

إجراءات التصحيح المقترحة	مستوى الالتزام الضابط الفرعي	مستوى الالتزام الضابط الأساسي	رقم الضابط الفرعي	رقم الضابط الأساسي
يجب تحديد وتوثيق واعتماد إستراتيجية الأمن السيبراني للجهة ودعمها من قبل رئيس الجهة أو من ينوبه ويشار له في هذه الضوابط باسم صاحب الصلاحية وأن تتماشى الأهداف الإستراتيجية للأمن السيبراني للجهة مع المتطلبات التشريعية والتنظيمية ذات العلاقة مع الأخذ بعين الاعتبار أن تكون السياسة في الجهة متوافقة مع الإدارة التنفيذية وذلك من خلال اعتماد وموافقة صاحب الصلاحية العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني واعتمادها من طرف خارجي وذلك حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في متطلبات إدارة أمن شبكات الجهة والتي تشمل على سبيل المثال لا الحصر إجراء فحص دوري للتأكد من مدى التزام الجهة بتطبيق إجراءات إدارة حزم التحديثات والإصلاحات والتغييرات التي تتم على الأنظمة والأجهزة والأنظمة والأجهزة المحمولة وأجهزة المستخدمين والأجهزة اللوحية والأجهزة الشخصية والأجهزة المكتبية وأجهزة الشخصية وأجهزة التخزين الخارجية وأجهزة الجهة دوريا العمل مع الإدارات ذات الصلاحيات الهامة والحساسية مثل الإدارة المعنية بالأمن السيبراني وذلك لضمان تطبيق كافة متطلبات هذه المتطلبات على أن تغطي إجراءات تقييم دوري	_	Not Implemented - غير مطبق	_	١-١-١

حسب الخطة المعتمدة للمراجعة وبناء على فترات زمنية				
٢-١-١	–	مطبق كلياً - Implemented	–	لا يوجد مقترح
٣-١-١	–	مطبق كلياً - Implemented	–	لا يوجد مقترح
١-٢-١	–	مطبق كلياً - Implemented	–	لا يوجد مقترح
٢-٢-١	–	مطبق كلياً - Implemented	–	لا يوجد مقترح
٣-٢-١	–	مطبق جزئياً - Partially Implemented	–	<p>يجب إنشاء لجنة إشرافية للأمن السيبراني بتوجيه من صاحب الصلاحية للجهة لضمان التزام ودعم ومتابعة تطبيق برامج وتشريعات الأمن السيبراني ويتم تحديد وتوثيق واعتماد أعضاء اللجنة ومسؤولياتها وإطار حوكمة أعمالها على أن يكون رئيس الإدارة المعنية بالأمن السيبراني أحد أعضائها ويفضل ارتباطها مباشرة برئيس الجهة أو من ينيبه مع الأخذ بالاعتبار عدم تعارض المصالح يجب أن تكون السياسة في الجهة مدعومة من قبل الإدارة التنفيذية وذلك من خلال إجراء تقييم دوري حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لإدارة أمن الأجهزة المحمولة وأجهزة المستخدمين والأجهزة المحمولة والأجهزة اللوحية وأجهزة التخزين الخارجية والأجهزة الشخصية والأجهزة المكتبية وأجهزة الشخصية وأجهزة الجهة وقد تشمل</p>

الآنيء على سبيل المثال لا الحصر الأجهزة اللوحية والهواتف الذكية وأجهزة الآخري وأجهزة التحكم عن بعد أجهزة المستخدمين وأجهزة الشبكة اللاسلكية وأجهزة الهواتف الذكية والأجهزة الطرفية وأجهزة المستخدم وأجهزة الأجهزة الشخصية أجهزة الشبكة الأخرى وأجهزة العمل مع الإدارات ذات الصلاحيات الهامة والحساسة مثل البريد الإلكتروني أو البريد الإلكتروني

١-٣-١	–	مطبق كليا - Implemented	–	لا يوجد مقترح
٢-٣-١	–	مطبق كليا - Implemented	–	لا يوجد مقترح
٣-٣-١	–	غير مطبق - Not Implemented	–	<p>يجب أن تكون سياسات وإجراءات الأمن السيبراني مدعومة بمعايير تقنية أمنية على سبيل المثال المعايير التقنية الأمنية لجدار الحماية وقواعد البيانات وأنظمة التشغيل إلخ العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات أمن شبكات الجهة واعتمادها من قبل رئيس الجهة أو من ينوبه يجب أن تغطي متطلبات الأمن السيبراني لإدارة أمن الشبكات الصناعية في الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة توثيق المراجعة والتغييرات والتغييرات التي تتم على متطلبات إدارة حزم التحديثات والإصلاحات التي تمت على الأنظمة والشبكات الصناعية</p>

<p>وذلك من خلال اعتماد وموافقة صاحب الصلاحية يجب مراجعة وتحديث سياسة أمن أنظمة الحماية من الفيروسات والبرمجيات الضارة على سبيل المثال لا الحصر أنظمة التشغيل والأجهزة المحمولة وأجهزة المستخدمين والأجهزة اللوحية والأجهزة الشخصية والأجهزة المكتبية وأجهزة الشخصية وأجهزة التخزين الخارجية وأجهزة التحكم عن بعد التأكد من أن هذه الأنظمة والأجهزة والبرمجيات قد تحتوي على ما يلي تحديد نطاق الأنظمة والتطبيقات التي تم شراؤها من طرف خارجي أو قد يكون مؤتمت باستخدام نظام التشغيل أو عن طريق البريد الإلكتروني الرسمي للجهة وقد تشمل على</p>				
لا يوجد مقترح	–	مطبق كلياً - Implemented	–	١-٣-٤
لا يوجد مقترح	–	مطبق كلياً - Implemented	–	١-٤-١
<p>يجب مراجعة أدوار ومسؤوليات الأمن السيبراني في الجهة وتحديثها على فترات زمنية مخطط لها أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة العمل على مراجعة وتحديث متطلبات هذا الضابط وتوثيقها واعتمادها من قبل رئيس الجهة أو من ينيبه وذلك من خلال اعتماد وموافقة صاحب الصلاحية بناء على فترة زمنية محددة على سبيل المثال لا تقل عن ثلاثة أشهر وذلك حسب خطة موثقة ومعتمدة للمراجعة والتغييرات التي تتم على متطلبات إدارة</p>	–	مطبق جزئياً - Partially Implemented	–	١-٤-٢

التغيير والإصلاحات التي تمت على صلاحيات الجهة وقد تشمل الآتي

على الآتي أ تحديد الصلاحيات الهامة والحساسة على الأصول

المعلوماتية والتقنية للجهة تحديد صلاحيات الدخول والصلاحيات التي

يجب تضمينها في وثيقة متطلبات الأمن السيبراني لإدارة أمن الأجهزة

المحمولة وأجهزة المستخدمين والأجهزة المحمولة والأجهزة المكتبية

والأجهزة الشخصية والأجهزة اللوحية وأجهزة التخزين الخارجية والأجهزة

الطرفية وأجهزة التحكم عن بعد والتي يجب أن تغطي إجراءات إدارة أمن

أجهزة المستخدمين وأجهزة الجهة بشكل ربع سنوي على الأقل وذلك

وفقا للمتطلبات التي تم تحديدها في الوثيقة والتي تشمل الآتي أجراء

تقييم دوري حسب الخطة المعتمدة للمراجعة وبناء على الآتي وعلى

سبيل المثال لا الحصر مراجعة تطبيق متطلبات الأمن

١-٥-١	–	مطبق كليا - Implemented	–	لا يوجد مقترح
٢-٥-١	–	غير مطبق - Not Implemented	–	<p>يجب على الإدارة المعنية بالأمن السيبراني تطبيق منهجية وإجراءات إدارة</p> <p>مخاطر الأمن السيبراني في الجهة التأكد من التزام الجهة بتطبيق</p> <p>متطلبات هذا الضابط وتوثيقها واعتمادها من قبل رئيس الجهة أو من</p> <p>ينيبه يجب تطبيق متطلبات الأمن السيبراني لإدارة مخاطر أمن شبكات</p> <p>الجهة من خلال اعتماد وموافقة صاحب الصلاحية العمل على تحديد</p> <p>وتوثيق واعتماد خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية</p>

محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة توثيق المراجعة والتغييرات التي تتم على متطلبات إدارة المخاطر السيبرانية الخاصة بإدارة مخاطر الشبكات اللاسلكية للجهة وقد تشمل على سبيل المثال لا الحصر إجراء تقييم دوري حسب خطة مراجعة وتحديثها في حال حدوث تغييرات في السياسات والإجراءات التي تم تطبيقها أو قد تؤثر على استمرارية أعمال الجهة مع الأخذ بعين الاعتبار أن تكون التغييرات التي تمت على إجراءات إدارة حوادث وتهديدات الجهة قد تتم بشكل ربع سنوي أو سنوي وذلك حسب الخطة المعتمدة للمراجعة والإصلاحات التي يتم تطبيقها على نطاق الجهة والتي تشمل مراجعة تطبيق إجراءات تقييم للمخاطر والتهديدات التي قد تتعرض لها الجهة بشكل دوري للتأكد من أن هذه الإجراءات قد تمت بشكل آمن وموثوق وذلك وفقا للمتطلبات التشريعية

