الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

ضوابط الأمن السيبراني للعمل عن بعد

خلال حالة الاستعداد لمواجهة فايروس كورونا المستجد (COVID-19)

إشارة المشاركة: أبيض
تصنيف الوثيقة: متاح

بسم الله الرحمن الرحيم

بروتوكول الإشارة الضوئية (TLP):

تم إنشاء نظام بروتوكول الإشارة الضوئية لمشاركة أكبر قدر من المعلومات الحساسة ويستخدم على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية):

أحمر – شخصي وسري للمستلم فقط

المستلم لا يحق له مشاركة المصنف بالإشارة الحمراء مع أي فرد سواء من داخل او خارج المنشأة خارج النطاق المحدد للاستلام.

برتقالي – مشاركة محدودة

المستلم بالإشارة البرتقالية يمكنه مشاركة المعلومات في نفس المنشأة مع الأشخاص المعنيين فقط، ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

أخضر – مشاركة في نفس المجتمع

حيث يمكنك مشاركتها مع آخرين من منشأتك أو منشأة أخرى على علاقة معكم أو بنفس القطاع، ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

أبيض – غير محدود

مقدمة

إشارة إلى ما اتخذته حكومة المملكة العربية السعودية من تدابير وقائية متعددة لمواجهة فايروس كورونا المستجد (COVID-19)، والحد من انتشاره على المستويين الوطني والدولي، وما تحتمه تلك التدابير من اتخاذ ما يمكن اتخاذه من إجراءات لتقليل الاتصال المباشر بين الأشخاص خلال المرحلة الحالية، وتزايد اعتماد بعض الجهات الوطنية على وسائل تقنية المعلومات والاتصالات عبر الفضاء السيبراني لتمكين العاملين والموظفين من أداء أعمالهم عن بعد دون الحاجة للحضور إلى مقر العمل.

ومما لا شك فيه، أن الاعتماد على تقنيات العمل عن بعد قد يساهم في المساعدة على دعم التدابير الوقائية الصحية في المرحلة الحالية، إلا أن ذلك يستوجب اتخاذ العديد من التدابير اللازمة بشأن الأمن السيبراني، حيث أن التوسع في توفير قنوات الاتصال بالأنظمة الداخلية للجهات عبر الفضاء السيبراني يزيد بدوره من حجم الأصول المعرضة للهجمات السيبرانية المباشرة، ويستوجب اتخاذ المزيد من الضوابط الإضافية الرامية إلى تقليل احتمالية المخاطر السيبرانية الناتجة عن ذلك، أو على الأقل تقليل تأثيرها خلال الفترة الحالية.

ودعماً لهذا الاحتياج الوطني خلال المرحلة الحالية لعدد من الجهات الوطنية، فقد تم تطوير «ضوابط الأمن السيبراني للعمل عن بعد خلال حالة الاستعداد لمواجهة فايروس كورونا المستجد (COVID-19)».

وقد تم الاستناد في تطوير هذه الضوابط على ما أصدرته الهيئة الوطنية للأمن السيبراني، ومن ذلك:

١. الضوابط الأساسية للأمن السيبراني.

٢. ضوابط الأمن السيبراني للأنظمة الحساسة.

٣. أدوات الأمن السيبراني.

نطاق عمل الضوابط

تطبق هذه الضوابط عند إتاحة العمل عن بعد خلال حالة الاستعداد لمواجهة فايروس كورونا المستجد (COVID-19)، وذلك على الجهات الحكومية في المملكة العربية السعودية (وتشمل الوزارات والهيئات والمؤسسات وغيرها) والجهات والشركات التابعة لها وجهات القطاع الخاص التي تمتلك بنى تحتية وطنية حساسة أو تقوم بتشغيلها أو استضافتها.

ويستثنى من هذه الضوابط الوظائف والاعمال التي يجب انجازها من موقع العمل بدون استخدام تقنيات العمل عن بعد، حسب السياسات الداخلية والإجراءات الأمنية للجهة.

ضوابط الأمن السيبراني للعمل عن بعد
خلال حالة الاستعداد لمواجهة فايروس كورونا المستجد (COVID-19)

١	التوعية بالأمن السيبراني
رقم الضابط	نص الضابط
١-١	توعية العاملين بطرق الاستخدام الآمن أثناء العمل عن بعد، ومنها: ١-١-١ التعامل الآمن مع التصفح والاتصال بالإنترنت. ١-١-٢ التعامل الآمن مع خدمات البريد الإلكتروني ووسائل التواصل الاجتماعي، وأخذ الحذر والحيطة من إمكانية استغلالها في التصيّد الإلكتروني (Phishing). ١-١-٣ التعامل الآمن مع الأجهزة المحمولة ووسائط التخزين. ١-١-٤ تجنب الدخول عن بعد باستخدام أجهزة أو شبكات عامة غير موثوقة أو أثناء التواجد في أماكن عامة. ١-١-٥ التواصل مباشرة مع إدارة الأمن السيبراني في الجهة في حال ملاحظة شك بوجود تهديد أمن سيبراني. ١-١-٦ حماية البيانات التي يتم حفظها على الأجهزة المستخدمة للدخول عن بعد وحذفها حسب تصنيفها وإجراءات وسياسات الجهة.
٢	إدارة هويات الدخول والصلاحيات
رقم الضابط	نص الضابط
١-٢	تطبيق التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) لعمليات الدخول عن بعد.
٢-٢	المراجعة الدورية لهويات الدخول والصلاحيات المستخدمة للعمل عن بعد.

