعرض.

معالجة المخاطر

وتصف معالجة المخاطر – والتي تعرف أيضاً بضبط المخاطر– جزءاً من إدارة المخاطر؛ حيث تتخذ فيها القرارات حول كيفية التعامل مع المخاطر التي جرى تحديدها سابقاً وتوضع الأولويات. قد تتضمن خيارات معالجة المخاطر؛ خيار تفاديها، أو الحد منها أو نقلها أو قبولها.

الأمن أو هندسة أمن المعلومات

يصف الهيكل والمكونات والبنية (التوصيل والتنسيق) من عناصر الضوابط الأمنية داخل البنية التحتية لتقنية المعلومات في المؤسسة. وتظهر بنية الأمن أو الإطار كيف يتم تنفيذ الدفاع وكيف ترتبط مستويات السيطرة في تنفيذ الضوابط الأمنية في بيئة تقنية المعلومات في الجهة.

الاختراق الأمني

يعد الاختراق الأمني فعلاً خارجياً يتجاوز السياسات أو الممارسات أو الإجراءات الأمنية أو يتعارض مع أي منها.

الضوابط الأمنية

وهي الضمانات أو التدابير المضادة المتخذة لتفادي المخاطر الأمنية أو للتصدي لها أو للتقليل منها. وقد تكون هذه الضوابط وقائية أو بحثية أو تصحيحية.

التدابير الأمنية

تدابير وقائية تؤخذ تجاه خطر أو ضرر ممكن وقوعه.

فصل المهام
ويهدف فصل المهام، بوصفه مبدأ من مبادئ الأمن، بصورة أساسية إلى منع التحايل ووقوع الأخطاء، ويتحقق هذا الهدف من خلال توزيع المهام والمزايا المرتبطة بإجراءات عمل محددة بين عدة مستخدمين.

الإدارة العليا
أحد أعلى مستويات الإدارة في الجهة وتتألف من شخص واحد أو مجموعة من الأشخاص المسؤولين عن توجيه المؤسسة وإدارتها. وتشمل الأمثلة عن ذلك مجلس الإدارة/المدير العام/رئيس مجلس الإدارة.

أصحاب المصلحة
شخص أو مجموعة أو منظمة لها اهتمام أو مصلحة في منظمة ما. ويمكن أن يؤثر أصحاب المصلحة على إجراءات المنظمة وأهدافها وسياساتها أو يتأثرون بها

دورة إقتناء/تطوير النظم
عملية شراء أو إنشاء أو تغيير نظم المعلومات، والنماذج والمنهجيات التي يستخدمها الأشخاص لتطوير هذه النظم.

النص المصدري للبرامج
أي مجموعة من التعليمات مكتوبة باستخدام لغة الكمبيوتر.

الأمان حسب التصميم
هو نهج للأمن السيبراني يتيح للجهة وضع ضوابط ذاتية لأمن البيانات وإضفاء الطابع الرسمي على تصميم بنيتها التحتية، ما يتيح لها بناء الجانب الأمني في عمليات إدارة تكنولوجيا المعلومات الخاصة بها. ويركز هذا النهج على الوقاية من الاختراقات السيبرانية بدلاً من معالجة المشكلة واستعادة الأنظمة بعد وقوع الاختراق.

الأصول
تعني أي عنصر يحمل قيمة مهمة للجهة، وتشمل أنواع الأصول: (أ) المعلومات؛ (ب) البرمجيات مثل برامج الحاسوب؛ (ت) الأصول المادية مثل الحاسوب؛ (ث) الخدمات؛ (ج) الأفراد وما إلى ذلك.

أصول المعلومات
تشمل المعلومات والموظفين والأجهزة والنظم والمرافق التي تتيح للمنظمة تحقيق أغراض العمل.

التدريبات السيبرانية
تُقيم الجهة هذه التدريبات المخطط لها لمحاكاة الهجمات السيبرانية وحوادث أمن المعلومات وغيرها من أنواع الاضطرابات. وتهدف التدريبات إلى اختبار القدرات السيبرانية للجهة من خلال قياس مدى قدرتها على اكتشاف الحوادث الأمنية والاستجابة لها.

التهديد
التهديد هو احتمال واضح لوقوع حدث ضار مثل هجوم ما. وقد يأتي التهديد من طرف ما مع توافر القصد والقدرة لديه على استغلال الضعف في أحد الأصول؛ مثل متطفل ضار أو موظف ساخط.

المستخدم
فرد أو عملية (نظام) تمتلك التصريح اللازم للوصول إلى المعلومات أو نظام المعلومات.

التقنيات الافتراضية
صنع نسخة افتراضية من شيء ما في عالم الحواسيب، مثل أجهزة الحاسب الآلي، ونظام التشغيل، وجهاز التخزين، أو موارد الشبكة. ويمكن أن ينظر إليه باعتباره جزءاً من الكيان الكلي لبيئة تكنولوجيا المعلومات.

الضعف
وهو ضعف في أحد الأصول التي يمكن استغلالها.

البيانات الاصطناعية
هي بيانات مصطنعة يتم إنشاؤها بناءً على البيانات الأصلية، وتشبه البيانات الأصلية في بعض خصائصها الإحصائية

إخفاء البيانات
تُستخدم هذه التقنية لإنشاء نسخة من البيانات تبدو مشابهة في هيكلها للمعلومات الأصلية، ولكنها في الواقع تخفي المعلومات الحساسة.

معلومات التهديدات
عملية تحديد تهديدات المعلومات/التهديدات السيبرانية وتحليلها. ويمكن أن يشير مصطلح «معلومات التهديدات» إلى البيانات التي تم جمعها عن تهديد محتمل، أو عملية جمع هذه البيانات ومعالجتها وتحليلها لفهم التهديدات بشكل أفضل.

الخدمات الرقمية
تشمل الخدمات الحكومية أو غير الحكومية المقدمة للعملاء من خلال القنوات الرقمية

القنوات الرقمية
تشير إلى المواقع الإلكترونية والتطبيقات الذكية وغيرها من الوسائط التي تتوفر من خلالها الخدمات الرقمية المقدمة

حادثة شديدة الخطورة
فقدان سرية المعلومات أو مصداقيتها أو توافرها مما قد يسبب تأثيراً سلبياً خطيراً أو كارثياً على العمليات التشغيلية أو أصول الجهة أو الأفراد أو مصالح الأمن القومي.

مركز عمليات الأمن السيبراني
وظيفة مركزية داخل الجهة توظف الموظفين، والعمليات، والتقنيات لمراقبة الوضع الأمني للجهة وتحسينه باستمرار، إلى جانب الوقاية من حوادث الأمن السيبراني والكشف عنها وتحليلها والاستجابة لها.

منهجية الثقة المعدومة
تشير إلى استراتيجية للأمن السيبراني تتبع مبدأ التحقق الدائم وانعدام الثقة، وتشتمل على تطبيق سياسة الأمان بناءً على السياق الذي يتم إنشاؤه من خلال ضوابط الوصول ذات الامتيازات الأقل والمصادقة الصارمة للمستخدمين والأجهزة، وليس بناءً على الثقة المفترضة.

حكومة دبي
GOVERNMENT OF DUBAI

مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER

DESC2409PP31V2