مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER

حكومة دبي
GOVERNMENT OF DUBAI

استراتيجية دبي للأمن الإلكتروني

تعزيز مكانة دبي كمدينة عالمية رائدة
في الابتكار والسلامة والأمن

استراتيجية دبي للأمن الإلكتروني

النسخة ١.٠

صاحب السمو الشيخ محمد بن راشد آل مكتوم

نائب رئيس دولة الإمارات
رئيس مجلس الوزراء حاكم دبي

لم تكن التحديات يوماً، ولن تكون، رادعةً لطموحاتنا لمستقبل دولة الإمارات مع إصرارنا على تحويل أي تحدي إلى فرصة للإبداع والابتكار والإتيان بأفكار ومبادرات تدفع جهودنا قُدُماً نحو تحقيق أهدافنا.

وتأتي "استراتيجية دبي للأمن الإلكتروني" كإضافة نوعيّة إلى سجل الانجازات الحكومية، في ضوء حرصنا الدائم على مضاعفة العمل لضمان استمرارية النجاح والتميز.

أشكر كل من ساهم في وضع هذه الاستراتيجية لتكون عوناً جديداً يدعم تطلعاتنا لإحراز أرقى درجات التميز والريادة، وبرهاناً لعزمنا استكمال مسيرة البناء والتطوير لينعم شعب الإمارات دائماً بالسعادة والرخاء.

ثقتنا كبيرة في إمكانيات القطاعين الحكومي والخاص في إنجاح هذه الاستراتيجية وأدعو الجميع لمضاعفة العمل والجهد لترسيخ مكانة دولة الإمارات بين أكثر الدول الآمنة إلكترونياً في العالم.

سمو الشيخ محمد بن راشد آل مكتوم

سمو الشيخ حمدان بن محمد بن راشد آل مكتوم

ولي عهد دبي
رئيس المجلس التنفيذي

”إن تاريخاً جديداً لدبي
تحت التنفيذ بتوقيع
محمد بن راشد آل مكتوم“

سمو الشيخ حمدان بن محمد بن راشد آل مكتوم

تعزيز مكانة دبي كوجهة رائدة للابتكار والأمن الإلكتروني

تعد دبي مركزاً دولياً رائداً ووجهة إقليمية جاذبة لأنشطة المؤسسات المحلية والإقليمية والدولية، تجذبها ريادة تكنولوجية تشكل أهم ركائزها، وساهمت الثورة التكنولوجية الهائلة التي تشهدها المنطقة حالياً في جعل الإمارة محور اهتمام جميع دول العالم.

لا تتحقق الغاية من التطور التكنولوجي في غياب أطر راعية تعزز أمن أنظمة المعلومات والبيانات وتضمن سلامتها، لذا فإن إقامة حيز موثوق وآمن في الفضاء الإلكتروني يعد أمراً جوهرياً لمواصلة التطور ومواجهة التحديات المستقبلية.

يأتي إطلاق خطة دبي الاستراتيجية للأمن الالكتروني توافقاً مع رؤية صاحب السمو الشيخ محمد بن راشد آل مكتوم نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي (رعاه الله) بجعل دبي أكثر مدن العالم أمناً إلكترونياً.

تحيط الخطة قواعد البيانات والأنظمة الإلكترونية بالضوابط الحامية من الأخطار والاعتداءات، وتحمي المستخدمين، أفراداً وشركات، وكل من يرتبط بتكنولوجيا المعلومات ارتباطاً وثيقاً.

إنَّ مسار التحول إلى مجتمع ذكي مليء بالتحديات، لكنه لن يحول دون تحقيق أهدافنا، وسنواصل العمل الجاد بإصرار ومثابرة تعلمناها من قدوتنا وقادتنا في الدولة، وسنجعل دبي واحة أمان إلكتروني وفقاً للرؤية الرشيدة لصاحب السمو الشيخ محمد بن راشد آل مكتوم.

تعد التوعية الأمنية الإلكترونية عنصراً أساسياً من عناصر نجاح الاستراتيجية، وترمي إلى بناء مجتمع معلوماتي آمن وأكثر إدراكاً لمخاطر الأمن الإلكتروني.

من الأهداف الرئيسية الأخرى لهذه الاستراتيجية الحد من مخاطر الشبكة ومكافحة أي اختراقات لها وتمكين المستخدمين أفراداً ومؤسسات من الوصول إلى تقنيات المعلومات المختلفة بما يدعم نجاح الاستراتيجية مستقبلاً.

يتوقف بلوغ هذه الأهداف على تعاضد القطاعات الحكومية والخاصة وتعاونهما، فلنعمل جميعاً بروح الفريق الواحد، بهدي توجيهات صاحب السمو الشيخ محمد بن راشد، بهدف وضع أسس عالم إلكتروني يتسم بالحرية والأمان، ويشجّع على البحث العلمي والابتكار.

سعادة يوسف الشيباني
المدير التنفيذي لمركز دبي للأمن الإلكتروني

1 المقدّمة

للتطور التكنولوجي أثر كبير على كافة قطاعات المجتمع، بدءًا من القطاع العام والخاص ووصولاً إلى الأفراد، حيث يتم الاعتماد على تكنولوجيا المعلومات والاتصالات في معظم نواحي الحياة الاجتماعية والاقتصادية، وتتجلى أهمية العالم الافتراضي في ما يوفره من انفتاح وحرية تسهم في إزالة الحواجز أمام التجارة الداخلية والخارجية، وبين الدول والمجتمعات والأفراد ويسمح بتبادل المعلومات في جميع أنحاء العالم، لذا لا بدّ من توفير بنية تحتية آمنة لمواجهة مخاطر الهجمات الإلكترونية التي تحد من فعالية عمل الأفراد والمؤسسات العامة والخاصة.

ونظراً للمكانة العالمية التي تشغلها إمارة دبي فقد أصبحت هدفًا رئيسيًّا للهجمات الإلكترونية التي تؤثر على أعمال القطاع العام والخاص وعلى مستوى الأفراد، وتشير الإحصاءات إلى ارتفاع الخسائرالناجمة عن الهجمات الإلكترونيّة والتي تتطوّر بشكل سريع.