٢-٣	ضبط إعدادات الدخول عن بعد ليتم إغلاقها تلقائياً بعد فترة زمنية محدّدة (تحددها الجهة) من عدم الاستخدام (Session Timeout).
٢-٤	إعطاء الصلاحيات للمستخدمين لفترة زمنية تحددها الجهة، يتم تجديدها عند استمرار الحاجة، بناء على احتياجات العمل عن بعد، مع مراعاة حساسية الأنظمة ومستوى الصلاحيات التقنية.
٢-٥	تقييد إمكانية تسجيل الدخول عن بعد لنفس المستخدم من أجهزة حاسبات متعدّدة في نفس الوقت (Concurrent Logins).
٢-٦	إدارة كلمات المرور المستخدمة للدخول عن بعد بطريقة آمنة تشمل تعليق إمكانية الدخول عن بعد مؤقتاً للحساب المستخدم في محاولات دخول متتالية غير صحيحة (خاطئة).
٢-٧	منع الدخول عن بعد على الأنظمة الحساسة، إلا في الحالات الحرجة وحسب السياسات الداخلية والإجراءات الأمنية للجهة مع اتخاذ الإجراءات الضرورية لتقليل مستوى المخاطر السيبرانية.
٣	**حماية الأنظمة وأجهزة معالجة المعلومات**
رقم الضابط	نص الضابط
٣-١	تحديد وحصر الأصول التقنية والأنظمة الخاصة بالجهة المستخدمة للعمل عن بعد.
٣-٢	تحديث الحزم الأمنية للأصول التقنية والأنظمة المستخدمة للدخول عن بعد بشكل دوري.
٣-٣	الحماية من الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة (Malware) على أجهزة المستخدمين والخوادم المستخدمة في عمليات الدخول عن بعد باستخدام تقنيات وآليات الحماية الحديثة والمتقدمة، وإدارتها بشكل آمن.
٣-٤	إدارة الأجهزة المحمولة مركزياً باستخدام نظام إدارة الأجهزة المحمولة (Mobile Device Management "MDM") ما أمكن.
٣-٥	فحص واكتشاف ومعالجة الثغرات على الأصول التقنية والأنظمة المستخدمة للدخول عن بعد بشكل دوري.
٣-٦	مراجعة الإعدادات المصنعية (Default Configuration) للأصول التقنية والأنظمة المستخدمة في عمليات الدخول عن بعد وضبطها والتأكد من عدم وجود كلمات مرور ثابتة، وخلفية افتراضية.
٤	**إدارة أمن الشبكات**
رقم الضابط	نص الضابط

٤-١	تقييد منافذ وبروتوكولات وخدمات الشبكة المستخدمة لعمليات الدخول عن بعد على المستوى الوطني و فتحها حسب الحاجة.
٤-٢	مراجعة إعدادات جدار الحماية (Firewall Rules) وقوائمه بشكل دوري.
٥	**التشفير**
رقم الضابط	نص الضابط
٥-١	استخدام طرق وخوارزميات آمنة ومحدثة لتشفير كامل الاتصال الشبكي المستخدم للعمل عن بعد.
٦	**مراقبة الأمن السيبراني وإدارة الحوادث**
رقم الضابط	نص الضابط
٦-١	تفعيل سجلات الأحداث (Event logs) الخاصة بالأمن السيبراني على الأصول التقنية والأنظمة المستخدمة في العمل عن بعد ومراقبتها.
٦-٢	تحديث إجراءات مراقبة الأمن السيبراني على مدار الساعة وتطبيقها، بحيث تشمل مراقبة عمليات الدخول عن بعد، لا سيما عمليات الدخول عن بعد من خارج المملكة والتحقق من صحتها.
٦-٣	التبليغ المباشر للهيئة الوطنية للأمن السيبراني عند حدوث حادثة أمن سيبراني.
٦-٤	تحديث خطط الاستجابة لحوادث الأمن السيبراني ومعلومات التواصل داخل الجهة بما يتوافق مع حالة العمل عن بعد وبما يضمن جاهزية فرق الاستجابة للحوادث حال دعت الحاجة لذلك.


الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority