الدليل الاسترشادي للأمن السيبراني

لدى أعضاء اتحاد هيئات الأوراق المالية العربية

إعداد

فريق العمل المكلف بتنفيذ أهداف و مبادرات المحور الثالث لخطة الاتحاد الاستراتيجية 2021 – 2025

حول تعزيز التعاون في مجالات التكنولوجيا المالية و المخاطر السيبرانية

دولة الإمارات العربية المتحدة

حزيران / يونيو 2024

المحتويات

التمهيد

تعريف الأمن السيبراني

يعرف المعهد الوطني للمعايير والتقنية (NIST) الأمن السيبراني بأنه "عملية حماية المعلومات عن طريق منع الهجمات من خلال كشفها والتصدي لها". وعلى غرار المخاطر المالية والمخاطر ذات الصلة بالسمعة، يمكن لمخاطر الأمن السيبراني أن تؤدي إلى ارتفاع التكاليف والتأثير في العائدات. كذلك من شأنها الإضرار بقدرة المؤسسة على الابتكار واكتساب العملاء والمحافظة عليهم.

أما المنظمة الدولية للمعايير (ISO) فترى أن الأمن السيبراني أو الفضاء السيبراني يتمثل في الحفاظ على السرية والسلامة وتوافر المعلومات في الفضاء السيبراني. ويُعرّف "الفضاء السيبراني" بدوره بأنه "البيئة الناتجة عن تفاعل الأفراد مع البرمجيات والخدمات المتاحة عبر الإنترنت عن طريق الأجهزة التقنية والشبكات المتصلة به، والتي ليس لها وجود مادي".

وفي حالة اعتماد الاتفاقيات أو الالتزامات الدولية التي تتضمن متطلبات ذات صلة بالأمن السيبراني على الصعيد المحلي، فيجب أن تلتزم الجهة بإحدى هذه المتطلبات (NIST) أو (ISO).

أهداف الأمن السيبراني

تتضمن الأهداف العامة للأمن السيبراني التالي:

- **السرية:** اتخاذ التدابير اللازمة لمنع اطلاع غير المصرح لهم على المعلومات الحساسة والسرية.
- **سلامة المعلومة:** الحماية ضد تعديل المعلومات أو تخريبها بشكل غير مصرح به، وتتضمن ضمان عدم الإنكار للمعلومات (Non-Repudiation) والموثوقية.
- **توافر المعلومة:** ضمان الوصول إلى البيانات والمعلومات والأنظمة والتطبيقات واستخدامها في الوقت المناسب.

1. المقدمة

أعدت هذه الوثيقة بالاستعانة والاسترشاد بعدد من الأطر التنظيمية والمعايير القياسية المحلية والدولية والتي كان من ضمنها ضوابط المنظمة الدولية للمعايير (ISO).

1.1. الهدف

يهدف الدليل الاسترشادي للأمن السيبراني لاتحاد هيئات الأوراق المالية العربية (ويشار إليها لاحقًا بـ "الدليل الاسترشادي") إلى تحديد الضوابط المتعلقة بالأمن السيبراني لدى أعضاء الاتحاد التي تساعد على تحسين إدارة المخاطر الأمن السيبراني من خلال تبني أفضل الممارسات العالمية وتشريعات الأمن السيبراني المحلية.

1.2. نطاق العمل

يوضح الدليل الاسترشادي الضوابط المتعلقة بالأمن السيبراني لاتحاد هيئات الأوراق المالية العربية.

1.3. قابلية التطبيق

تعد هذه الوثيقة استرشادية على جميع أعضاء اتحاد هيئات الأوراق المالية العربية.

1.4. المراجعة والتحديث

يضطلع فريق عمل المخاطر السيبرانية بالمراجعة الدورية للدليل الاسترشادي وفقًا للمستجدات والمتطلبات التنظيمية ذات العلاقة، وتحديثها متى تطلب الأمر ذلك.