وتشكل خطة دبي ٢٠٢١ منظورة شاملة ومتكاملة لمستقبل الإمارة؛ بدءاً من الفرد والمجتمع ووصولاً إلى ما يتعلق بالبنية التحتية أو ما يتعلق بالتجربة الحياتية التي يعيشها أفراد المجتمع من مواطنين أو مقيمين أو زوار سواءً في تفاعلهم فيما بينهم، أو مع عناصر البنية الحضرية والخدمات المرتبطة بها اجتماعية كانت أم اقتصادية، وتتوافق استراتيجية المركز مع غايات خطة دبي٢٠٢١، وتحديدًا الغاية الآتية:

"الأكثر أمناً: تحظى دبي بانطباع إيجابي للغاية لدى مواطنيها وساكنيها وزائريها باعتبارها مدينة آمنة للعيش والإقامة والعمل، وبقدرة الأجهزة المختصة فيها على التعامل بكفاءة وحرفية عالية وشفافية مع كل ما يخص أمن الفرد أو المجتمع."▲

▲ Dubai Plan 2021, "The Experience", Aim 3

وصدر القانون رقم (١١) لسنة ٢٠١٤ بشأن إنشاء مركز دبي للأمن الإلكتروني بهدف تطوير استخدام الوسائل اللازمة في مجال أمن المعلومات ووضع المعايير الكفيلة بتوفير الأمن الإلكتروني في الإمارة والإشراف على تنفيذها وإعداد خطة استراتيجية لمواجهة أي مخاطر أو تهديدات أو اعتداءات على المعلومات.

وأصدر المركز هذه الاستراتيجية لحماية إمارة دبي من مخاطر الفضاء الالكتروني ودعم نموّ الإمارة وابتكارها واقتصادها. وتوضح هذه الاستراتيجية الإجراءات اللازمة للحدّ من المخاطر وبناء مجتمع واع بمخاطر الأمن الإلكتروني لتوفير بنية تحتية آمنة للمؤسسات والأفراد، بما يدعم نجاحها في المستقبل، وقد تمّ تحديد مدّة خمس سنوات كجدول زمني لتحقيق أهداف هذه الاستراتيجية.

ويوضح الشكل التالي كيفيّة ارتباط مختلف محاور هذه الاستراتيجية مع بعضها البعض.

2 دواعي الاستراتيجية

يتعلق هذا القسم بفرص النموّ والابتكار في الفضاء الإلكتروني وما يهدده من مخاطر.

1.2 الاتصال العالمي

تخطت نسبة استخدام ▲ الإنترنت في دولة الإمارات العربية المتّحدة ٩١٪ في ديسمبر ٢٠١٦، ويشهد الاقتصاد الإلكتروني نموًّا سريعًا، وتقوم التطورات التكنولوجية الجديدة مثل الحوسبة السحابية وإنترنت الأشياء (IoT) والمدن الذكية جميعها على ترابط الفضاء الإلكتروني.

ولذلك من المتوقع أن تزيد نسبة استخدام سكان دولة الإمارات العربية المتّحدة لشبكة الانترنت، وتستفيد المؤسسات العامة والخاصة أيضًا من التقدّم التكنولوجي في مجال الإنترنت والهاتف المحمول من خلال تقديم منتجات وخدمات مصمّمة خصّيصًا وفقًا لاحتياجات الأفراد.

وبالإضافة إلى اتّساع نطاق الاتّصال بشبكة الإنترنت، لم تعد ثمّة أيّ قيود فعلية أمام ارتباط الأشياء والأشخاص في العالم الافتراضي وذلك باستخدام التبادل الآمن للمعلومات والاتّصالات في الفضاء الإلكتروني، حيث يخلق هذا الارتباط "مجتمع معلومات متماسك" يندمج فيه العالم الفعليّ والافتراضي أكثر، ويمكّن إمارة دبي ومواطنيها من ابتكار مستوى جديد من المنتجات والخدمات.

ولا يمكن تقديم منتجات وخدمات مبتكرة إلا في فضاء إلكتروني آمن ومرن يدعم بدوره الأعمال والازدهار الاقتصادي للأفراد والمؤسسات، ولتحقيق ذلك يركّز مركز دبي للأمن الإلكتروني على تنفيذ هذه الاستراتيجية كأحد أولويات المركز لحماية المؤسسات العامة والخاصة في الإمارة، والأفراد من الجرائم الإلكترونية والمخاطر التي تهدّد الأمن الإلكتروني.

2.2 تهديدات ومخاطر العالم الإلكتروني

تنتج عن أعمال القرصنة والهجمات الالكترونية عدة تهديدات من أهمها:

الاحتيال
التجسّس
انتهاك الخصوصية
الإرهاب
التشهير

▲ http://www.internetworldstats.com/me/ae.htm

وتشكّل هذه التهديدات خطرًا على عمل المؤسسات العامة والخاصة، والأفراد مستخدمي شبكات الانترنت والتواصل في الإمارة.

بالإضافة إلى ذلك، تشكّل دولة الإمارات العربية المتّحدة هدفاً لأعمال القرصنة؛▲حيث شهد عام ٢٠١٦ خسارة بقيمة ٥,١٤ مليار درهم بسبب الجرائم الإلكترونية.

وتشير الإحصائيات الصادرة عن شرطة دبي إلى الزيادة المستمرّة للهجمات الإلكترونية في إمارة دبي؛◆حيث أنه واحد من أصل خمسة من سكان الإمارة وقع ضحيّة للجرائم الإلكترونية خلال عام ٢٠١٥، وارتفع عدد تقارير الإبلاغ عن الجرائم الإلكترونية بنسبة ٢٣ في المائة خلال عام ٢٠١٦، ومن المتوقّع أن تزداد هذه المعدلات بشكل أسرع حتى العام ٢٠٢٠.

ويهدف مركز دبي للأمن الإلكتروني■ وفقاً لقانون إنشائه لمكافحة الجرائم الإلكترونية وأعمال القرصنة وتطوير الحلول التقنية اللازمة للحد منها.

▲ http://gulfnews.com/business/sectors/technology/cybercrime-cost-uae-dh5-14b-this-year-1.1933736

◆ http://www.arabianbusiness.com/dubai-cybercrime-rises-23-percent--621167.html

■ http://gulfnews.com/news/uae/government/cyber-security-centre-established-in-dubai-1.1346144

3 المبادئ الرئيسية

تتعدد المبادئ الرئيسية التي يجب الاستناد إليها لتحقيق غايات هذه الاستراتيجية، ومنها:

1.3 التبادل الآمن للمعلومات

يجب أن يتمتع كل شخص بحق الوصول إلى الفضاء الالكتروني من خلال التقنيات المتاحة حول العالم، ويجب أن يبقى هذا الفضاء الإلكتروني منفتحًا للابتكار والتبادل الآمن للأفكار والمعلومات والآراء، وذلك يتطلب حماية للمعلومات المستخدمة ومصداقيتها وأن يتم تبادل تلك المعلومات في إطار قانوني.