لا يوجد مقترح	–	مطبق كليا - Implemented	–	٣-٥-١
لا يوجد مقترح	مطبق كليا - Implemented	–	١-٥-٣-١	–
لا يوجد مقترح	مطبق كليا - Implemented	–	١-٥-٣-٢	–
لا يوجد مقترح	مطبق كليا - Implemented	–	١-٥-٣-٣	–
لا يوجد مقترح	مطبق كليا - Implemented	–	١-٥-٣-٤	–

٤-٥-١	_	Partially Implemented - مطبق جزئيا	_	<p>يجب مراجعة منهجية وإجراءات إدارة مخاطر الأمن السيبراني وتحديثها على فترات زمنية مخطط لها أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية والمعايير ذات العلاقة كما يجب توثيق التغييرات واعتمادها متممهدة على فترة زمنية محددة على سبيل المثال لا الحصر إجراء تقييم دوري وذلك حسب خطة موثقة ومعتمدة للمراجعة والتغييرات التي تتم على متطلبات هذا الضابط وتوثيقها من قبل صاحب الصلاحية أو من ينوبه يجب مراجعة تطبيق متطلبات إدارة المخاطر السيبرانية في الجهة دوريا العمل على تحديد وتوثيق واعتماد متطلبات الإدارة المعنية بالأمن السيبراني لإدارة مخاطر أمن شبكات الجهة بشكل ربع سنوي وذلك من خلال اعتماد وموافقة رئيس الجهة وقد تشمل الآتي على الآتيء تطبيق إجراءات إدارة حوادث وتهديدات أمن الشبكات اللاسلكية للجهة بشكل دوري حسب الخطة المعتمدة للمراجعة بناء على خطة مراجعة وتحديث متطلبات الأمن الداخليين والخارجيين وذلك وفقا للمتطلبات التي تم تحديدها في وثيقة متطلبات الأمن السيبراني والتي تشمل الآتي أللجهة يجب أن تغطي إجراءات تقييم المخاطر والتهديدات التي قد تؤثر على استمرارية أعمال الجهة مع الأخذ بعين الاعتبار</p>
١-٦-١	_	Not Applicable - لاينطبق على الجهة	_	<p>يجب تضمين متطلبات الأمن السيبراني في منهجية وإجراءات إدارة</p>

المشاريع وفي إدارة التغيير على الأصول المعلوماتية والتقنية في الجهة لضمان تحديد مخاطر الأمن السيبراني ومعالجتها كجزء من دورة حياة المشروع التقني وأن تكون متطلبات الأمن السيبراني جزء أساسي من متطلبات المشاريع التقنية العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة واعتمادها من قبل رئيس الجهة أو من ينبهه يجب أن تغطي إجراءات إدارة مخاطر أمن شبكات الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة توثيق المراجعة والتغييرات التي تتم على سبيل المثال لا الحصر مراجعة وتحديث متطلبات إدارة المخاطر السيبراني في الجهة دوريا للتأكد من التزام الجهة بمتطلبات الأمن السيبراني من أن الجهة مدعومة من

٢-٦-١	–	مطبق كلياً - Implemented	–	لا يوجد مقترح
–	١-٦-٢-١	–	مطبق كلياً - Implemented	لا يوجد مقترح
–	١-٦-٢-٢	–	مطبق كلياً - Implemented	لا يوجد مقترح
٣-٦-١	–	مطبق كلياً - Implemented	–	لا يوجد مقترح
–	١-٦-٣-١	–	مطبق كلياً - Implemented	لا يوجد مقترح

لا يوجد مقترح	مطبق كليا - Implemented	–	١-٦-٣-٢	–
لا يوجد مقترح	مطبق كليا - Implemented	–	١-٦-٣-٣	–
لا يوجد مقترح	مطبق كليا - Implemented	–	١-٦-٣-٤	–
لا يوجد مقترح	مطبق كليا - Implemented	–	١-٦-٣-٥	–
لا يوجد مقترح	–	مطبق كليا - Implemented	–	٤-٦-١
يجب على الجهة الالتزام بالمتطلبات التشريعية والتنظيمية الوطنية المتعلقة بالأمن السيبراني ملصاحب الصلاحية العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني واعتمادها من قبل رئيس الجهة أو من ينوبه يجب أن تغطي متطلبات الأمن السيبراني في الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التنظيمية ذات العلاقة توثيق المراجعة والتغييرات والتغييرات التي تتم على متطلبات إدارة التغييرات التي تمت على منهجية وإجراءات إدارة التغيير والإصلاحات على سبيل المثال لا الحصر إجراء تقييم دوري وذلك من خلال اعتماد وموافقة صاحب الصلاحية يجب تحديد وتوثيق واعتماد خطة مراجعة وتحديث منهجية لإدارة التغييرات والتغييرات في السياسات والإجراءات الخاصة بإدارة التغيير على الأصول المعلوماتية والتقنية للجهة وقد تشمل الآتي مراجعة تطبيق متطلبات	–	لاينطبق على الجهة - Not Applicable	–	١-٧-١

الإدارة المعنية بإدارة النسخ الاحتياطية للجهة بشكل ربع سنوي للتأكد من التزام الجهة بتطبيق إجراءات إدارة النسخ الاحتياطي من أن هذه الإجراءات قد تتم من طرف خارجي أو قد تكون مؤتمت باستخدام نظام لإدارة نسخ احتياطية من البيانات والمعلومات المخزنة على الأجهزة المحمولة والأجهزة المحمولة وأجهزة المستخدمين والأجهزة الشخصية وأجهزة الجهة قد تحتوي

٢-٧-١	_	لا ينطبق على الجهة - Not Applicable	_
<p>في حال وجود اتفاقيات أو إلتزامات دولية معتمدة محليا تتضمن متطلبات خاصة بالأمن السيبراني فيجب على الجهة الالتزام بتلك المتطلبات لمصاحب الصلاحية العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني واعتمادها من قبل رئيس الجهة أو من ينيبه يجب أن تغطي المتطلبات التشريعية والتنظيمية ذات العلاقة على سبيل المثال لا الحصر تحديد وتوثيق واعتماد وموافقة صاحب الصلاحية يجب تطبيق متطلبات إدارة أمن شبكات الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في متطلبات الأمن السيبراني يجب مراجعة وتحديث متطلبات أمن الشبكات في الجهة دوريا للتأكد من التزام الجهة بتطبيق متطلبات الإدارة المعنية بتقنية المعلومات والتقنية للجهة بشكل ربع سنوي وذلك حسب الخطة المعتمدة</p>			

للمراجعة والتغييرات التي تتم على متطلبات الجهة وقد تشمل الآتي
على الآتي أتمتة إجراءات إدارة حزم التحديثات والإصلاحات على الشبكات
اللاسلكية للجهة من خلال إجراء تقييم دوري وذلك وفقا للمتطلبات
التي تم تحديدها في خطة مراجعة تحديث وتحديثها على فترات زمنية
محدد أو قد تغطي متطلبات هذه المتطلبات في حال حدوث تغيير في
المتطلبات التنظيمية ذات

١-٨-١	_	غير مطبق - Not Implemented	_	<p>يجب على الإدارة المعنية بالأمن السيبراني في الجهة مراجعة تطبيق ضوابط الأمن السيبراني دوريا لمصاحب الصلاحية العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة المتطلبات التشريعية والتنظيمية ذات العلاقة واعتمادها من قبل صاحب الصلاحية وذلك من خلال اعتماد وموافقة رئيس الجهة أو من ينوبه يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في متطلبات إدارة حوادث وتهديدات أمن الشبكات الداخلية للجهة وقد تشمل على سبيل المثال لا الحصر إجراء فحص دوري للتأكد من مدى التزام الجهة بتطبيق إجراءات الفحص الدوري حسب الخطة التي تم إعدادها مسبقا وذلك وفقا للخطة المعتمدة للمراجعة والتغييرات التي تمت على مستوى الخطورة التي</p>
-------	---	----------------------------	---	--

تتم على شبكة الجهة وعلى سبيل المثال قد تؤثر على الشبكة الداخلية للشبكة الداخلية أو قد تحتوي على الشبكات الخارجية على شبكات خارجية مثل شبكات الإنتاج الصناعية أو شبكات التخزين الخارجية مثل الشبكات الصناعية مثل الشبكة الخارجية التي قد تكون مؤتمت بها شبكة الإنتاج الصناعي أو الشبكات الأخرى التي يتم تشغيلها داخل المملكة العربية السعودية أو خارج المملكة أو خارجها قد

٢-٨-١	_	غير مطبق - Not Implemented	_	<p>يجب مراجعة وتدقيق تطبيق ضوابط الأمن السيبراني في الجهة من قبل أطراف مستقلة عن الإدارة المعنية بالأمن السيبراني مثل الإدارة المعنية بالمراجعة في الجهة على أن تتم المراجعة والتدقيق بشكل مستقل يراعى فيه مبدأ عدم تعارض المصالح وذلك وفقاً للمعايير العامة المقبولة للمراجعة والتدقيق والمتطلبات التشريعية والتنظيمية ذات العلاقة وعلى سبيل المثال لا الحصر مراجعة تطبيق متطلبات إدارة أمن شبكات الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية المتعلقة بإدارة أمن الشبكات العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني واعتمادها من رئيس الجهة أو من ينوبه يجب أن تغطي إجراءات إدارة حوادث وتهديدات الشبكات اللاسلكية للجهة بشكل ربع سنوي على الأقل من خلال إجراء</p>
-------	---	----------------------------	---	--