2. المكونات الفرعية

الشكل 1 المكونات الفرعية

2.1. حوكمة الامن السيبراني

1-1	إدارة الأمن السيبراني
الهدف	تحديد الهيكل التنظيمي للأمن السيبراني والأدوار والمسؤوليات وتوثيقها وتنفيذها واعتمادها من قبل إدارة الجهة.
الضوابط	
1-1-1	إنشاء وحدة تنظيمية معنية بالأمن السيبراني مستقلة عن الوحدة التنظيمية الخاصة بإدارة عمليات تقنية المعلومات مع الأخذ بالاعتبار عدم تعارض المصالح تطبيق الهيكل التنظيمي المناسب لإدارة الأمن السيبراني بما يتماشى مع الجهات المشرعة في الدولة وبما لا يتعارض مع تعارض المصالح
2-1-1	تخصيص واعتماد ميزانية كافية لتنفيذ مهام وأعمال الأمن السيبراني من قبل مجلس إدارة الجهة.
3-1-1	إنشاء لجنة معنية بالأمن السيبراني على أن ترتبط بالرئيس التنفيذي للجهة أو من ينوب عنه مع الأخذ بالاعتبار عدم تعارض المصالح.
4-1-1	إعداد لائحة عمل للجنة المعنية بالأمن السيبراني وتوثيقها واعتمادها من صاحب الصلاحية، مع توضيح الأهداف والأدوار والمسؤوليات.
5-1-1	ان تتضمن مسؤوليات لجنة الأمن السيبراني التالي:
	1-5-1-1 مراقبة درجة تَقبُّل مخاطر الأمن السيبراني للجهة ومراجعتها والإبلاغ عنها بشكل دوري أو عند حدوث تغيير جوهري بخصوص معدل تقبل المخاطر.
	2-5-1-1 المراجعة الدورية لاستراتيجية الأمن السيبراني لضمان دعمها لأهداف الجهة.
	3-5-1-1 اعتماد ونشر وتوفير الدعم اللازم والمراقبة بشأن: • حوكمة الأمن السيبراني • استراتيجية الأمن السيبراني • سياسات الأمن السيبراني • برامج الأمن السيبراني (مثل: برامج التوعية، وبرامج تصنيف البيانات، وخصوصية البيانات، ومنع ترسيب البيانات) • إدارة مخاطر الأمن السيبراني • مؤشرات المخاطر الرئيسية ومؤشرات الأداء الرئيسية للأمن السيبراني
6-1-1	تتضمن مسؤوليات مدير الوحدة التنظيمية المختصة بالأمن السيبراني، على سبيل المثال، التالي:
	1-6-1-1 الرفع إلى اللجنة المعنية بالأمن السيبراني حول أي تطوير وتحديث لما يلي: • استراتيجية الأمن السيبراني • سياسات الأمن السيبراني • بنية الأمن السيبراني • إدارة مخاطر الأمن السيبراني
	2-6-1-1 ضمان تحديد معايير وإجراءات الأمن السيبراني وتوثيقها واعتمادها وتنفيذها
	3-6-1-1 ضمان تطوير وتدريب موظفي الأمن السيبراني
	4-6-1-1 مراقبة أنشطة الأمن السيبراني (مراقبة مركز العمليات الأمنية)
	5-6-1-1 مراقبة الالتزام بأنظمة وسياسات ومعايير وإجراءات الأمن السيبراني
	6-6-1-1 الإشراف على التحقيق في حوادث الأمن السيبراني
	7-6-1-1 الحصول على المعلومات الاستباقية (Threat Intelligence) والتعامل معها
	8-6-1-1 مراجعة وتدقيق برنامج الأمن السيبراني
	9-6-1-1 الدعم الفعال للوظائف الأخرى المتعلقة بالأمن السيبراني
	10-6-1-1 تصميم برامج التوعية بالأمن السيبراني وتنفيذها
	11-6-1-1 القياس والإبلاغ عن مؤشرات المخاطر الرئيسية ومؤشرات الأداء الرئيسية بشأن: • استراتيجية الأمن السيبراني • الالتزام بسياسات الأمن السيبراني • معايير وإجراءات الأمن السيبراني

	• برامج الأمن السيبراني (مثل برامج التوعية، وبرنامج تصنيف البيانات)
7-1-1	يُناط بجميع موظفي الجهة مسؤولية الالتزام بسياسات الأمن السيبراني ومعاييرها وإجراءاتها.
2-1	**سياسات وإجراءات الأمن السيبراني**
الهدف	تحديد سياسات واستراتيجية الأمن السيبراني وتوثيقها واعتمادها وتنفيذها ونشرها لذوي العلاقة والالتزام بها.
الضوابط	
1-2-1	تحديد سياسات الأمن السيبراني، وتوثيقها، واعتمادها، ونشرها لذوي العلاقة والأطراف المعنية.
2-2-1	ضمان تنفيذ والالتزام بسياسات الأمن السيبراني وتحديثها بشكل دوري.
3-2-1	مراجعة سياسات الأمن السيبراني بشكل دوري وفقًا لخطة مراجعة محددة مسبقًا.
4-2-1	تتضمن سياسات الأمن السيبراني، على سبيل المثال، التالي: 1-4-2-1 تعريف بالأمن السيبراني 2-4-2-1 نطاق وأهداف الأمن السيبراني للجهة 3-4-2-1 دعم الإدارة العليا لبرنامج الأمن السيبراني وأهدافه 4-4-2-1 تعريف المسؤوليات والأدوار للأمن السيبراني 5-4-2-1 الإشارة إلى مرجعية معايير الأمن السيبراني المطبقة 6-4-2-1 تتضمن ضوابط الأمن السيبراني التالي: • تصنيف المعلومات بطريقة توضح أهميتها للجهة • تحديد الملكية لأصول المعلومات كافة • تقييم مخاطر الأمن السيبراني لأصول المعلومات • توعية العاملين في الجهة بالأمن السيبراني • الالتزام بالاتفاقيات والالتزامات التنظيمية والتعاقدية • الإبلاغ عن اختراقات الأمن السيبراني والثغرات الأمنية المشتبه فيها • تطبيق متطلبات الأمن السيبراني على إدارة استمرارية الأعمال
3-1	**المراجعة والتدقيق الدوري للأمن السيبراني**
الهدف	تحديد آلية المراجعة والتدقيق والتقييم الدوري لضوابط الأمن السيبراني المتعلقة بأصول الجهة المعلوماتية والتقنية؛ للتأكد من أن ضوابط الأمن السيبراني لدى الجهة مطبقة وفقًا للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
1-3-1	إجراء مراجعة وتدقيق لتطبيق ضوابط الأمن السيبراني بشكل دوري
2-3-1	مراجعة تطبيق ضوابط الأمن السيبراني من قبل أطراف مستقلة عن إدارة الأمن السيبراني وفقًا للمعايير العامة المقبولة للمراجعة والتدقيق بما يتماشى مع الدليل الاسترشادي للأمن السيبراني للجهات
4-1	**برنامج التوعية والتدريب بالأمن السيبراني**
الهدف	تحديد برنامج خاص بالأمن السيبراني لتدريب وتوعية موظفي الجهة وعملائها والأطراف الخارجية ذات العلاقة؛ لحماية الأصول المعلوماتية والتقنية للجهة
الضوابط	
1-4-1	تطوير برنامج توعية بالأمن السيبراني، واعتماده، وتوثيقة، وتنفيذه؛ لتعزيز الوعي بالأمن السيبراني
2-4-1	ضمان تنفيذ برنامج التوعية بالأمن السيبراني بشكل دوري
3-4-1	يتضمن برنامج التدريب والتوعية الخاص بالأمن السيبراني الحماية من التهديدات السيبرانية شاملًا: 1-3-4-1 الأدوار والمسؤوليات المتعلقة بالأمن السيبراني 2-3-4-1 معلومات عن حوادث الأمن السيبراني والتهديدات السيبرانية، على سبيل المثال: التصيد الإلكتروني 3-3-4-1 التعامل الآمن مع الأجهزة المحمولة ووسائط التخزين 4-3-4-1 التصفح الآمن للإنترنت 5-3-4-1 التعامل الآمن مع مواقع التواصل الاجتماعي
	6-3-4-1 التعامل الآمن مع البريد الالكتروني