كما يجب احترام خصوصية الأفراد وتوفير الحماية المناسبة للملكية الفكرية، لذا لابد من تحقيق التوازن بين الانفتاح التكنولوجي وخصوصية الافراد، إلى جانب ذلك يجب توفير بيئة تنافسية في الفضاء الإلكتروني تضمن عائد مقبول على الاستثمار في البنية التحتية والخدمات والمعلومات، وتدعم مبادرة بيانات دبي التي تديرها مؤسّسة بيانات دبي التبادل الآمن للمعلومات في الإمارة وتضمن تبادل البيانات بين مختلف الجهات الحكومية والخاصة والمستثمرين والمقيمين والزوار.

"لا ينصبّ التركيز على جمع البيانات، بل على تحقيق الاستفادة المثلى منها وخلق تجارب متميّزة لكافة أفراد المجتمع"

صاحب السموّ الشيخ محمد
بن راشد آل مكتوم

يحدّد دليل بيانات دبي المبادئ التوجيهية التي يجب على الجهات الحكومية في إمارة دبي اتّباعها لإدارة البيانات، تماشيًا مع التزام حكومة دبي في تطوير الخدمات التي تركز على المستخدم وتعتمد على البيانات.

وتعتمد رؤية دبي على التبادل الآمن للمعلومات، حيث تعمل مؤسسات القطاع العام على تحويل إمارة دبي إلى المدينة الأذكى والأسعد في العالم، وسيتاح لكل من المؤسسات العامة والخاصة والمواطنين والمقيمين والزوار تبادل البيانات والمعلومات وتطوير طرق جديدة ومبتكرة للعيش والتعلّم والقيام بالأعمال في ثقافة قائمة على التبادل الآمن للبيانات.

2.3 تقييم المخاطر

يجب أن يعي مستخدمي شبكة الانترنت بأن توفير الحماية والأمن الإلكتروني المطلق أمر غير متصور تحقيقه، ولكن ينبغي أن يتوافر لديهم الوعي والإدراك والدراية كاملة بالمخاطر التي من الممكن أن تواجههم. والتقييم الاحترازي للمخاطر هو هدف أساسي من نظام أمن المعلومات (ISR) المعمول به في إمارة دبي.

ويُعتبر تنفيذ هذا النظام إلزاميًّا بالنسبة لمؤسسات القطاع العام في إمارة دبي، ويوصى بتطبيقه في مؤسسات القطاع الخاص أيضًا، أو بتطبيق أنظمة مماثلة (بما يناسب متطلبات العمل)، مثل معايير الأيزو ٢٧٠٠١ أو معايير NESA UAE IAS، وتجدر الإشارة إلى أنّ كل الأنظمة المذكورة أعلاه تركز بشكل مماثل على تقييم المخاطر، وتخضع لآليات تقييم متوافقة، وحيث أن قطاع الأفراد لا يمكنه تطبيق آلية تقييم المخاطر لذلك ستعالج استراتيجية دبي للأمن الالكتروني للأمن الإلكتروني المخاطر التي يواجهها ذلك القطاع وذلك في محور "مجتمع واع بمخاطر الأمن الإلكتروني".

3.3 التعاون

أصبح من الصعب إدارة أمن الفضاء الإلكتروني من قبل مدينة واحدة أو دولة واحدة في العالم وذلك نتيجة لارتباطه بمستويات عدة ومختلفة، ويجب على المؤسسات العامة والخاصة والأفراد في إمارة دبي العمل جنبًا إلى جنبٍ وينبغي على جميع العاملين في مجال الفضاء الإلكتروني بما في ذلك المؤسسات المصنّفة ضمن برنامج حماية البنية التحتية للمعلومات الحيوية (CII) العمل ضمن رؤية مشتركة للأمن الإلكتروني والقيام بمسؤولياتهم لتحقيق الأمن والمرونة في الفضاء الإلكتروني (وسيتم مناقشة هذا الموضوع بشكلٍ مفصل في القسم ٤,٤ أدناه).

وتتجاوز الخطورة التي قد تنجم عن استخدام الفضاء الالكتروني حدود الامارة، الأمر الذي يتطلب معه وجود شراكات مع إمارات ودول ومبادرات أخرى إقليمية ودولية، حيث أن الجهود الفردية أو على مستوى الإمارة أو الدولة وحدها لا يُمكن معها السيطرة على تلك المخاطر باعتبار أن عمليات القرصنة تتم في كل أنحاء العالم.

"متى كانت الرؤية واضحة سهل تطبيق الأهداف."

الشيخ محمد بن راشد آل مكتوم

ويمكن للدول مواجهة التهديدات من خلال تحسين التعاون بين فرق الاستجابة لطوارئ الحواسيب (CERTs) وتضافر الجهود في الشؤون الدبلوماسية الدولية، ويمكن استخدام المعايير الدولية مثل معيار الأيزو ٢٧٠٠١ لدعم التعاون، والتي ترتبط بشكلٍ وثيق مع نظام أمن المعلومات المعمول به في إمارة دبي، والاستفادة من التعاون الدولي في مجال تنسيق الأعمال في المسائل القانونية.

4.3 الامتثال للتشريعات

يلزم استكمال البناء التشريعي في مجال الفضاء الالكتروني ووضعها موضع التنفيذ بما يكفل

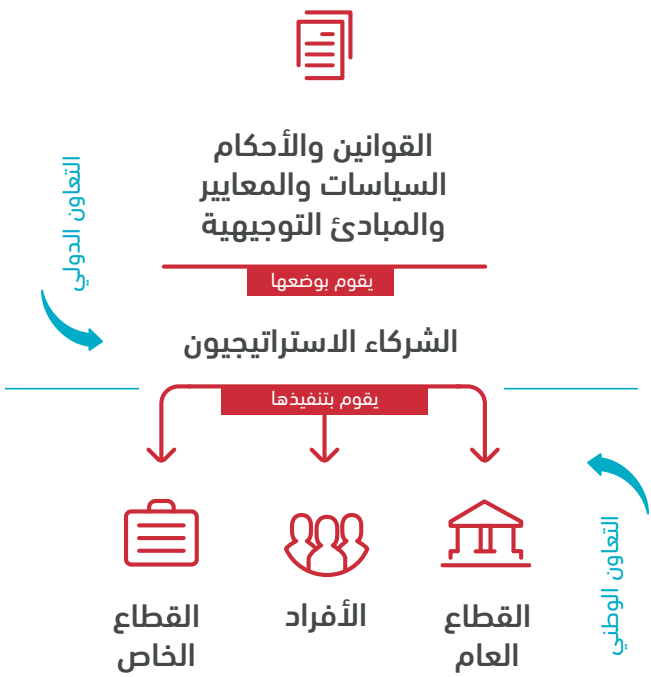
تحقيق غايات الأمن الالكتروني، والعمل على تعزيز المعرفة والوعي لدى كافة شرائح المجتمع بأهمية هذه القوانين إلى جانب أهمية الامتثال لها، ومن التشريعات التي تم الاستناد إليها عند وضع هذه الاستراتيجية مايلي:

