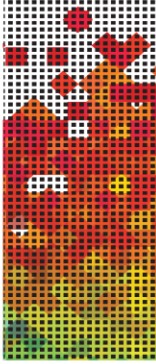

ضوابط الأمن السيبراني للعمل عن بعد

ص.ب: ١٨٠٧، الرمز البريدي: ١٣٠ العذيبة، سلطنة عُمان، هاتف: ٢٤١٦٦٦٠٠ (٠٠٩٦٨)، فاكس: ٢٤١٦٦٦٠٤ (٠٠٩٦٨)
P.O. Box: 1807, Postal Code: 130 Al Athaiba, Sultanate of Oman, Tel.: (00968) 24166600, Fax: (00968) 24166604

مقدمة:

يتناول هذا الملخص الاجراءات و الضوابط التي يجب إتباعها لتفعيل العمل عن بعد للمؤسسات الحكومية وغيرها من مؤسسات البنى الأساسية .

الأهداف:

تهدف هذه الضوابط إلى:

١- ضمان الأمن السيبراني عند تفعيل خاصية العمل عن بعد للمؤسسات .

٢- تعزيز الكفائة الإنتاجية للموظفين من خلال تطبيق ضوابط الأمن السيبراني .

٣- حماية الأصول المعلوماتية للمؤسسات في حال اتاحة خاصية العمل عن بعد .

٤- توعية وتأهيل الموظفين على الاستخدام الآمن و التعامل مع مخاطر الأمن السيبراني المرتبطة بالعمل عن بعد .

نطاق تطبيق الضوابط:

تشمل ضوابط الأمن السيبراني الجوانب و الإجراءات التي تعنى بالحد من المخاطر الناشئة من العمل عن بعد وتتضمن:

- أمن أجهزة المستخدمين عن بعد (الموظفين) .

- أمن قنوات الإتصال .
- أمن بوابة الإتصال عن بعد (شبكة المؤسسة) .
- التأهيل والتوعية المتعلقة بالعمل عن بعد .
- التقيد و الإلتزام بالضوابط .
- أقسام ودوائر أمن المعلومات الإلكترونية .
- الحوادث الأمنية السيبرانية .

أولاً: أمن أجهزة المستخدمين عن بعد (الموظفين): تعنى بالضوابط والممارسات التي يجب تفعيلها و اتباعها في الجهاز المستخدم للعمل عن بعد .

١. يجب أن يكون المستخدم عن بعد على دراية بمخاطر الأمن السيبراني المرتبطة بالعمل عن بعد .
٢. تجنب استخدام جهاز العمل عن بعد للاستخدامات الشخصية.
٣. التأكد من فحص جهاز العمل عن بعد وتوافقه مع معايير المؤسسة بشكل صحيح قبل الشروع في استخدامه .
٤. التأكد من اتخاذ الاجراءات الكفيلة بحماية جهاز العمل عن بعد من السرقة أو الفقد والأضرار المادية.
٥. التأكد من عمل كافة التحديثات اللازمة بأجهزة العمل عن بعد خاصة التحديثات الأمنية .
٦. يجب أن يحتوي جهاز العمل عن بعد على برنامج مضاد للفيروسات محدث بشكل دائم .
٧. تخزين وحفظ البيانات بما يتوافق مع سياسات الأمن السيبراني وتصنيف البيانات .

٨. التأكد من عمل نسخ احتياطية للبيانات بشكل مستمر.

٩. يجب تشفير الجهاز المستخدم للعمل عن بعد بشكل صحيح ومناسب.

١٠. إستخدام البرامج الموثوقة و المرخصة فقط.

ثانياً: أمن قنوات الاتصال: تعنى بالشبكات وشبكة الإنترنت التي يستخدمها الموظف أثناء العمل عن بعد

١. يجب على المستخدم عن بعد استخدام شبكة آمنة وموثوقة للإتصال بشبكة المؤسسة وعدم استخدام الشبكات العامة.

٢. إستخدام بروتوكول نفق آمن (Tunneling) .

٣. التأكد من تشفير الإتصال باستخدام خوارزمية آمنة ومحدثة.

ثالثاً: أمن بوابة الإتصال عن بعد: تعنى بالضوابط والممارسات التي يجب اتباعها في شبكة المؤسسة والتي تستخدم من قبل الموظفين أثناء العمل عن بعد

١. تحديد الوصول عن بعد إلى الحد الأدنى من الموارد المطلوبة لإنجاز المهام.

٢. إستخدام المصادقة متعددة التحقق (Multifactor Authentication) للمستخدمين عن بعد.

٣. التأكد من منح الصلاحيات المناسبة مع قائمة التحكم في الوصول (ACL) الممنوحة لكل مستخدم.

٤. يفضل تحديد معرف بروتوكول انترنت محدد (IP address) للوصول الى بوابة الاتصال عن بعد في المؤسسة.

٥. تحديد توقيت (Session Timeout) للمستخدمين .

٦. تفعيل و تكثيف مراقبة سجلات الدخول إلى الأنظمة .

٧. التأكد من عمل نسخ احتياطية للانظمة بشكل مستمر .

رابعاً: التأهيل والتدريب:

- يتم تأهيل وتدريب الموظفين المصرح لهم العمل عن بعد على الاستخدام الآمن للعمل عن بعد بما يتوافق مع ضوابط واجراءات الأمن السيبراني المعتمدة .
- يتم مراعاة سياسة تصنيف البيانات المعتمدة بكل مؤسسة عند استخدام خاصية العمل عن بعد .

خامساً: الالتزام والتقيد بضوابط الأمن السيبراني:

- يعتمد رئيس الوحدة / المسؤول المباشر الموظفين المصرح لهم للعمل عن بعد .
- يتعهد الموظف المصرح له العمل عن بعد بالالتزام بالضوابط واجراءات الأمن السيبراني .
- يقوم القسم المختص بكل مؤسسة بمتابعة وتقييم الإلتزام بهذه الضوابط و الإجراءات بعد تطبيق اللوائح و الأحكام المتعلقة بعدم الالتزام بالسياسات و الإجراءات المعتمدة للأمن السيبراني .

سادساً: أقسام ودوائر الأمن الالكتروني:

- تفعيل دور وعمل أقسام دوائر الأمن الالكتروني بالمؤسسات لمتابعة الإلتزام بضوابط الأمن السيبراني .
- تعزيز التوعية الأمنية السيبرانية بالمخاطر و التحديات المرتبطة بالعمل عن بعد وآليات التعامل معها .

سابعاً: الحوادث الأمنية السيبرانية:

- تفعيل خطط واجراءات الاستجابة للحوادث الأمنية السيبرانية .
- التنسيق المباشر مع المركز الوطني للسلامة المعلوماتية بوزارة التقنية و الاتصالات بخصوص حوادث الأمن السيبراني على البريد الالكتروني : ocert999@mtc.gov.om أو هاتف رقم: ٢٤١٦٦٨٢٨ .