هيئة أبوظبي الرقمية
ABU DHABI DIGITAL AUTHORITY

قائمة متطلبات الأمن السيبراني للعمل عن بعد

مقدمة

بناءً على توجيهات الحكومة بتمكين الموظفين للعمل عن بعد لمواجهة فايروس كورونا المستجد Covid-19, فإن تزايد الاعتماد على الأنظمة والوسائل التقنية وتكنولوجيا المعلومات يزيد من حجم الأصول المعرضة للتهديدات والمخاطر، وعليه يستوجب اتخاذ المزيد من الضوابط والإجراءات للتعامل معها وإدارتها بفعالية في الوقت المناسب.

التوعية المستمرة والحماية الفعالة لسرية ونزاهة وتوفر أصول المعلومات تعد من المتطلبات اللازمة لأمن المعلومات، وعليه فإن على جميع الجهات الحكومية تحديث برامجها وأنظمتها الأمنية خلال المرحلة الحالية.

طورت هيئة أبوظبي الرقمية قائمة متطلبات استنادا على أفضل الممارسات العالمية لضمان توفير بيئة عمل آمنه للعمل عن بعد.

نطاق عمل تطبيق الضوابط

تطبق قائمة الضوابط في هذه الوثيقة على موظفي حكومة أبوظبي والمتعاقدين والأطراف الأخرى التابعة لها والمسؤولة عن إنشاء ومعالجة وتخزين ونقل واتلاف أصول المعلومات الخاصة بحكومة أبوظبي، بما في ذلك نظم المعلومات وغيرها من الأنظمة الأخرى.

الجهات الحكومية مسؤولة عن ضمان تطبيق الضوابط بشمولية تامة للتعامل مع التهديدات بطريقة فعالة.

قائمة متطلبات الأمن السيبراني

توعية الموظفين

زيادة الأنشطة اليومية التي تتم عن بعد من قبل الموظفين تشكل مخاطر إضافية على الجهات الحكومية. وللمساعدة في منع الهجمات السيبرانية بشكل أفضل، يجب إرسال رسائل توعوية للموظفين بشكل مستمر وبطرق مختلفة لتذكيرهم بما يلي:

- [ ] فريق تكنولوجيا المعلومات **لن** يقوم بالتواصل مع الموظفين بشأن إعادة تعيين كلمة المرور (لتجنب الوقوع في فخ الاحتيال).

- [ ] **عدم** فتح روابط أو مستندات أو خرائط المواقع التي تحتوي على معلومات تخص فايروس كورونا أو أي من وسائل الخداع الأخرى.

- [ ] **التأكد** من أن الموظفين على **دراية** بأرقام الهواتف وعناوين البريد الإلكتروني الهامة في حال وقوع أي حادثة أمنية.

- [ ] **يجب** على الموظفين الإبلاغ عن البرامج الخبيثة/ برامج الفدية على الفور من خلال القنوات الرسمية.

- [ ] **عدم** استخدام أقراص التخزين المحمولة والخدمات السحابية الغير موثوقة.

- [ ] **التأكد** من تسجيل الخروج من أجهزة الكمبيوتر في حال عدم الاستخدام.

- [ ] **يجب** على الموظفين الحرص على سرية الاتصالات (المعلومات) الحساسة وعدم قراءتها من قبل أطراف غير مصرح بهم، بما في ذلك أفراد الأسرة أو الزوار.

يجب على الموظفين عدم مشاركة المعلومات الحساسة عبر البريد الإلكتروني الشخصي أو تخزين المعلومات الحكومية في مواقع غير موثوقة.

يجب على الموظفين استخدام التطبيقات والبرامج **المعتمدة** لعقد الاجتماعات الخاصة بالعمل مع الأخذ بالاعتبار التالي:

- الحصول على كلمة مرور خاصة لكل اجتماع حيثما ينطبق ذلك.
- التأكد من عدم تسجيل الاجتماع المنعقد وفي حالة التسجيل يجب ابلاغ جميع الأطراف المشاركة.
- تذكير الموظفين بضرورة إغلاق الاجتماع بعد الانتهاء منه.

قائمة متطلبات الأمن السيبراني

الضوابط الواجب تنفيذها حيثما ينطبق ذلك

- ☐ **RW.C.1** التأكد من أن موظفي الدعم في حالة تأهب قصوى لطلبات إعادة تعيين كلمة المرور أو الطلبات "المثيرة للشبهات".
- ☐ **RW.C.2** التأكد من أن المستخدمين ذوي الصلاحية لا يقومون بتسجيل الدخول للمهام اليومية مع الصلاحيات العالية.
- ☐ **RW.C.3** يتطلب إجراء جميع عمليات تسجيل الدخول عن بُعد (المستخدمون والإداريون) عبر القنوات الآمنة.
- ☐ **RW.C.4** حظر الوصول إلى الجهاز (سواء عن بُعد أو محليًا) للحسابات في مستوى حساب المسؤول.
- ☐ **RW.C.5** يجب أن تتم جميع اتصالات الوصول عن بعد عبر شبكة افتراضية خاصة(VPN).
- ☐ **RW.C.6** يجب إنشاء اتصال شبكة افتراضية خاصة (VPN) باستخدام إمكانيات IPSec أو SSL.
- ☐ **RW.C.7** يجب أن تكون برامج / تكوينات عميل الشبكة الافتراضية الخاصة (VPN) معتمدة ومقدمة من قسم تكنولوجيا المعلومات في الجهة.
- ☐ **RW.C.8** يجب مراجعة سجلات نشاط الوصول عن بُعد وتحليلها بانتظام لتحديد أي حالات غير طبيعية محتملة أو أنشطة مشبوهة.

RW.C.9	يجب على بوابة الوصول عن بعد أن تقبل اتصال واحد لكل حساب مستخدم معتمد في أي وقت.	☐
RW.C.10	تعيين حد أقصى لوقت دخول المستخدمين للأنظمة والتطبيقات الحساسة.	☐
RW.C.11	إيقاف الجلسة غير الفعالة بعد تعين فترة محددة من عدم النشاط.	☐
RW.C.12	يجب فحص الأجهزة المتصلة بالشبكة الأساسية بانتظام من الفيروسات والبرامج الخبيثة.	☐
RW.C.13	يجب استخدام توثيق ثنائي (Two factor authentication) لتحسين آليات التوثيق لاتصال المستخدم عن بعد.	☐
RW.C.14	التأكد من عدم تجاوز أي من الإجراءات (لا تغير طارئ بدون موافقه , إلخ).	☐
RW.C.15	التأكد من وجود إجراء واضح لاتباعه في حالة وقوع حادث أمني وإبلاغ الأطراف المعنية.	☐