- القانون الاتحادي رقم (٧) لسنة ٢٠٠٢ في شأن حقوق المؤلف والحقوق المجاورة
- القانون الاتحادي رقم (١) لسنة ٢٠٠٦ في شأن المعاملات والتجارة الالكترونية
- مرسوم بقانون اتحادي رقم (٥) لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات
- القانون رقم (٤) لسنة ٢٠١٦ بشأن مركز دبي للأمن الاقتصادي
- قرار المجلس التنفيذي لحكومة دبي رقم (١٣) لسنة ٢٠١٢ بشأن أمن المعلومات في حكومة دبي

يجب وضع القواعد والمعايير الدولية بما يتّفق مع القيم العالمية إذ لا يقتصر الفضاء الإلكتروني على إمارة دبي فحسب بل يتسع نطاقه ليشمل جميع أنحاء العالم، وستتمّ مناقشة هذا الموضوع بالتفصيل في محور "التعاون المحلي والدولي أدناه".

5.3 هيكلة الأمن الإلكتروني

يجب على المعنيين العمل معًا لتوفير الخطة الاستراتيجية للأمن الإلكتروني للمؤسسات العامة والخاصة، والأفراد في إمارة دبي. وتُظهر هيكلة الأمن الإلكتروني أدناه المسؤوليات المختلفة في البرنامج العام للأمن الإلكتروني:



4 محاور الاستراتيجية

تستند خطة دبي الاستراتيجية للأمن الالكتروني على تنفيذ مجموعة من المحاور الرئيسية لخلق فضاء إلكتروني آمن.

مجتمع واع بمخاطر الأمن الإلكتروني

بناء الوعي والمهارات والقدرات اللازمة لإدارة مخاطر الأمن الإلكتروني في المؤسسات العامة والخاصة والأفراد في إمارة دبي.

الإبتكار

تشجيع الابتكار والبحث العلمي في مجال الأمن الإلكتروني، وإنشاء فضاء إلكتروني يتّسم بالحريّة والعدل والأمن ويشجّع الابتكار في إمارة دبي.

أمن الفضاء الإلكتروني

وضع ضوابط لحماية سرية البيانات ومصداقيّتها وتوفّرها وخصوصيتها للمؤسسات العامة والخاصة والأفراد في إمارة دبي.

الحفاظ على مرونة الفضاء الإلكتروني

العمل على ضمان استمرارية أنظمة تكنولوجيا المعلومات وتوفّرها في الفضاء الإلكتروني.

التعاون المحلي والدولي

التعاون مع القطاعات المختلفة المحلية والعالمية لإدارة مخاطر الفضاء الالكتروني.

ستقوم الجهات المعنية في إمارة دبي بتنفيذ هذه الاستراتيجية والعمل معًا لتحقيق الأهداف المفصّلة في الأقسام أدناه والرامية لخق فضاء إلكتروني آمن في الإمارة.

مجتمع واع بمخاطر الأمن الالكتروني

يهدف هذا المحور إلى التأكد من بناء مجتمع يعي ويدرك مخاطر الأمن الإلكتروني، حيث يشمل توفير التدريب للعاملين في القطاعات العامة والخاصة في إمارة دبي، وتوفير برامج توعية للأطفال والطلاب وغيرهم من الأفراد، لزيادة معرفتهم بالأمن الإلكتروني.

"المستقبل سيكون لأصحاب الأفكار والابتكار."
الشيخ محمد بن راشد آل مكتوم

1 وجود موظفين من أصحاب المعرفة والخبرة في مجال الأمن الإلكتروني في القطاعات العامة والخاصة

ينبغي تشجيع المؤسّسات (في القطاع العام والخاص) على بناء قوة عاملة تتمتع بالمعرفة الكافية بالأمن الإلكتروني لأداء الأدوار والمسؤوليات ذات الصلة، ومن المهم أن تكون هذه القوى العاملة موجودة للاستجابة للحوادث وحماية المؤسّسة، ويجب اتّخاذ تدابير مسبقة في ما يخص تهديدات الأمن الإلكتروني ودعم هذه القوى العاملة من خلال توفير الدورات التدريبية والمؤتمرات وورش العمل، وقياس نتائجها.

2 توفير البرامج التوعوية الخاصة بالأمن الإلكتروني لموظفي القطاع العام والخاص

يجب على المؤسّسات تقديم برامج توعوية شاملة تتناول مسؤوليات كلّ الموظفين، بما فيهم الموظفين الجدد تجاه الأمن الإلكتروني، وأهمية دعمهم، والمخاطر المترتبة على انتهاك السياسات والإجراءات ذات الصلة.

وتشمل هذه الدورات التهديدات والمخاطر المرتبطة بالأمن الإلكتروني وتدابير الحماية اللازمة وذلك بناء على مسؤوليات الموظفين وأدوارهم الوظيفية.

3 توفير التوعية الخاصة بالأمن الإلكتروني للأفراد

يزداد عدد الأشخاص الذين يتعرضون للهجمات الإلكترونية، ومن المتوقع ارتفاع هذا العدد مع الاعتماد المتزايد على التكنولوجيا في حياتنا اليومية.

يجب على المدارس والجامعات والمؤسسات الأخرى توفير دورات وحملات توعوية بالأمن الإلكتروني والتهديدات والمخاطر المرتبطة بالفضاء الإلكتروني، وتطوير حملات توعوية مختلفة وتنظيمها بحيث تكون موجهة إلى الفئات المختلفة لبناء مجتمع واعٍ بمخاطر الأمن الإلكتروني، والاستفادة مما يقدمه المركز والمؤسسات الأخرى لتعزيز المعرفة بالأمن الإلكتروني ودورهم تجاهه.

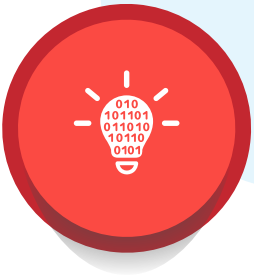
4 زيادة مهارات الخبراء في الأمن الإلكتروني

يجب على مؤسسات القطاع العام والمدارس والجامعات في إمارة دبي تطوير خطة لزيادة عدد الخبراء في مجال الأمن الإلكتروني ويجب على المدارس والجامعات إدراج الأمن الإلكتروني في مناهجها الدراسية، من خلال إضافة مقررات متخصصة في مجال الأمن الالكتروني.

كما يجب أن تعمل الجامعات مع المؤسسات لوضع خطة لزيادة عدد الخبراء في الأمن الإلكتروني، وتحفيز الأشخاص لزيادة معرفتهم في مجال الأمن الالكتروني.

كما يجب توفير برامج تدريبية للعاملين في المؤسسات لزيادة المعرفة بالأمن الإلكتروني، ويمكن أيضاً وضع نظام لإصدار الشهادات للمختصين في الأمن الإلكتروني، باستخدام معايير الأيزو ٢٧٠٢١ على سبيل المثال.

ويجب أيضاً السعي للتعاون مع المؤسسات الأخرى لتطوير المنتجات والخدمات ذات الصلة بالأمن الإلكتروني، وإدراجها في الأنشطة التعليمية في المدارس والجامعات، كتنظيم المحاضرات الخاصة بالأمن الالكتروني.



الإبتكار

يهدف هذا المحور إلى تطوير أنشطة البحث ومراحل تصميم التقنيات الجديدة واستحداث أنظمة حديثة لإصدار الشهادات للمنتجات والأشخاص لضمان تحقيق الأمن الالكتروني في الابتكارات ذات الصلة.

"الابتكار رحلة مستمرة لا تنحصر في وقت ولا تقف عند حدود الزمن."

الشيخ محمد بن راشد آل مكتوم

1 تعزيز أنشطة البحث والتطوير التي تدعم الأمن الإلكتروني

أصبحت التهديدات والمخاطر المرتبطة بالفضاء الإلكتروني أكثر تعقيدًا مع التطورات التقنية، لذلك يجب أن توفر أنشطة البحث والتطوير أفضل التقنيات الممكنة في مجال الأمن الإلكتروني.

ويجب على المؤسسات العامة والخاصة في إمارة دبي تعزيز أنشطة البحث والتطوير، والعمل على تحقيق الآتي:

- اعتماد القوانين والأحكام.
- إدراج الأمن الالكتروني في مرحلة تصميم المنتجات والخدمات.
- تشجيع البحوث متعددة التخصصات.
- إتباع آليات مراقبة ورصد متقدّمة.
- استخدام التقنيات الحديثة، مثل الذكاء الاصطناعي لزيادة القدرات الدفاعية.

الاستفادة من التعاون مع القطاعات المختلفة المحلية والعالمية

2 اعتماد الأمن الإلكتروني في التقنيات الجديدة

تتيح التقنيات الجديدة مثل إنترنت الأشياء (IoT) أو المدن الذكية إمكانيات جديدة لإمارة دبي، ولكنها قد تشكل خطراً أيضاً في حال استخدامها لأعمال القرصنة.

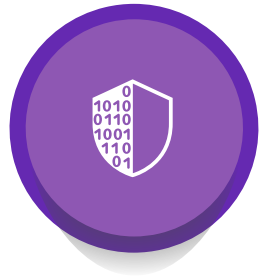
لذلك يجب على مؤسسات القطاع العام في إمارة دبي خلق لذلك يجب على مؤسسات القطاع العام في إمارة دبي خلق أنظمة آمنة وإدراج مجال الأمن الإلكتروني باعتباره جزءًا لا يتجزأ من التصميم لإنتاج أجهزة خاصة بإنترنت الأشياء وكذلك عند تطوير تقنيات المدن الذكية.

وينبغي دعم ذلك من خلال خطة تحفيزية تكافئ المؤسسات التي تتناول موضوع الأمن الإلكتروني في منتجاتها.

3 وضع خطط جديدة لإصدار الشهادات في مجال الأمن الإلكتروني

يجب على مؤسسات القطاع العام في إمارة دبي استحداث خطط جديدة لإصدار الشهادات التي تتناول موضوع الأمن الإلكتروني في التقنيات الجديدة أو وضع خطط إضافية للتقنيات المختلفة، ومراعاة التقنيات لتصميم أجهزة آمنة، واستخدام الشهادات الخاصة بأنظمة الإدارة لمزودي خدمات الحوسبة السحابية على سبيل المثال.

ويجب تطوير المواصفات للتقنيات الجديدة والشهادات المرتبطة بها بعد الاطلاع على أفضل الممارسات العالمية في هذا المجال.



أمن الفضاء الالكتروني

يهدف محور أمن الفضاء الإلكتروني الى التأكد من أنّ القطاعات العامة والخاصة، وبالتحديد تلك المصنفة ضمن برنامج حماية البنية التحتية للمعلومات الحيوية (CII)، تقوم بتطبيق معايير نظام إدارة أمن المعلومات.

وسيتم وضع مجموعة من الضوابط الأمنية الأساسية للأفراد، وتوفير الدعم لتنفيذها ومواصلة الجهود في تطوير المعايير والتوجيهات لأمن المعلومات والفضاء الإلكتروني لحماية شبكات الإنترنت والفضاء الإلكتروني.

1 يجب إدراك الإدارة التنفيذية العليا بأهمية الأمن الإلكتروني

يجب أن تدرك الإدارة التنفيذية العليا في المؤسسات أنّ الأمن الإلكتروني هو أحد الأصول الهامة التي تسمح للمؤسسات بالنمو وتحقيق أهدافها، والاستفادة من الأمن الإلكتروني لتطوير المنهجية الإدارية.

2 تنفيذ نظام إدارة أمن المعلومات

ثمّة مواصفات مختلفة يمكن للمؤسسات في إمارة دبي الاستفادة منها؛ إذ تساهم في تحقيق قاعدة حماية مشتركة، ويُعد نظام أمن المعلومات (ISR) إلزاميًّا لكل الجهات الحكومية وشبه الحكومية في إمارة دبي، وعلى مؤسسات القطاع الخاص النظر في تنفيذه أو تنفيذ أيّة أنظمة أخرى معمول بها، مثل معايير الأيزو ٢٧٠٠١ و/أو معايير NESA UAE IAS (لنظام إدارة أمن المعلومات)، ويُعتبر هذا الأمر مهماً بشكل خاص للمؤسسات المصنفة ضمن برنامج حماية البنية التحتية للمعلومات الحيوية (CII)، وتشمل المواصفات الأخرى التي يمكن النظر فيها معايير٢٧٠٣٥ (لإدارة جرائم أمن المعلومات) ومعايير٢٧٠٣١ (لجاهزية تقنية المعلومات والاتصالات لاستمرارية الأعمال) أو معايير ٢٢٣٠١ و/أو معايير الهيئة الوطنية لإدارة الطوارئ والأزمات NCEMA ٧٠٠٠ (وكلاهما لاستمرارية الأعمال).

