CITRA
الهيئة العامة للاتصالات وتقنية المعلومات
COMMUNICATION & INFORMATION TECHNOLOGY REGULATORY AUTHORITY

الضوابط الأمنية للعمل عن بعد

خلال فترة مواجهة فايروس كورونا المستجد (COVID-19)

مقدمة

في ظل الظروف الراهنة التي نعيشها اليوم وتماشيا مع تنفيذ الخطط الرامية للحد من انتشار فايروس COVID-19 الصادرة عن مجلس الوزراء الموقر، الأمر الذي يحتم البعض العمل بالمنزل ومن خلال تفعيل نظام العمل عن بعد دعما لاستمرارية العمل وحفاظا على سلامة المجتمع.

ودعماً لهذا الاحتياج خلال المرحلة الحالية للجهات الحكومية، فقد تم اعداد "الضوابط الأمنية للعمل عن بعد".

نطاق عمل الضوابط

تطبق هذه الضوابط عند تفعيل نظام العمل عن بعد وذلك من قبل الجهات الحكومية في دولة الكويت وتشمل الوزارات والهيئات والمؤسسات وجهات القطاع الخاص التي تمتلك أو تشغل بنى تحتية حساسة تابعة لها أو لاحد الجهات الحكومية.

أولا: التوعية بالمخاطر الالكترونية

توعية العاملين بطرق الاستخدام الآمن لتقنيات العمل عن بعد، وباتباع التالي:

- مراعاة التصفح من خلال صفحات الإنترنت الآمنة.
-
- عدم الاتصال من خلال الشبكات العامة الغير موثوقة والمتواجدة في الأماكن العامة.
- حماية الأجهزة المحمولة ووسائط التخزين المستخدمة في العمل عن بعد.
- حماية البيانات التي يتم حفظها على الأجهزة المستخدمة للدخول عن بعد وحسب تصنيفها وإجراءات وسياسات الجهة.
- التعامل الآمن مع خدمات البريد الإلكتروني ووسائل التواصل الاجتماعي ،والحذر من رسائل التصيّد الإلكتروني (Phishing).
- إبلاغ المختصين بالجهة عن أي تهديد الكتروني.

ثانيا: إدارة صلاحيات الدخول على الأنظمة

- عدم تفعيل صلاحية الدخول عن بعد إلا في الحالات القصوى مع مراعاة اتباع السياسات والإجراءات الأمنية المتبعة بالجهة.

- مراعاة أن تحدد صلاحية الدخول عن بعد بفترة زمنية تنتهي بعدها تلقائيا، ويتم تجديدها وفق الحاجة.
- المراجعة الدورية لصلاحيات الدخول والصلاحيات المستخدمة للعمل عن بعد.
- تطبيق تقنية التحقق المتعددة للهوية (Multi-Factor Authentication) للدخول عن بعد.
- تفعيل إعدادات الدخول عن بعد لتغلق بعد فترة زمنية محددة من عدم الاستخدام Session Timeout.
- تفعيل اعدادات تقييد إمكانية تسجيل الدخول عن بعد لنفس المستخدم من أجهزة حاسبات متعدّدة في نفس الوقت Concurrent Logins.
- تفعيل اعدادات إمكانية تعليق الدخول عن بعد مؤقتاً للحساب المستخدم في حالة محاولات الدخول المتتالية الخاطئة.

ثالثا: حماية الأجهزة المحمولة وأجهزة الخدمة الرئيسية

- إعادة ضبط الإعدادات المصنعية Default Configuration لكافة الأجهزة المحمولة وأجهزة الخدمة الرئيسية المستخدمة في الدخول.
- تحميل أنظمة الحماية من الفيروسات والبرمجيات الضارة (Malware) على الأجهزة المحمولة وأجهزة الخدمة الرئيسية المستخدمة في الدخول عن بعد وتحديثها بصورة دورية.
- الفحص الدوري للثغرات الأمنية ومعالجتها الأجهزة المحمولة وأجهزة الخدمة الرئيسية المستخدمة في الدخول عن بعد.

رابعا: إدارة أمن الشبكات

- تفعيل بروتوكولات الدخول عن بعد من خلال أجهزة الحماية Firewall وفقا للحاجة.
- المراجعة الدورية لإعدادات وسياسات أجهزة الحماية Firewall Rules.

خامسا: التشفير

- استخدام تقنيات آمنة وتحديثها بصورة دورية لتشفير الاتصال المستخدم للعمل عن بعد.

سادسا: مراقبة وإدارة الحوادث الالكترونية

- تفعيل سجلات الأحداث Event logs على الأجهزة المحمولة وأجهزة الخدمة الرئيسية المستخدمة في الدخول عن بعد ومراجعتها بصورة دورية.
- تفعيل مراقبة عمليات الدخول عن بعد والتحقق من صحتها.