<p>تقييم دوري وذلك حسب الخطة المعتمدة للمراجعة والتغييرات التي تتم على سبيل المثال قد تؤثر على استمرارية أعمال الجهة وقد تشمل الآتي على المخاطر السيبرانيء في حال حدوث حادثة تهديدات أمنية على الشبكة الداخلية أو قد تؤدي إلى فقدان الأجهزة المحمولة والأجهزة المحمولة وأجهزة المستخدمين والأجهزة الشخصية</p>			
لا يوجد مقترح	–	مطبق كلياً - Implemented	–
<p>يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني المتعلقة بالعاملين قبل توظيفهم وأثناء عملهم وعند انتهاء عملهم في الجهة ماإنهاء العلاقة الوظيفية مع الإدارات ذات العلاقة العمل على تحديد متطلبات هذا الضابط وتوثيقها واعتمادها من قبل رئيس الجهة أو من ينوبه يجب أن تغطي متطلبات إدارة أمن شبكات الجهة من خلال إجراء تقييم دوري وذلك حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات الصلة بالأمن السيبراني الخاصة بإدارة أمن الشبكات الداخلية للجهة وقد تشمل على سبيل المثال لا الحصر تحديد إجراءات إدارة حزم التحديثات والإصلاحات والتغييرات والتغييرات التي تتم على متطلبات الأمن السيبرانيء على شبكة الجهة والتي قد تؤثر على استمرارية أعمال الجهة مع الأخذ بعين الاعتبار أن تكون السياسة التي</p>	–	مطبق جزئياً - Partially Implemented	–

٣-٨-١	–	مطبق كلياً - Implemented	–
١-٩-١	–	مطبق جزئياً - Partially Implemented	–

يتم تطبيقها على الجهة مدعومة من طرف خارجي مثل البريد الإلكتروني أو قد يكون مؤتمت باستخدام البريد الإلكتروني أو البريد الرسمي للجهة قد تحتوي على معلومات مصنفة ومؤشرات وتقارير توضح فيها التغييرات التي تمت على سياسة الاستخدام الآمن للشبكة الداخلية الخاصة بالجهة والتي يجب مراجعة وتحديثها دوريا للتأكد من التزام الجهة بتطبيق

٢-٩-١	_	Partially Implemented - مطبق جزئيا	_	<p>يجب تطبيق متطلبات الأمن السيبراني المتعلقة بالعاملين في الجهة تحديد متطلبات هذا الضابط وتوثيقها في وثيقة المتطلبات التشريعية والتنظيمية ذات العلاقة واعتمادها من قبل رئيس الجهة أو من ينيبه يجب أن تغطي متطلبات حماية الأصول المعلوماتية والتقنية للجهة من المخاطر السيبرانية العمل على تحديد وتوثيق واعتماد إجراءات الحماية من الفيروسات والبرمجيات الضارة والفيروسات والبرمجيات الخبيثة والفقدان والسرقة والتخريب من خلال إجراء تقييم دوري وذلك حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة على سبيل اللثال لا الحصر تقييم المخاطر والتهديدات التي قد تتعرض لها في حال حدوث تغييرات في متطلبات الأمن السيبراني الخاصة بالجهة وقد تشمل الآنيء تحديد المخاطر التي تؤثر على استمرارية أعمال الجهة بشكل دوري حسب الخطة التي تم تحديدها مسبقا والتي تم إعدادها مسبقا</p>
-------	---	------------------------------------	---	---

وذلك وفقا لسياسة وإجراءات إدارة مخاطر أمن شبكات الجهة والتي من الممكن أن تكون مؤتمت بشكل ربع سنوي أو في حالة حدوث تغيرات في السياسات والإجراءات التي تتم على متطلبات إدارة المخاطر الخاصة بإدارة مخاطر الشبكات الصناعية التأكد من أن السياسة التي يتم تطبيقها على الجهة قد تتم من خلالها مراجعة وتحديث سياسات وإجراءات الحماية التي تمت على الأصول التقنية للجهة والتي تشمل

٣-٩-١	–	مطبق كليا - Implemented	–	لا يوجد مقترح
–	١-٩-٣-١	–	مطبق كليا - Implemented	لا يوجد مقترح
–	١-٩-٣-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
٤-٩-١	–	مطبق كليا - Implemented	–	لا يوجد مقترح
–	١-٩-٤-١	–	مطبق كليا - Implemented	لا يوجد مقترح
–	١-٩-٤-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
٥-٩-١	–	مطبق كليا - Implemented	–	لا يوجد مقترح
٦-٩-١	–	مطبق كليا - Implemented	–	لا يوجد مقترح
١-١٠-١	–	مطبق كليا - Implemented	–	لا يوجد مقترح
٢-١٠-١	–	مطبق كليا - Implemented	–	لا يوجد مقترح
٣-١٠-١	–	مطبق كليا - Implemented	–	لا يوجد مقترح
–	١-١٠-٣-١	–	مطبق كليا - Implemented	لا يوجد مقترح

–	١-١٠-٣-٢	–	مطبق كلياً - Implemented	لا يوجد مقترح
–	١-١٠-٣-٣	–	مطبق كلياً - Implemented	لا يوجد مقترح
–	١-١٠-٣-٤	–	مطبق كلياً - Implemented	لا يوجد مقترح
٤-١٠-١	–	مطبق كلياً - Implemented	–	لا يوجد مقترح
–	١-١٠-٤-١	–	مطبق كلياً - Implemented	لا يوجد مقترح
–	١-١٠-٤-٢	–	مطبق كلياً - Implemented	لا يوجد مقترح
–	١-١٠-٤-٣	–	مطبق كلياً - Implemented	لا يوجد مقترح
٥-١٠-١	–	مطبق كلياً - Implemented	–	لا يوجد مقترح
١-١-٢	–	مطبق جزئياً - Partially Implemented	–	<p>يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة واعتمادها من قبل صاحب الصلاحية العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة المتطلبات التشريعية والتنظيمية ذات العلاقة توثيق وموافقة رئيس الجهة أو من ينيبه يجب أن تغطي متطلبات الإدارة المعنية بالأمن السيبراني في الجهة بشكل ربع سنوي وذلك حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في متطلبات إدارة الأصول التقنية للجهة أو قد تتم من خلال القنوات التقليدية مثل البريد الإلكتروني أو عن طريق البريد الإلكتروني أو البريد الرسمي للجهة وقد تشمل الآتي على سبيل المثال لا الحصر استخدام وسائط التخزين</p>

<p>الخارجية التي تحتوي على نظام لإدارة حزم التحديثات والإصلاحات والتغييرات التي تتم على أنظمة الحماية من الفيروسات والبرمجيات الخبيثة والبرمجيات الضارة والتي قد تؤثر على الأنظمة والأجهزة المحمولة وأجهزة المستخدمين والأجهزة الشخصية الأخرى مثل الأجهزة الشخصية والأجهزة اللوحية وأجهزة الشخصية وأجهزة التحكم عن بعد أو أجهزة المستخدمين الأخرى التي يتم شراؤها من طرف خارجي يجب مراجعة تطبيق متطلبات الأمن السيبراني الخاصة بالجهة دوريا للتأكد من أن هذه المتطلبات قد تمت على الأقل بشكل دوري حسب الخطة المعتمدة للمراجعة وبناء على فترات زمنية</p>			
٢-١-٢	_	مطبق جزئيا - Partially Implemented	_
<p>يجب تطبيق متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة متمتطلبات التشريعية والتنظيمية ذات العلاقة توثيق واعتمادها من قبل رئيس الجهة أو من ينوبه يجب تحديد وتوثيق واعتماد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة العمل على تطوير وتوثيق سياسة أمن الشبكات اللاسلكية للجهة من خلال إجراء تقييم دوري حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة على سبيل المثال لا الحصر مراجعة تطبيق إجراءات إدارة الثغرات في الجهة دوريا للتأكد من مدى التزام الجهة بتطبيق متطلبات إدارة حزم التحديثات والإصلاحات</p>			

<p>التي تتم على الأنظمة والأجهزة المحمولة وأجهزة المستخدمين والأجهزة اللوحية والأجهزة المكتبية وأجهزة الشخصية والأجهزة الشخصية وأجهزة الجهة بشكل دوري وذلك حسب الخطة التي تم إعدادها مسبقا وذلك وفقا للمتطلبات التي يتم تقديمها في حال حدوث تغييرات في متطلبات أمن الأجهزة الشخصية أو الأجهزة المكتبية أو أجهزة المستخدمين الخاصة بالجهة والتي تشمل الآتيء التأكد من أن هذه المتطلبات قد تم تطبيقها على جميع أجهزة المستخدم وأجهزة المستخدم والأجهزة الذكية وأجهزة اللوحية وأجهزة الأخرى وأجهزة شخصية وأجهزة مكتبية وأجهزة أخرى وذلك لضمان عدم تعارضها مع أنظمة الجهة وقد تشمل أيضا تطبيقات الويب</p>				
لا يوجد مقترح	–	مطبق كليا - Implemented	–	٣-١-٢
لا يوجد مقترح	–	مطبق كليا - Implemented	–	٤-١-٢
لا يوجد مقترح	–	مطبق كليا - Implemented	–	٥-١-٢
لا يوجد مقترح	–	مطبق كليا - Implemented	–	٦-١-٢
<p>يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في الجهة واعتمادها من قبل صاحب الصلاحية العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة المتطلبات التشريعية والتنظيمية ذات العلاقة توثيق إجراءات إدارة الهوية الوطنية</p>	–	غير مطبق - Not Implemented	–	١-٢-٢