يضم تنفيذ هذه المواصفات عدداً من الأسس المهمة:

يجب تحديد المسؤوليات وفقاً للمعرفة والخبرة والدورات التدريبية في مجال الأمن الإلكتروني، مما يسهم في اتخاذ القرارات المناسبة.

يجب أن تدرك كل مؤسسة أنها عرضة لمخاطر الأمن الإلكتروني، كما يجب تحديد طريقة في تقييم المخاطر (انظر إلى المبادئ الرئيسية «تقييم المخاطر») و توفير معلومات كافية لاتخاذ قرارات بشأن الحلول المناسبة وتنفيذها.

ويمكن القيام بذلك باستخدام المواصفات المقبولة دولياً أو محلياً كما هو موضح أعلاه، وينبغي لهذا النوع من الحلول أن يأخذ بعين الاعتبار أي ضوابط أمنيه قائمة وتحديد المسؤولين عنها و التزاماتهم والمدة الزمنية وغيرها من الأدوار.

3 إنشاء مجموعة من الضوابط الأساسية للأمن الإلكتروني ودعم تنفيذها

تنجح نسبة كبيرة من الهجمات الإلكترونية في استغلال نقاط الضعف في الأنظمة المستهدفة، وتتركز الهجمات الإلكترونية على أهداف محددة كقطاع المصارف والقطاع العام بينما لا تزال بسيطة على الأفراد (مثل الهجوم من خلال الاحتيال الإلكتروني أو سرقة كلمة السر)، إلا أنه يمكن مكافحة الهجمات الإلكترونية من خلال زيادة مستوى حماية الأنظمة.

ويتم إنشاء مجموعة من ضوابط الحماية الأساسية وصيانتها، ودعم تنفيذها من الأفراد في إمارة دبي، ومنها على سبيل المثال:

- الحماية ضد البرمجيات الخبيثة.
- حسن اختيار كلمات السر وإدارتها (بما في ذلك أجهزة إنترنت الأشياء (IoT)).
- استخدام جدران الحماية المناسبة وأدوات حماية أمن الشبكات.
- تطبيق تحديثات النظام في الوقت المناسب.
- الاستخدام الأمثل لمواقع التواصل الاجتماعي.
- الحفاظ على الأمن الفعلي للحواسيب والأجهزة في الأماكن العامة.
- استخدام خدمة الواي فاي العامة بطريقة مسؤولة وتأمين حماية شبكة الواي فاي الخاصة.

وينبغي دعم تنفيذ هذه الضوابط من خلال برامج مكافآت وتوفير أدوات للتحقق من الوضع الأمني للأنظمة.

4 التطوير المستمر للمعايير والمبادئ التوجيهية الخاصة بالمعلومات والأمن الإلكتروني

قام مركز دبي للأمن الإلكتروني بتطوير نظام أمن المعلومات (ISR) الذي يُعتبر تنفيذه إلزامي لكل الجهات الحكومية وشبه الحكومية في إمارة دبي والتدقيق على تنفيذه بالشكل الصحيح.

وقام المركز أيضًا بتطوير هذه الاستراتيجية التي تُعنى بالأمن الإلكتروني، و وضع المعايير والأنظمة وتطويرها، بما في ذلك المعايير الخاصة بمزودي الخدمات.

كما سيعمل مركز دبي للأمن الالكتروني مع الجهات المعنية على وضع المعايير والمبادئ التوجيهية والأدوات الأخرى التي يمكن أن تساعد في زيادة فعالية المؤسسات العامة والخاصة والأفراد في إمارة دبي في مجال الأمن الإلكتروني.

المرونة في الفضاء الإلكتروني

يهدف هذا المحور إلى التأكد من أن المؤسسات العامة والخاصة في إمارة دبي، لا سيما المصنفة ضمن برنامج حماية البنية التحتية للمعلومات الحيوية (CII) تتمتع بالمرونة اللازمة تجاه الهجمات الإلكترونية، ويمكنها استكمال عملياتها الهامة حتى في حال وقوع أية مشاكل أو أضرار.

يتمثل العنصر الأساسي للمرونة بتوفير منصة لتبادل المعلومات والدعم في إدارة الجرائم الخاصة بالأمن الإلكتروني والآليات المتطورة لمكافحة التهديدات.

ولتحقيق المرونة في الفضاء الإلكتروني، يجب على المؤسسات العامة والخاصة، المصنفة ضمن برنامج حماية البنية التحتية للمعلومات الحيوية (CII) تطبيق معايير تضمن استمرارية نظام تقنية المعلومات وإدارة الكوارث واستمرارية الأعمال على نطاق أوسع.

"نقدم للعالم نموذجاً جديداً وفريداً في تنمية المدن وإدارتها، التي بحاجة دائماً لفكر مختلف وإبداعات مبتكرة."
الشيخ محمد بن راشد آل مكتوم

1 إبلاغ مركز دبي للأمن الإلكتروني عن الجرائم وتبادل المعلومات حول المخاطر المرتبطة بالأمن الإلكتروني

يجب على المؤسسات العامة تبادل المعلومات عن المخاطر و الجرائم المرتبطة بالأمن الإلكتروني واستخدام البنية التحتية لإدارة الجرائم التي يقدّمها مركز دبي للأمن الإلكتروني، والتي تساعد في:

- تجنب انتشار المخاطر و الجرائم
- الإبلاغ عن الجرائم الإلكترونية
- وضع خطة شاملة للإبلاغ والتحليل والتوقع في المستقبل

يُعتبر تعاون مزودي الخدمات مهم لضمان الفعالية في خدمات المركز باعتبارهم المعنيين في الهجمات الإلكترونية وحوادث أمن المعلومات. سيتم بيان الدعم الذي يقدمه مركز دبي للأمن الإلكتروني بشكل مفصل أدناه.

2 تطوير القدرات اللازمة لحماية أمن الفضاء الإلكتروني ومرونته والحفاظ عليه وتحسينه

يضم الفضاء الإلكتروني مزودي الاتصالات وخدمات الإنترنت والمؤسسات التي تقوم بتطوير البرمجيات والأجهزة الرقمية وتقديم الخدمات عبر الإنترنت والتي غالبًا ما تكون من القطاع الخاص أو المؤسسات شبه الحكومية، ويجب أن تتبع كل المؤسسات المعنية بالفضاء الإلكتروني في إمارة دبي، مجموعة من القواعد لضمان أمن هذا الفضاء، وكذلك المؤسسات المصنفة ضمن برنامج حماية

البنية التحتية للمعلومات الحيوية (CII) في إمارة دبي.

ومن المهم أن تقوم هذه المؤسسات بوضع إطار عمل يدعم الحفاظ على القدرات اللازمة لحماية الفضاء الإلكتروني وتطويرها باستمرار، على سبيل المثال من خلال تنفيذ نظام أمن المعلومات (ISR).

3 تقديم الدعم لإدارة الجرائم المرتبطة بالأمن الإلكتروني واعتماد آليات متطورة لمواجهة التهديدات، وتوفير منصة لتبادل المعلومات

يجب على مركز دبي للأمن الإلكتروني توفير الخدمات التالية:

- مراقبة الجرائم المرتبطة بالأمن الإلكتروني ودعم المؤسسات في معالجتها.
- توفير معلومات حول الاتجاهات والقضايا والتهديدات في الفضاء الإلكتروني.
- تقديم معلومات حول الآليات المتطورة المعتمدة لمواجهة التهديدات من خلال ربط المصادر المختلفة واستخدام المعلومات والقدرات الفنية المتاحة في المركز لتقييم الوضع الأمني.
- توفير منصة لتبادل المعلومات حول الاحتمالات والثغرات والمخاطر المرتبطة بالفضاء الإلكتروني الخاص بإمارة دبي.

4 الامتثال لمعايير المرونة في الفضاء الإلكتروني

يجب وضع أحكام لضمان استمرارية كافة الوظائف المهمة في الفضاء الإلكتروني. كما يمكن أن يستفيد مزودي الخدمات بالمعايير المتعلّقة باستمرارية الأعمال وجاهزية تقنية المعلومات والاتصالات (معايير الأيزو ٢٧٠٣١ لجاهزية تقنية المعلومات والاتصالات لاستمرارية الأعمال) ومعايير ٢٢٣٠١ و/أو NCEMA ٧٠٠٠ (لاستمرارية الأعمال).

يجب الطلب من مزودي الخدمات في إمارة دبي (على سبيل المثال مزودي خدمات الاتصالات و خدمات الحوسبة السحابية) الالتزام بمجموعة القواعد التي يحدّدها مركز دبي للأمن الإلكتروني لضمان عدم المساس بأمن الفضاء الإلكتروني في الإمارة.

ويجب على مؤسّسات القطاع الخاص، لا سيّما تلك المصنّفة ضمن برنامج حماية البنية التحتية للمعلومات الحيوية (CII)، النظر أيضًا في تنفيذ هذه المعايير.

التعاون المحلي والدولي

يهدف هذا المحور إلى تعزيز التعاون مع القطاعات المختلفة المحلية والدولية لتوفير فضاء إلكتروني آمن ومرن في إمارة دبي.

حيث يتم على المستوى المحلي تحديد المؤسسات المصنفة ضمن برنامج حماية البنية التحتية للمعلومات الحيوية (CII) لإمارة دبي، وإنشاء نظام يسمح بتبادل المعلومات والتواصل بشكل آمن وتشجيع المؤسسات الخاصة غير المصنفة ضمن البرنامج على التعاون على المستوى المحلي، و يعنى التعاون الدولي بالأحكام الموحدة والتهديدات العالمية.

كما يجب تطوير تشريعات أو أحكام جديدة عند الضرورة، لتوفير فضاء إلكتروني آمن في إمارة دبي.

"أمامنا هدف واضح نعمل جميعاً على تحقيقه، وهو أن تكون دبي المدينة الأذكى عالمياً."

الشيخ حمدان بن محمد بن راشد

1 التعاون على المستوى العالمي

تتجلى أهمية التعاون وتبادل المعلومات على المستوى الدولي في معالجة القضايا العالمية المتعلقة بالأمن الإلكتروني، ومن أجل إدارة الوضع بشكل فعال، سيتم التعاون على المستوى الدولي في المجالات الآتية:

- وضع التشريعات والقوانين والمعايير الخاصة بالأمن الالكتروني.
- إجراء الأبحاث المشتركة
- مكافحة التهديدات العالمية

ويقوم مركز دبي للأمن الإلكتروني ببناء علاقات التعاون المحلية و الدولية لإدارة الجرائم الإلكترونية، كما تقوم هيئة تنظيم الاتصالات بالتعاون على المستوى الدولي من خلال متابعة والجرائم الإلكترونية، وتوقيع اتفاقيات مع منظمات متعدّدة الجنسيات، كما وقعت شرطة دبي اتفاقيات مع اليوروبول والانتربول، وغيرهما.

2 التعاون بين المؤسسات المصنفة ضمن برنامج حماية البنية التحتية للمعلومات الحيوية (CII) وإقامة شراكات مع القطاعات العامة والخاصة

يجب على مؤسسات القطاع العام في إمارة دبي تطوير مبادرة وطنية لتحديد المؤسسات المصنفة ضمن برنامج حماية البنية التحتية للمعلومات الحيوية (CII) في الإمارة والتعاون معها لتوفير فضاء إلكتروني آمن، ويشمل هذا التعاون أنشطة متعددة منها:

- إنشاء نظام لتبادل المعلومات بين المؤسسات المصنفة ضمن برنامج حماية البنية التحتية للمعلومات الحيوية (CII)
- التعاون والتواصل بين المؤسسات المصنّفة ضمن برنامج حماية البنية التحتية للمعلومات الحيوية (CII) (مع إمكانية الاستفادة من المتطلّبات والإرشادات الواردة في معايير الأيزو ٢٧٠١٠)
- توفير الدعم من مؤسسات القطاع العام في إمارة دبي.
- إنشاء نظام حوافز لتشجيع مؤسسات القطاع الخاص (غير المصنفة ضمن برنامج حماية البنية التحتية للمعلومات الحيوية (CII)) على المشاركة في مجال الأمن الالكتروني

بالإضافة إلى ذلك، يجب على مؤسسات القطاع العام في إمارة دبي التعاون مع المؤسسات الاتحادية والمؤسسات المصنفة ضمن برنامج حماية البنية التحتية للمعلومات الحيوية (CII) لتطوير الأمن الإلكتروني في دولة الإمارات العربية المتحدة.

3 وضع تشريعات وقوانين خاصة بالأمن الإلكتروني

تتخذ الجرائم الإلكترونية أشكالاً عدة، منها الاتصالات الرقمية بهدف الاحتيال (الرسائل الإلكترونية غير المرغوب بها) وانتهاك حقوق الملكية الفكرية لذلك يجب وضع إجراءات مفصلة لمعالجتها نظرًا لاتساع نطاقها.

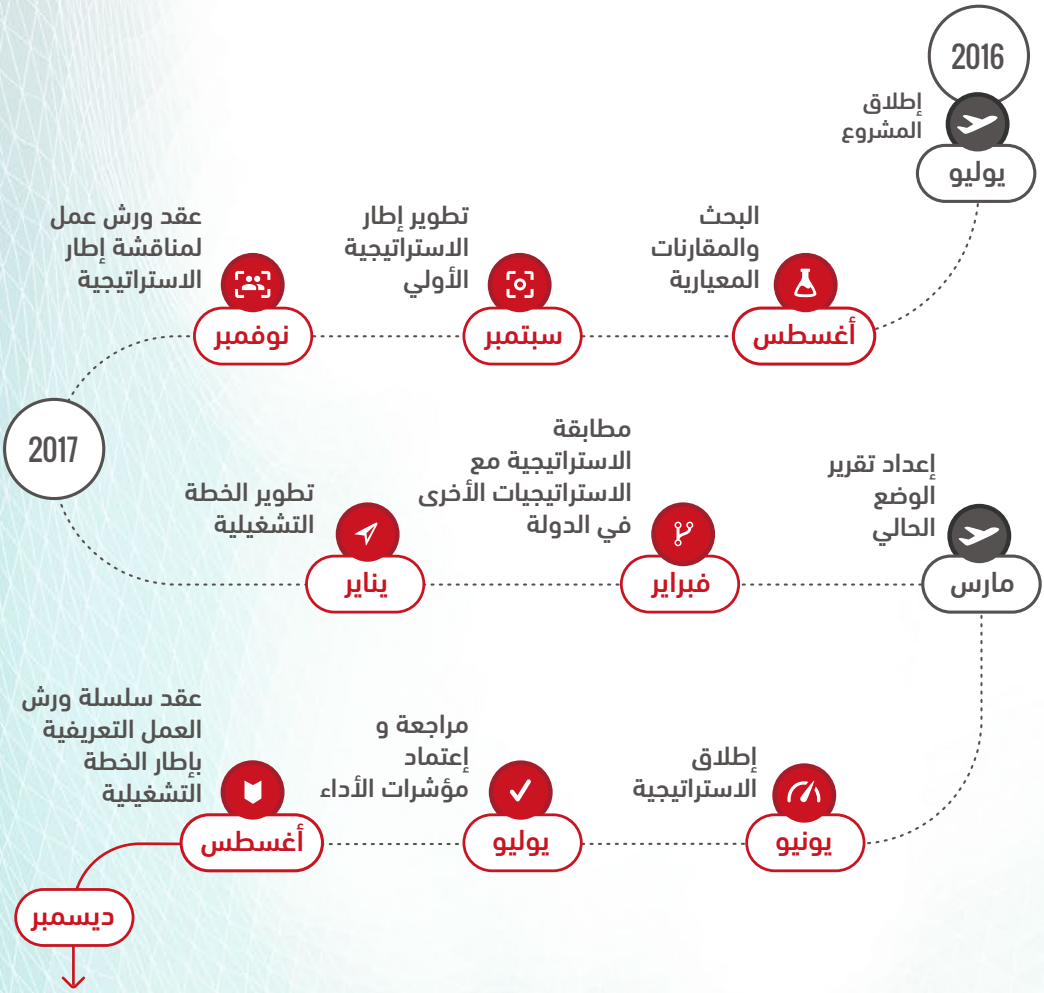
ويتطلب تطوير التشريعات والأحكام الخاصة بالفضاء الإلكتروني مشاركة من كافة القطاعات العامة والخاصة في إمارة دبي، كما يجب توقيع اتفاقيات دولية لإدارة الجرائم الإلكترونية.

رحلة التطوير

قام مركز دبي للأمن الإلكتروني بتطوير استراتيجية دبي للأمن الإلكتروني لحماية الإمارة من مخاطر التهديدات الإلكترونية بهدف دعم نموّها وابتكارها واقتصادها. وسيكون للاستراتيجية تأثيرٌ كبيرٌ على مختلف القطاعات في دبي، بما في ذلك المؤسّسات العامة والخاصة والأفراد. وبناءً عليه، تمّ تطوير هذه الاستراتيجية بالتعاون مع مختلف القطاعات الحيوية في الإمارة.

وقد بدأ العمل على الاستراتيجية باتّباع آلية المقارنة المعيارية و التي خضعت خلالها استراتيجيات الأمن الإلكتروني في نحو ١٥ بلدًا مختلفًا للمقارنة والتحليل. ثمّ، عُقدت سلسلة من ورش العمل التعريفية والاجتماعات مع مختلف القطاعات في دبي لمناقشة وجهات النظر المختلفة بهدف تحسين الاستراتيجية والتمهيد لتنفيذها.

إنّ إطلاق هذه الاستراتيجية هو بداية لمسيرتنا، حيث سنعمل على وضع خطة تشغيليّة لضمان تحقيق غايات هذه الاستراتيجية و نعمل حاليا على تنفيذها بمشاركة عددٍ كبير من الخبراء في القطاعات المختلفة في الإمارة. وقد تمّ تحديد فترة خمس سنوات كإطار زمني لتنفيذ استراتيجية دبي للأمن الإلكتروني.


2016
إطلاق المشروع
يوليو
البحث والمقارنات المعيارية
أغسطس
تطوير إطار الاستراتيجية الأولي
سبتمبر
عقد ورش عمل لمناقشة إطار الاستراتيجية
نوفمبر
2017
إعداد تقرير الوضع الحالي
مارس
مطابقة الاستراتيجية مع الاستراتيجيات الأخرى في الدولة
فبراير
تطوير الخطة التشغيلية
يناير
إطلاق الاستراتيجية
يونيو
مراجعة و إعتماد مؤشرات الأداء
يوليو
عقد سلسلة ورش العمل التعريفية بإطار الخطة التشغيلية
أغسطس
ديسمبر


DUBAI ELECTRONIC SECURITY CENTER
مركز دبي للأمن الإلكتروني