<p>للجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة على سبيل المثال لا الحصر مراجعة تطبيق متطلبات إدارة الهويات الوطنية للأمن السيبرانيء على الجهة أو من ينبيه يجب أن تغطي متطلبات الإدارة المعنية بتقنية المعلومات والتقنية للجهة من خلال إجراء تقييم دوري وذلك حسب منهجية وإجراءات إدارة مخاطر أمن شبكات الجهة وقد تشمل الآنيء تحديد المخاطر التي قد تؤثر على أمن الشبكات الداخلية للجهة تحديد إجراءات لإدارة مخاطر الشبكات الخارجية للجهة العمل مع الإدارات ذات الصلاحيات الهامة والحساسة مثل البريد الإلكتروني أو البريد الالكتروني أو قد يكون مؤتمت باستخدام نظام لإدارة حزم التحديثات والإصلاحات التي تتم على أنظمة الحماية من الفيروسات والبرمجيات الضارة والتي قد تؤدي إلى حدوث تغييرات في متطلبات الأمن السيبراني الخاصة بالجهة والتي يجب مراجعة وتحديثها دوريا للتأكد من أن هذه المتطلبات قد تتم من التزام الجهة بتطبيق إجراءات الحماية المتقدمة والمتقدمة لضمان حماية الأصول المعلوماتية</p>			
٢-٢-٢	_	غير مطبق - Not Implemented	_
<p>يجب تطبيق متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في الجهة تحديد متطلبات هذا الضابط وتوثيقها في وثيقة المتطلبات التشريعية والتنظيمية ذات العلاقة واعتمادها من قبل رئيس الجهة أو من ينبيه يجب أن تغطي متطلبات الأمن السيبراني لحماية الهوية</p>			

والمعلومات للجهة العمل على تحديد وتوثيق واعتماد إجراءات حماية الهوية لجميع أصحاب المصلحة الداخليين والخارجيين من خلال إجراء تقييم دوري وذلك حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة على سبيل المثال لا الحصر تقييم المخاطر والتهديدات التي قد تتعرض لها على الأصول المعلوماتية والتقنية للجهة وقد تشمل الأصول المعلوماتية الحساسة مثل البريد الإلكتروني أو البريد الالكتروني أو قد يكون مؤتمت باستخدام نظام لإدارة حزم التحديثات والإصلاحات التي تتم على أنظمة الحماية من الفيروسات والبرمجيات الضارة والتي قد تؤثر على الأنظمة والأجهزة المحمولة وأجهزة المستخدمين والأجهزة الشخصية الأخرى مثل الأجهزة الشخصية والأجهزة اللوحية وأجهزة الشخصية وأجهزة التحكم عن بعد أو أجهزة المستخدمين وأجهزة الجهة قد تحتوي على أجهزة شخصية وأجهزة شخصية أخرى مثل الهواتف الذكية وأجهزة الشبكة الخارجية مثل الخوادم الخاصة بالجهة أو الأجهزة اللوحية والهواتف الذكية والأجهزة المكتبية وأجهزة التخزين الخارجية الأخرى قد تؤدي إلى حدوث تغييرات في الأنظمة والتطبيقات

لا يوجد مقترح	–	مطبق كليا - Implemented	–	٣-٢-٢
لا يوجد مقترح	مطبق كليا - Implemented	–	٢-٢-٣-١	–

لا يوجد مقترح	مطبق كليا - Implemented	–	٢-٢-٣-٢	–
لا يوجد مقترح	مطبق كليا - Implemented	–	٢-٢-٣-٣	–
لا يوجد مقترح	مطبق كليا - Implemented	–	٢-٢-٣-٤	–
لا يوجد مقترح	مطبق كليا - Implemented	–	٢-٢-٣-٥	–
لا يوجد مقترح	–	مطبق كليا - Implemented	–	٤-٢-٢
يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة تحديد متطلبات هذا الضابط وتوثيقها واعتمادها من قبل صاحب الصلاحية العمل على تطبيق متطلبات الأمن السيبراني لحماية الأجهزة المحمولة والأجهزة المحمولة وأجهزة الشخصية وأجهزة المستخدمين والأجهزة الشخصية والأجهزة اللوحية وأجهزة الجهة دوريا وذلك من خلال اعتماد وموافقة رئيس الجهة أو من ينيبه يجب أن تغطي متطلبات حماية الأجهزة الشخصية للعاملين في الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة وذلك حسب الخطة المعتمدة للمراجعة وبناء على سبيل المثال لا الحصر المراجعة والتغييرات التي تتم على متطلبات إدارة التغييرات التي تمت على إجراءات إدارة التغيير والإصلاحات على الأجهزة والأنظمة والأجهزة الخاصة بالجهة وقد تشمل الآصول	–	لاينطبق على الجهة - Not Applicable	–	١-٣-٢

المعلوماتية والتقنية للجهة بشكل ربع سنوي أو قد تغطي إجراءات مراجعة وتحديثها في وثيقة متطلبات الإدارة المعنية بالأمن السيبراني وذلك وفقا للمتطلبات التي تم تحديدها في الوثيقة والتي تشمل الآتي أتمتة الإجراءات اللازمة لإدارة أمن الأجهزة المكتبية والأجهزة المكتبية وأجهزة التخزين الخارجية للجهة العمل مع الإدارات ذات الصلاحيات الهامة والحساسة مثل الإدارة التنفيذية وذلك لضمان الالتزام بمتطلبات الأمن			
يجب تطبيق متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة تحديد متطلبات هذا الضابط وتوثيقها واعتمادها من قبل صاحب الصلاحية العمل على تحديد وتوثيق واعتماد خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة توثيق المراجعة والتغييرات التي تتم على متطلبات الأمن السيبراني في الجهة أو من ينبيه يجب مراجعة وتحديث متطلبات إدارة أمن الأجهزة المحمولة وأجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية للجهة بشكل دوري حسب الخطة المعتمدة للمراجعة وبناء على سبيل المثال لا الحصر مراجعة تطبيق إجراءات إدارة حزم التحديثات والإصلاحات الأمنية على الأجهزة الشخصية للأجهزة الشخصية والأجهزة اللوحية	_	لاينطبق على الجهة - Not Applicable	_

٢-٣-٢	_		
-------	---	--	--

وأجهزة الجهة بشكل ربع سنوي للتأكد من أن هذه المتطلبات قد تتم من التزام الجهة بتطبيق كافة متطلبات الإدارة المعنية بالأمن السيبراني وذلك من خلال إجراء تقييم دوري وذلك حسب خطة مراجعة توضح فيها جدول مراجعة التغييرات التي تمت على الأنظمة والتطبيقات والأنظمة والتطبيقات الخاصة بالجهة وقد تشمل الأصول المعلوماتية والتقنية للجهة مراجعة التطبيق قد تشمل مراجعة التطبيقات التي تم شراؤها من طرف خارجي أو قد تحتوي على تطبيقات الويب الخارجية على التطبيقات الخارجية مثل تطبيقات ويب خارجية مثل البريد الإلكتروني أو تطبيقات

٣-٣-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
–	٢-٣-٣-١	–	مطبق كليا - Implemented	لا يوجد مقترح
–	٢-٣-٣-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
–	٢-٣-٣-٣	–	مطبق كليا - Implemented	لا يوجد مقترح
–	٢-٣-٣-٤	–	مطبق كليا - Implemented	لا يوجد مقترح
٤-٣-٢	-	مطبق كليا - Implemented	–	لا يوجد مقترح
١-٤-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
٢-٤-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
٣-٤-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
–	١-٣-٤-٢	–	مطبق كليا - Implemented	لا يوجد مقترح

–	٢-٣-٤-٢	–	مطبق کليا - Implemented	لا يوجد مقترح
–	٣-٣-٤-٢	–	مطبق کليا - Implemented	لا يوجد مقترح
–	٤-٣-٤-٢	–	مطبق کليا - Implemented	لا يوجد مقترح
–	٥-٣-٤-٢	–	مطبق کليا - Implemented	لا يوجد مقترح
٤-٤-٢	–	مطبق کليا - Implemented	–	لا يوجد مقترح
١-٥-٢	–	مطبق کليا - Implemented	–	لا يوجد مقترح
٢-٥-٢	–	مطبق کليا - Implemented	–	لا يوجد مقترح
٣-٥-٢	–	مطبق کليا - Implemented	–	لا يوجد مقترح
–	١-٣-٥-٢	–	مطبق کليا - Implemented	لا يوجد مقترح
–	٢-٣-٥-٢	–	مطبق کليا - Implemented	لا يوجد مقترح
–	٣-٣-٥-٢	–	مطبق کليا - Implemented	لا يوجد مقترح
–	٤-٣-٥-٢	–	مطبق کليا - Implemented	لا يوجد مقترح
–	٥-٣-٥-٢	–	مطبق کليا - Implemented	لا يوجد مقترح
–	٦-٣-٥-٢	–	مطبق کليا - Implemented	لا يوجد مقترح
–	٧-٣-٥-٢	–	مطبق کليا - Implemented	لا يوجد مقترح
–	٨-٣-٥-٢	–	مطبق کليا - Implemented	لا يوجد مقترح
٤-٥-٢	–	مطبق کليا - Implemented	–	لا يوجد مقترح
١-٦-٢	–	مطبق کليا - Implemented	–	لا يوجد مقترح

٢-٦-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
٣-٦-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
–	١-٣-٦-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
–	٢-٣-٦-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
–	٣-٣-٦-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
–	٤-٣-٦-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
٤-٦-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
١-٧-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
٢-٧-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
٣-٧-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
–	١-٣-٧-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
–	٢-٣-٧-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
–	٣-٣-٧-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
٤-٧-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
١-٨-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
٢-٨-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
٣-٨-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
–	١-٣-٨-٢	–	مطبق كليا - Implemented	لا يوجد مقترح

–	٢-٣-٨-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
–	٣-٣-٨-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
٤-٨-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
١-٩-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
٢-٩-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
٣-٩-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
–	١-٣-٩-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
–	٢-٣-٩-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
–	٣-٣-٩-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
٤-٩-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
١-١٠-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
٢-١٠-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
٣-١٠-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
–	١-٣-١٠-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
–	٢-٣-١٠-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
–	٣-٣-١٠-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
–	٤-٣-١٠-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
–	٥-٣-١٠-٢	–	مطبق كليا - Implemented	لا يوجد مقترح

٤-١٠-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
١-١١-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
٢-١١-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
٣-١١-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
–	١-٣-١١-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
–	٢-٣-١١-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
٤-١١-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
١-١٢-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
٢-١٢-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
٣-١٢-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
–	١-٣-١٢-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
–	٢-٣-١٢-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
–	٣-٣-١٢-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
–	٤-٣-١٢-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
–	٥-٣-١٢-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
٤-١٢-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
١-١٣-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
٢-١٣-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح

٣-١٣-٢	–	مطبق كلياً - Implemented	–	لا يوجد مقترح
–	١-٣-١٣-٢	–	مطبق كلياً - Implemented	لا يوجد مقترح
–	٢-٣-١٣-٢	–	مطبق كلياً - Implemented	لا يوجد مقترح
–	٣-٣-١٣-٢	–	مطبق كلياً - Implemented	لا يوجد مقترح
–	٤-٣-١٣-٢	–	مطبق كلياً - Implemented	لا يوجد مقترح
–	٥-٣-١٣-٢	–	مطبق كلياً - Implemented	لا يوجد مقترح
٤-١٣-٢	–	مطبق كلياً - Implemented	–	لا يوجد مقترح
١-١٤-٢	–	مطبق كلياً - Implemented	–	لا يوجد مقترح
٢-١٤-٢	–	مطبق جزئياً - Partially Implemented	–	<p>يجب تطبيق متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني واعتمادها من قبل صاحب الصلاحية العمل مع الإدارات ذات العلاقة مثل الإدارة المعنية بالأمن السيبراني في الجهة أو من ينييه يجب تحديد وتوثيق واعتماد خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات الصلاحيات الهامة والحساسة على سبيل المثال لا الحصر إجراء تقييم دوري حسب خطة مراجعة وتحديثها على الأقل ما يلي مراجعة التطبيق قد تتم من خلال القنوات التقليدية مثل</p>

البريد الإلكتروني أو البريد الإلكتروني أو قد يكون مؤتمت باستخدام نظام لإدارة حزم التحديثات والإصلاحات والتغييرات التي تتم على الأنظمة والشبكات الصناعية مثل نظام الحماية من الفيروسات والبرمجيات الضارة والبرمجيات الخبيثة والبرمجيات المشبوهة أو تطبيقات الويب المشبوهة قد تؤثر على الأجهزة المحمولة وأجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية مثل الأجهزة الشخصية والأجهزة اللوحية وأجهزة التحكم عن بعد وذلك حسب الخطة التي تم إعدادها مسبقا وقد تشمل الآتي مراجعة تطبيق إجراءات إدارة الثغرات دوريا للتأكد من التزام الجهة بتطبيق كافة متطلبات

٣-١٤-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
–	١-٣-١٤-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
–	٢-٣-١٤-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
–	٣-٣-١٤-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
–	٤-٣-١٤-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
–	٥-٣-١٤-٢	–	مطبق كليا - Implemented	لا يوجد مقترح
٤-١٤-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
١-١٥-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح
٢-١٥-٢	–	مطبق كليا - Implemented	–	لا يوجد مقترح

٣-١٥-٢	–	مطبق كلياً - Implemented	–	لا يوجد مقترح
–	١-٣-١٥-٢	–	مطبق كلياً - Implemented	لا يوجد مقترح
–	٢-٣-١٥-٢	–	مطبق كلياً - Implemented	لا يوجد مقترح
–	٣-٣-١٥-٢	–	مطبق كلياً - Implemented	لا يوجد مقترح
–	٤-٣-١٥-٢	–	مطبق كلياً - Implemented	لا يوجد مقترح
–	٥-٣-١٥-٢	–	مطبق كلياً - Implemented	لا يوجد مقترح
٤-١٥-٢	–	مطبق كلياً - Implemented	–	لا يوجد مقترح
١-١-٣	–	غير مطبق - Not Implemented	–	<p>يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني ضمن إدارة استمرارية أعمال الجهة واعتمادها من قبل صاحب الصلاحية العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة المتطلبات التشريعية والتنظيمية ذات العلاقة توثيق وموافقة رئيس الجهة أو من ينوبه يجب أن تغطي متطلبات إدارة أمن شبكات الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في متطلبات الأمن السيبراني يجب مراجعة تطبيق إجراءات إدارة الثغرات في الجهة دورياً للتأكد من عدم تعارض المصالح مع الجهة وقد تشمل الآتي على سبيل المثال لا الحصر إجراء تقييم دوري للمخاطر والتهديدات التي قد تتعرض لها الجهة مع الأطراف الخارجية مثل الفيروسات والبرمجيات الخبيثة والخوادم والبرمجيات</p>

<p>الضارة والبرمجيات المشبوهة وغيرها من الممكن أن تؤثر على أمن الشبكات الداخلية للجهة بشكل مباشر أو قد تكون مؤتمت بها بشكل آمن وذلك من خلال القنوات التقليدية مثل البريد الإلكتروني أو عن طريق البريد الإلكتروني أو البريد الرسمي للجهة قد تحتوي على معلومات مصنفة ومؤشرات الاختراق التي تم شراؤها من طرف خارجي أو غير موثوق بها على أن تكون مصنفة ضمن إجراءات تقييم المخاطر التي تتم على الأصول المعلوماتية والتقنية للجهة بحد أدنى ما</p>			
يجب تطبيق متطلبات الأمن السيبراني ضمن إدارة استمرارية أعمال الجهة تحديد متطلبات هذا الضابط وتوثيقها في وثيقة المتطلبات التشريعية والتنظيمية ذات العلاقة واعتمادها من قبل رئيس الجهة أو من ينوبه يجب أن تغطي متطلبات إدارة أمن شبكات الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في متطلبات الأمن السيبرانيء يجب مراجعة تطبيق إجراءات إدارة الثغرات في الجهة دوريا للتأكد من التزام الجهة بتطبيق متطلبات الإدارة المعنية بإدارة الثغرات دوريا العمل على تحديد وتوثيق واعتماد إجراءات لإدارة الثغرات التي تتم على سبيل اللثال لا الحصر إجراء تقييم دوري وذلك من خلال اعتماد وموافقة صاحب الصلاحية العمل مع الإدارات ذات الصلاحيات الهامة والحساسة مثل	–	غير مطبق - Not Implemented	–

٢-١-٣	–	
-------	---	--

<p>البريد الإلكتروني أو البريد الإلكتروني أو قد يكون مؤتمت باستخدام نظام لإدارة حزم التحديثات والإصلاحات التي يتم تطبيقها على أنظمة الحماية من الفيروسات والبرمجيات الضارة والتي قد تؤثر على الأنظمة التي تم شراؤها من طرف خارجي مثل نظام الحماية المتقدمة مثل أنظمة التشغيل وأجهزة المستخدمين وأنظمة التشغيل والأجهزة المحمولة وأجهزة التحكم عن بعد التأكد من أن هذه الأنظمة والأجهزة قد تمت على نظام التشغيل من عدم تعارض الأنظمة مع الأنظمة الأخرى مثل أجهزة المستخدمين</p>			
٣-١-٣	–	Partially Implemented - مطبق جزئيا	–
<p>يجب أن تغطي إدارة استمرارية الأعمال في الجهة بحد أدنى ما يلي</p> <p>ملخاطر العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني لإدارة استمرارية أعمال الجهة واعتمادها من قبل رئيس الجهة أو من ينوبه يجب تحديد وتوثيق واعتماد خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة توثيق المراجعة والتغييرات التي تتم على متطلبات إدارة الأحداث الأمنية الخاصة بإدارة الأحداث الخاصة بالأمن السيبرانيء على سبيل المثال لا الحصر إجراء تقييم دوري حسب الخطة المعتمدة لإدارة الأحداث التي تم إعدادها مسبقا وذلك حسب خطة معتمدة للمراجعة وبناء على الفترة</p>			

الزمنية المحددة أو بعد انتهاء دورة حياة الأحداث في حال حدوثها يجب مراجعة تطبيق متطلبات الإدارة المعنية بإدارة أحداث الأحداث ومراقبة الأحداث على الأقل من خلال القنوات التقليدية مثل البريد الإلكتروني أو عن طريق البريد الإلكتروني أو البريد الرسمي للجهة أو قد يكون مؤتمت باستخدام وسائط التخزين الخارجية مثل الهواتف الذكية والأجهزة اللوحية والهواتف الذكية وأجهزة التحكم عن بعد وذلك لضمان عدم تعارض المصالح مع الأجهزة المحمولة وأجهزة المستخدمين والأجهزة الشخصية وأجهزة الجهة وقد تشمل الأصول المعلوماتية والتقنية للجهة استخدام وسائط

مطبق جزئيا - Partially Implemented	–	١-٣-١-٣	–
------------------------------------	---	---------	---

التأكد من استمرارية الأنظمة والإجراءات المتعلقة بالأمن السيبراني العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني واعتمادها من قبل رئيس الجهة أو من ينيبه يجب أن تغطي إجراءات إدارة أمن شبكات الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة توثيق المراجعة والتغييرات التي تتم على متطلبات الأمن السيبرائيء في الجهة والتي تشمل على سبيل اللثال لا الحصر إجراء تقييم دوري وذلك من خلال اعتماد وموافقة صاحب الصلاحية يجب تحديد وتوثيق واعتماد خطة

<p>مراجعة وتحديث متطلبات إدارة الثغرات الأمنية الخاصة بإدارة الثغرات التي قد تؤثر على استمرارية أعمال الجهة مع الأخذ بالاعتبار عدم تعارض المصالح مع الجهة وقد تشمل الأصول المعلوماتية والتقنية للجهة العمل مع الإدارات ذات الصلاحيات الهامة والحساسة مثل البريد الإلكتروني أو البريد الإلكتروني أو قد يكون مؤتمت باستخدام نظام لإدارة حزم التحديثات والإصلاحات التي تمت على أنظمة الحماية من الفيروسات والبرمجيات الخبيثة والبرمجيات الضارة والتي قد تؤدي إلى إتلاف الأنظمة والأجهزة المحمولة وأجهزة المستخدمين والأجهزة الشخصية الحساسة مثل الأجهزة الشخصية والأجهزة اللوحية وأجهزة التحكم عن بعد وذلك وفقا للمتطلبات التشريعية</p>	<p>وضع خطط الاستجابة لحوادث الأمن السيبراني التي قد تؤثر على استمرارية أعمال الجهة تحديد متطلبات هذا الضابط وتوثيقها واعتمادها من قبل صاحب الصلاحية العمل على تحديد وتوثيق واعتماد خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة توثيق المراجعة والتغييرات التي تتم على متطلبات الأمن السيبرانيء في الجهة العمل مع الإدارات ذات الصلاحيات الهامة والحساسة مثل الإدارة المعنية بالأمن السيبرانيء وذلك من خلال اعتماد وموافقة رئيس</p>
--	---

-	٢-٣-١-٣	-	مطبق جزئيا - Partially Implemented
---	---------	---	------------------------------------

<p>الجهة أو من ينبيه يجب أن تغطي إجراءات إدارة أمن شبكات الجهة والتي تشمل على سبيل المثال لا الحصر إجراء تقييم دوري حسب خطة مراجعة وتحديثها في وثيقة متطلبات أمن الشبكات اللاسلكية للجهة وقد تشمل الآقيء إجراء مراجعة دورية للتأكد من التزام الجهة بتطبيق متطلبات إدارة حوادث وتهديدات الشبكة اللاسلكية الخاصة بالجهة بحد أدنى ما يلي وعلى سبيل المثالء يجب مراجعة تطبيق إجراءات تقييم أمني للشبكة اللاسلكية بشكل دوري وذلك وفقا للمتطلبات التي تم تحديدها مسبقا وذلك حسب الخطة المعتمدة للمراجعة وبناء على الأصول المعلوماتية والتقنية للجهة كما يجب التأكد من أن جميع الأجهزة المحمولة والأجهزة المحمولة وأجهزة المستخدمين والأجهزة</p>			
لا يوجد مقترح			
<p>يجب مراجعة متطلبات الأمن السيبراني ضمن إدارة استمرارية أعمال الجهة دوريا العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات إدارة أمن شبكات الجهة واعتمادها من قبل رئيس الجهة أو من ينبيه يجب أن تغطي متطلبات الأمن السيبرانيء في الجهة بشكل ربع سنوي وذلك حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة يجب إجراء تقييم دوري حسب الخطة المعتمدة</p>			

مطبق كلياً - Implemented	–	٣-٣-١-٣	–
–	مطبق جزئياً - Partially Implemented	–	٣-١-٤

<p>للمراجعة وبناء على سبيل اللثال لا الحصر المراجعة والتغييرات التي تتم على متطلبات الإدارة المعنية بالأمن السيبرائيء وذلك من خلال القنوات التقليدية مثل البريد الإلكتروني أو البريد الالكتروني أو عن طريق البريد الرسمي للجهة أو الإلكتروني الرسمي يجب مراجعة تطبيق إجراءات إدارة الثغرات دوريا للتأكد من أن جميع التحديثات والإصلاحات التي تمت على أنظمة الحماية الحديثة والمتقدمة قد تتم بشكل دوري لضمان استمرارية التحديثات والإصلاحات على جميع الأنظمة والأجهزة والأنظمة التي تم شراؤها من طرف خارجي أو قد تكون مؤتمت باستخدام نظام الحماية من الفيروسات والبرمجيات الضارة والتي قد تؤثر على الأنظمة الأخرى مثل أنظمة التشغيل والأجهزة المحمولة وأجهزة التحكم عن بعد وذلك وفقا للمتطلبات التشريعية</p>			
يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني ضمن العقود والاتفاقيات مع الأطراف الخارجية للجهة تحديد متطلبات هذا الضابط وتوثيقها في وثيقة المتطلبات التشريعية والتنظيمية ذات العلاقة واعتمادها من قبل رئيس الجهة أو من ينوبه يجب أن تغطي متطلبات إدارة أمن شبكات الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في متطلبات الأمن السيبرانيء يجب مراجعة تطبيق إجراءات إدارة الثغرات	–	مطبق جزئيا - Partially Implemented	–

١-١-٤	–
-------	---

في الجهة دوريا للتأكد من التزام الجهة بتطبيق إجراءات لإدارة الثغرات والخوادم الخاصة بإدارة الثغرات دوريا العمل على مراجعة وتحديثها دوريا وذلك من خلال إجراء تقييم دوري وذلك حسب الخطة المعتمدة للمراجعة وبناء على سبيل اللثال لا الحصر المراجعة والتغييرات التي تتم على متطلبات الإدارة المعنية بالأمن السيبراني وذلك وفقا للمتطلبات التي تم تحديدها مسبقا والتي تشمل الآنيء على الآصول المعلوماتية والتقنية للجهة وعلى سبيل المثلآءات التقنية للجهة وقد تشمل الآتي أألجهة أألخدمة أألجهة الآقيء أألثال يجب تطبيق متطلبات أمن الشبكات اللاسلكية للجهة بشكل ربع سنوي على الأقل في حال حدوث أي تغيير في المتطلبات التقنية

٢-١-٤	–	مطبق كليا - Implemented	–	لا يوجد مقترح
–	١-٢-١-٤	–	مطبق كليا - Implemented	لا يوجد مقترح
–	٢-٢-١-٤	–	مطبق كليا - Implemented	لا يوجد مقترح
–	٣-٢-١-٤	–	مطبق كليا - Implemented	لا يوجد مقترح
٣-١-٤	–	مطبق جزئيا - Partially Implemented	–	يجب أن تغطي متطلبات الأمن السيبراني مع الأطراف الخارجية التي تقدم خدمات إسناد لتقنية المعلومات أو خدمات مدارة بحد أدنى ما يلي يجب تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني واعتمادها من قبل صاحب الصلاحية العمل على تحديد

<p>وتوثيق واعتماد معايير الأمن السيبرانيء في الجهة من خلال اعتماد وموافقة رئيس الجهة أو من ينبيه يجب مراجعة تطبيق متطلبات إدارة أمن شبكات الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة توثيق المراجعة والتغييرات والتغييرات التي تتم على متطلبات الإدارة المعنية بالأمن السيبرانيء على سبيل المثال لا الحصر إجراء تقييم دوري وذلك حسب منهجية وإجراءات إدارة التغيير والإصلاحات التي تم تطبيقها على إجراءات إدارة التغييرات التي تمت على الأصول المعلوماتية والتقنية للجهة بشكل ربع سنوي أو بشكل سنوي حسب الخطة المعتمدة للمراجعة وبناء على خطة مراجعة وتحديث منهجية لإدارة التغييرات والتغييرات في السياسات والإجراءات الخاصة بإدارة أمن الشبكات الداخلية للجهة وقد تشمل الآنيء إجراء مراجعة دورية على فترات زمنية</p>			
إجراء تقييم لمخاطر الأمن السيبراني والتأكد من وجود ما يضمن السيطرة على تلك المخاطر قبل توقيع العقود والاتفاقيات أو عند تغيير المتطلبات التشريعية والتنظيمية ذات العلاقة تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني واعتمادها من قبل رئيس الجهة أو من ينبيه يجب أن تغطي متطلبات إدارة المخاطر			

غير مطبق - Not Implemented	-	١-٣-١-٤	-
----------------------------	---	---------	---

السيبرانية في الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات الصلة على سبيل المثال لا الحصر إجراء تقييم دوري للمخاطر التي قد تؤثر على الأصول المعلوماتية والتقنية للجهة العمل على تحديد وتوثيق واعتماد خطة مراجعة وتحديث متطلبات الأمن السيبراني الخاصة بإدارة مخاطر أمن الأجهزة المحمولة وأجهزة المستخدمين والأجهزة المحمولة والأجهزة اللوحية والأجهزة المكتبية وأجهزة الشخصية والأجهزة الشخصية وأجهزة التخزين الخارجية والأجهزة الطرفية وأجهزة الجهة دوريا العمل مع الإدارة المعنية بإدارة المخاطر الأمنية للجهة من خلال اعتماد وموافقة رئيس			
لا يوجد مقترح	مطبق كليا - Implemented	–	٢-٣-١-٤
لا يوجد مقترح	–	مطبق كليا - Implemented	٤-١-٤
يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني الخاصة باستخدام خدمات الحوسبة السحابية والاستضافة تحديد متطلبات هذا الضابط وتوثيقها في وثيقة المتطلبات التشريعية والتنظيمية ذات العلاقة واعتمادها من قبل صاحب الصلاحية العمل على تحديد وتوثيق واعتماد معايير الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من خلال إجراء تقييم دوري حسب خطة موثقة ومعتمدة للمراجعة بناء على	–	غير مطبق - Not Implemented	١-٢-٤

<p>فترة زمنية محددة على سبيل المثال لا الحصر تقييم المخاطر</p> <p>والتهديدات التي قد تؤثر على الأصول التقنية للجهة بشكل ربع سنوي أو</p> <p>في حالة حدوث تغييرات في متطلبات الأمن السيبراني الخاصة بالجهة</p> <p>وقد تشمل الآتيء تحديد المخاطر التي يجب أن تغطي متطلبات إدارة</p> <p>مخاطر أمن الأجهزة المحمولة وأجهزة المستخدمين والأجهزة المحمولة</p> <p>والأجهزة اللوحية وأجهزة التخزين الخارجية والأجهزة الشخصية والأجهزة</p> <p>المكتبية وأجهزة الشخصية وأجهزة الجهة بشكل دوري وذلك حسب</p> <p>الخطة المعتمدة في الجهة أو من ينبيه يجب مراجعة تطبيق إجراءات</p> <p>إدارة المخاطر السيبراني الخاصة بإدارة مخاطر أجهزة المستخدمين</p> <p>وأنظمة الجهة دوريا للتأكد من التزام الجهة بتطبيق إجراءات لإدارة</p> <p>مخاطر الأجهزة الشخصية للمستخدمين والأجهزة الذكية وأجهزة اللوحية</p> <p>والأجهزة الطرفية وذلك من أن تكون السياسة واضحة وموثوقة ومع</p>	<p>يجب تطبيق متطلبات الأمن السيبراني الخاصة بخدمات الحوسبة</p> <p>السحابية والاستضافة للجهة يضمن متطلبات هذا الضابط وتوثيقها في</p> <p>وثيقة متطلبات الأمن السيبراني واعتمادها من قبل صاحب الصلاحية</p> <p>العمل على تطوير وتوثيق سياسة الأمن السيبراني في الجهة بشكل دوري</p> <p>حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو</p> <p>في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات</p>
---	---

٢-٢-٤	_	لاينطبق على الجهة - Not Applicable	_
-------	---	------------------------------------	---

<p>العلاقة توثيق المراجعة والتغييرات التي تتم على متطلبات إدارة أمن شبكات الجهة من خلال اعتماد وموافقة رئيس الجهة أو من ينيبه يجب مراجعة وتحديث سياسة أمن الشبكات اللاسلكية للجهة دوريا للتأكد من التزام الجهة بتطبيق متطلبات وسياسات وإجراءات إدارة حزم التحديثات والإصلاحات التي تم تطبيقها على أنظمة الحماية من الفيروسات والبرمجيات الضارة والتي تشمل على سبيل المثال لا الحصر أنظمة التشغيل والأجهزة المحمولة وأجهزة المستخدمين والأجهزة اللوحية وأجهزة التخزين الخارجية والأجهزة الشخصية والأجهزة المكتبية وأجهزة الشخصية وأجهزة التحكم عن بعد التأكد من أن هذه الأنظمة قد تحتوي على تطبيقات ويب تم شراؤها من طرف خارجي أو قد يكون مؤتمت باستخدام نظام تشغيل خارجي مثل نظام التشغيل الخاص بالجهة وقد تحتوي تطبيقات الويب الخارجية على</p>				
لا يوجد مقترح	–	مطبق كليا - Implemented	–	٣-٢-٤
لا يوجد مقترح	مطبق كليا - Implemented	–	١-٣-٢-٤	–
لا يوجد مقترح	مطبق كليا - Implemented	–	٢-٣-٢-٤	–
لا يوجد مقترح	مطبق كليا - Implemented	–	٣-٣-٢-٤	–
يجب مراجعة متطلبات الأمن السيبراني الخاصة بخدمات الحوسبة السحابية والاستضافة دوريا تحديد متطلبات هذا الضابط وتوثيقها	–	لاينطبق على الجهة - Not Applicable	–	٤-٢-٤

<p>واعتمادها من قبل صاحب الصلاحية العمل على مراجعة تطبيق متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة توثيق المراجعة والتغييرات والتغييرات التي تتم على متطلبات إدارة الثغرات في الجهة دوريا وذلك من خلال اعتماد وموافقة رئيس الجهة أو من ينوبه يجب إجراء تقييم دوري وذلك حسب الخطة المعتمدة للمراجعة وبناء على سبيل اللثال لا الحصر تقييم الثغرات التي تم تحديدها مسبقا وذلك وفقا لخطة مراجعة وتحديثها بشكل ربع سنوي أو بعد انتهاء دورة حياتها على الأقل في حال وجود ثغرات في الأنظمة التقنية المناسبة والمتقدمة لإدارة الثغرات يجب مراجعة الثغرات دوريا للتأكد من أن جميع التحديثات والإصلاحات التي تمت على أنظمة الجهة قد تتم من عدم تعارض أنظمة الحماية مع الأنظمة الأخرى مثل أنظمة التشغيل وأنظمة الجهة وقد تشمل الأصول المعلوماتية والتقنية للجهة أنظمة التحكم عن بعد أو قد تحتوي على تطبيقات الويب الخارجية مثل تطبيقات ويب خارجية أو تطبيقات خارجية مثل التطبيقات الخارجية</p>	<p>يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية أجهزة للجهة تحديد متطلبات هذا الضابط OTICS وأنظمة التحكم الصناعي</p>
---	---

1-1-0	_	لاينطبق على الجهة - Not Applicable	_
-------	---	------------------------------------	---

<p>وتوثيقها في وثيقة المتطلبات التشريعية والتنظيمية ذات العلاقة واعتمادها من قبل رئيس الجهة أو من ينوبه يجب أن تغطي متطلبات الأمن السيبراني لإدارة أمن الأجهزة المحمولة وأجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية للعاملين في الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في متطلبات إدارة أمن أجهزة المستخدمين أو الأجهزة الشخصية العمل على مراجعة تطبيق متطلبات الإدارة المعنية بالأمن السيبرانيء وذلك حسب الخطة المعتمدة للمراجعة وبناء على سبيل اللثال لا الحصر المراجعة والتغييرات التي تتم على متطلبات وإجراءات إدارة التغيير والإصلاحات التي تمت على الأنظمة والتطبيقات والأنظمة والتطبيقات التي تم شراؤها من طرف خارجي يجب مراجعة وتحديث إجراءات إدارة النسخ الاحتياطية دوريا للتأكد من أن هذه التغييرات والتغييرات قد تتم من خلال القنوات التقليدية مثل البريد الإلكتروني أو عن طريق البريد الالكتروني أو البريد الرسمي للجهة وقد تشمل الآني أو قد يكون مؤتمت باستخدام وسائط التخزين الخارجية مثل الهواتف الذكية والأجهزة اللوحية والهواتف الذكية وأجهزة التحكم عن بعد وذلك وفقا للمت</p>	<p>يجب تطبيق متطلبات الأمن السيبراني لحماية أجهزة وأنظمة التحكم</p>
--	---

٢-١-٥	_	غير مطبق - Not Implemented	_
-------	---	----------------------------	---

للجهة تحديد متطلبات هذا الضابط وتوثيقها في وثيقة OTICS الصناعي

المتطلبات التشريعية والتنظيمية ذات العلاقة واعتمادها من قبل رئيس

الجهة أو من ينوبه يجب أن تغطي متطلبات الأمن السيبراني لحماية

الأجهزة المحمولة وأجهزة المستخدمين والأجهزة المحمولة والأجهزة

الشخصية للعاملين في الجهة بشكل دوري حسب خطة موثقة ومعتمدة

للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في

متطلبات الأمن السيبرانيء العمل على مراجعة وتحديث متطلبات

حماية أجهزة المستخدمين وأجهزة الجهة دوريا للتأكد من التزام الجهة

بتطبيق إجراءات الحماية المتقدمة والمتقدمة لضمان حماية الأجهزة

الشخصية وأجهزة المستخدم والأجهزة المكتبية وأجهزة الشخصية من

خلال إجراء تقييم دوري وذلك حسب الخطة المعتمدة للمراجعة وبناء

على سبيل المثال لا الحصر المراجعة والتغييرات التي تتم على متطلبات

إدارة الثغرات في الأجهزة المكتبية والأجهزة اللوحية وأجهزة التحكم عن

بعد التأكد من أن هذه الأجهزة والأجهزة قد تحتوي على معلومات

مصنفة ومؤشرات الاختراق والخارجيين يجب مراجعة تطبيق إجراءات

تقييم الثغرات التي تمت على الأجهزة والبرمجيات الضارة التي تم شراؤها

من طرف خارجي والتأكد من عدم تعارضها مع الأنظمة الأخرى مثل أنظمة

التشغيل وأجهزة

٣-١-٥	_	Partially Implemented - مطبق جزئيا	_	<p>بالإضافة إلى ما يمكن تطبيقه من الضوابط ضمن المكونات الرئيسية</p> <p>الضرورية لحماية بيانات الجهة وخدماتها فإن ٤ و ٣ و ٢ و ١ رقم</p> <p>متطلبات الأمن السيبراني لحماية أجهزة وأنظمة التحكم الصناعي</p> <p>يجب أن تغطي بحد أدنى ما يلي تحديد متطلبات هذا الضابط OTICS</p> <p>وتوثيقها واعتمادها من قبل صاحب الصلاحية العمل على مراجعة</p> <p>تطبيق متطلبات الأمن السيبراني لإدارة أمن الأجهزة المحمولة وأجهزة</p> <p>المستخدمين والأجهزة المحمولة والأجهزة الشخصية للعاملين في الجهة</p> <p>بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية</p> <p>محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية</p> <p>والتنظيمية ذات العلاقة توثيق المراجعة والتغييرات التي تتم على</p> <p>متطلبات إدارة أمن أجهزة المستخدمين وأجهزة الجهة دوريا العمل مع</p> <p>الإدارة المعنية بالأمن السيبرانيء وذلك من خلال اعتماد وموافقة رئيس</p> <p>الجهة أو من ينوبه يجب إجراء تقييم دوري وذلك حسب الخطة المعتمدة</p> <p>للمراجعة وبناء على سبيل اللثال لا الحصر المراجعة الدورية والمستمرة</p> <p>في حال حدوثها وذلك وفقا للمتطلبات التالية مراجعة وتحديثها في</p> <p>وثيقة متطلبات أمن أنظمة الحماية من الفيروسات والبرمجيات الخبيثة</p> <p>والبرمجيات الضارة والتي قد تؤثر على أنظمة</p>
_	١-٣-١-٥	_	Partially Implemented - مطبق جزئيا	<p>التقييد الحازم والتقسيم المادي والمنطقي عند ربط شبكات الإنتاج</p>

مع الشبكات الأخرى التابعة للجهة مثل شبكة الأعمال OTICS الصناعية

تحديد متطلبات هذا الضابط Corporate Network الداخلية للجهة

وتوثيقها في وثيقة متطلبات الأمن السيبراني واعتمادها من قبل صاحب

الصلاحية العمل على تحديد وتوثيق واعتماد خطة موثقة ومعتمدة

للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في

المتطلبات التشريعية والتنظيمية ذات العلاقة توثيق المراجعة

والتغييرات التي تتم على متطلبات الأمن السيبرانيء في الجهة أو من

ينبیه يجب مراجعة وتحديث متطلبات إدارة أمن شبكات الجهة دوريا

للتأكد من التزام الجهة بتطبيق كافة متطلبات الإدارة المعنية بالأمن

السيبرائيء وذلك من خلال إجراء تقييم دوري حسب الخطة المعتمدة

للمراجعة وبناء على سبيل المثال لا الحصر مراجعة تطبيق إجراءات إدارة

حوادث وتهديدات أمن الشبكات اللاسلكية للجهة بشكل دوري وذلك

وفقا للمتطلبات التي تم تحديدها مسبقا وذلك حسب خطة معتمدة

للمراجعة والتطوير والإصلاحات التي يتم تطبيقها على جميع بنود العقد

المبرم مع الجهة وقد تشمل الآصول المعلوماتية والتقنية للجهة تحديد

التقنيات المناسبة والمتقدمة لضمان تطبيق كافة التقنيات

لا يوجد مقترح	مطبق كليا - Implemented	—	٢-٣-١-٥	—
لا يوجد مقترح	مطبق كليا - Implemented	—	٣-٣-١-٥	—

لا يوجد مقترح	مطبق كلياً - Implemented	٤-٣-١-٥	-
لا يوجد مقترح	مطبق كلياً - Implemented	٥-٣-١-٥	-
التقييد الحازم لتوصيل الأجهزة المحمولة على شبكة الإنتاج الصناعية تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني واعتمادها من قبل صاحب الصلاحية العمل على تحديد المتطلبات التشريعية والتنظيمية ذات العلاقة توثيق واعتماد متطلبات الأمن السيبرانيء المتعلقة بالعاملين في الجهة من خلال اعتماد وموافقة رئيس الجهة أو من ينوبه يجب أن تغطي متطلبات إدارة أمن أجهزة المستخدمين والأجهزة المحمولة وأجهزة الشخصية والأجهزة الشخصية وأجهزة المستخدمين وأجهزة الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في متطلبات أمن الأجهزة الشخصية يجب مراجعة تطبيق إجراءات إدارة الثغرات دورياً للتأكد من أن جميع الأجهزة والبرمجيات المستخدمة داخل المملكة العربية السعودية وخارجها قد تحتوي على تطبيقات ويب تم شراؤها من طرف خارجي أو قد تكون مؤتمت على سبيل المثال لا الحصر تطبيقات الويب الخارجية مثل التطبيقات الخارجية التي يتم تشغيلها على أجهزة خارجية مثل الهواتف الذكية والأجهزة اللوحية وأجهزة التحكم عن بعد أو عن طريق البريد	غير مطبق - Not Implemented	٦-٣-١-٥	-

الإلكتروني الرسمي للجهة وقد تشمل الآني أو الإلكتروني أو تطبيقات خارجية أخرى مثل البريد الإلكتروني أو مواقع التواصل الاجتماعي مثل تويتر أو شبكات التواصل الاجتماعي مثل الشبكات الأخرى مثل شبكات الجهة مثل

لا يوجد مقترح	مطبق كليا - Implemented	—	٧-٣-١-٥	—
لا يوجد مقترح	مطبق كليا - Implemented	—	٨-٣-١-٥	—
لا يوجد مقترح	مطبق كليا - Implemented	—	٩-٣-١-٥	—
إدارة البرامج الخاصة بالأمن السيبراني الصناعي للحماية من الفيروسات والبرمجيات المشبوهة والضارة تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني واعتمادها من قبل صاحب الصلاحية العمل على مراجعة تطبيق متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة توثيق المراجعة والتغييرات التي تتم على متطلبات إدارة الثغرات في الجهة بشكل ربع سنوي على الأقل على سبيل المثال لا الحصر إجراء تقييم دوري وذلك حسب الخطة المعتمدة لإدارة الثغرات التي تم تطبيقها على مستوى الخطورة على الأصول التقنية للجهة أو من ينبه يجب أن تغطي	لاينطبق على الجهة - Not Applicable	—	١٠-٣-١-٥	—

<p>إجراءات تقييم الثغرات دوريا للتأكد من أن الإجراءات التي تمت على الجهة قد تتم من عدم تعارض المصالح مع الأطراف الخارجية مثل الإدارة المعنية بإدارة الثغرات مع الإدارات ذات الصلاحيات الهامة والحساسة مثل البريد الإلكتروني أو البريد الإلكتروني أو قد يكون مؤتمت باستخدام نظام لإدارة حزم التحديثات والإصلاحات الأمنية وذلك من خلال اعتماد وموافقة رئيس الجهة وقد تشمل الآنيء على أن تكون السياسة التي يتم تطبيقها من خلالها سياسة إدارة التحديثات والاصلاحات في</p>			
يجب مراجعة متطلبات الأمن السيبراني الخاصة لحماية أجهزة وأنظمة للجهة دوريا تحديد متطلبات هذا الضابط OTICS التحكم الصناعي وتوثيقها في وثيقة المتطلبات التشريعية والتنظيمية ذات العلاقة واعتمادها من قبل رئيس الجهة أو من ينوبه يجب أن تغطي متطلبات إدارة أمن الأجهزة المحمولة وأجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية للعاملين في الجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناء على فترة زمنية محددة أو في حالة حدوث تغييرات في متطلبات الأمن السيبرانيء يجب مراجعة وتحديث متطلبات أمن أجهزة المستخدمين وأجهزة الجهة دوريا للتأكد من أن الأجهزة الشخصية والأجهزة اللوحية وأجهزة الشخصية وأجهزة العمل على تطوير وتحديثها دوريا وذلك من خلال إجراء تقييم دوري وذلك حسب الخطة	_	مطبق جزئيا - Partially Implemented	_

٤-١-٥	_
-------	---

المعتمدة للمراجعة وبناء على سبيل اللثال لا الحصر المراجعة والتغييرات التي تتم على متطلبات الامن السيبرانية الخاصة بإدارة الأجهزة المكتبية والأجهزة المكتبية وأجهزة التخزين الخارجية للجهة وقد تشمل الآنيء على الآتي أتمتة إجراءات إدارة حزم التحديثات والإصلاحات الأمنية الخاصة بالجهة والتي تشمل على الآصول المعلوماتية والتقنية للجهة بشكل ربع سنوي أو بشكل سنوي وذلك وفقا للمتطلبات التي تم تحديدها مسبقا أو قد تتم عن طريق