2.2. تعزيز الامن السيبراني

1-2	**إدارة الأصول المعلوماتية والتقنية**

الهدف	تحديد عملية إدارة الأصول المعلوماتية والتقنية وتوثيقها واعتمادها وتنفيذها ونشرها ومراقبتها بهدف الحصول على سجل دقيق موحد ومحدث للأصول , وذلك لدعم الجهة في الحصول على قائمة جرد دقيقة وحديثة.
الضوابط	
1-1-2	تحديد عملية إدارة الأصول المعلوماتية والتقنية، وتوثيقها، واعتمادها، وتنفيذها، ومراقبتها، وتقييمها بشكل دوري.
2-1-2	يجب تطبيق متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة.
2-2	**إدارة هويات الدخول والصلاحيات**
الهدف	تقييد الوصول إلى أصول المعلومات وفقا لمتطلبات العمل المعنية وبما يتماشى مع مبادئ الحاجة إلى المعرفة والاستخدام وذلك لضمان توافر امتيازات وصول كافية ومصرح بها لاعتماد المستخدمين ,"Know-to-Need or Have-to-Need
الضوابط	
1-2-2	إدارة وصول المستخدمين
2-2-2	استخدام تقنية المصادقة متعددة العوامل لعمليات الدخول عن بعد والتطبيقات الخارجية للتحكم في الوصول (كمبدأ الحاجة إلى المعرفة والاستخدام" Have-to-Need Know-to-Need "ومبدأ الحد الادنى من الصلاحيات والامتيازات "Least Privilege")؛
3-2-2	إدارة الصلاحيات الهامة والحساسة
4-2-2	تحديد سياسة إدارة هويات الدخول والصلاحيات، وتوثيقها، واعتمادها، وتنفيذها، ومراقبتها
5-2-2	قياس مدى فعالية ضوابط الأمن السيبراني ضمن سياسة إدارة هويات الدخول والصلاحيات وتقييمها بشكل دوري
3-2	**حماية الأنظمة وأجهزة معالجة المعلومات**
الهدف	ضمان حماية الأنظمة, أجهزة معالجة المعلومات. بما في ذلك أجهزة المستخدمين والخوادم وأجهزة الشبكة للجهة من المخاطر السيبرانية.
الضوابط	
1-3-2	تحديد عملية إدارة تهديدات الأمن السيبراني، وتوثيقها، واعتمادها، وتنفيذها كما يجب ان تغطي بحد أدني ما يلي:
	2-3-1-1 الحماية من الفيروسات , والبرامج والأنشطة المشبوهة ,والبرمجيات الضارة على الخوادم , واجهزة المستخدمين والأجهزة المحمولة ,باستخدام تقنيات الحماية الحديثة وآلياتها وإدارتها بشكل آمن.
	2-3-1-2 تغيير الإعدادات الافتراضية/ الضعيفة
2-3-2	يجب الالتزام بتطبيق ضوابط الأمن السيبراني وحماية الأنظمة واجهزة معالجه المعلومات.
4-2	**حماية البريد الالكتروني**
الهدف	ضمان حماية البريد الالكتروني للجهة من المخاطر السيبرانية وتوثيقها واعتمادها وتنفيذها
الضوابط	
1-4-2	تطبيق نظام التصفية الخاص بمكافحة الرسائل الإلكتروني التطفلية ورسائل التصيد الإلكتروني "Filtering spam-Anti"و "phishing Emails"
2-4-2	مصادقة مجال البريد الالكتروني بالطرق التقنية مثل طريقة إطار سياسة المرسل ("Sender Policy Framework)
3-4-2	يجب تطبيق متطلبات الأمن السيبراني الخاصة بالبريد الالكتروني للجهة
5-2	**إدارة أمن الشبكات**
الهدف	تحديد ضوابط الأمن السيبراني للشبكات وتوثيقها واعتمادها وتنفيذها؛ ومراقبة الالتزام بهذه ضوابط وتقييم مدى فعاليتها داخل الجهة بشكل دوري.
الضوابط	

1-5-2	تحديد متطلبات الأمن السيبراني لإدارة أمن الشبكات، وتوثيقها، واعتمادها، وتنفيذها.
	2-5-1-1 استخدام جدران الحماية للشبكة وبوابات الوصول الآمنة.
	2-5-1-2 العزل والتقسيم المادي أو المنطقي لأجزاء الشبكات بشكل آمن.
	2-5-1-3 أمن الشبكات اللاسلكية, وحمايتها, باستخدام وسائل آمنة.
2-5-2	يجب تطبيق متطلبات الأمن السيبراني لإدارة أمن الشبكات
2-6	**التشفير**
الهدف	تحديد استخدام حلول التشفير داخل الجهة وتوثيقها واعتمادها وتنفيذها؛ لضمان حماية الوصول إلى المعلومات الحساسة وسلامتها.
الضوابط	
2-6-1	تحديد معايير التشفير، وتوثيقها، واعتمادها، وتنفيذها. وتشمل:
	2-6-1-1 تشفير البيانات أثناء النقل والتخزين بناء على تصنيفها وبحسب أفضل الممارسات والمعايير والمتطلبات التشريعية والتنظيمية ذات الصلة.
	2-6-1-2 أن يتضمن معيار التشفير استعراض عام لحلول التشفير المعتمدة والقيود المطبقة عليها (تقنيا وتنظيميا).
2-6-2	مراقبة الالتزام بمعايير التشفير.
2-7	**إدارة النسخ الاحتياطية**
الهدف	تحديد عملية إدارة النسخ الاحتياطية لضمان حماية البيانات والمعلومات والإعدادات التقنية للأنظمة والتطبيقات الخاصة من الأضرار غير المتوقعة.
الضوابط	
2-7-1	تحديد متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية، وتوثيقها، واعتمادها، وتنفيذها. وتشمل:
	2-7-1-1 إجراء نسخ احتياطية للأنظمة الأعمال الحساسة.
	2-7-1-2 إجراء فحص دوري لاختبار استعادة النسخ الاحتياطي
2-7-2	يجب تطبيق متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية.
2-8	**إدارة الثغرات**
الهدف	تحديد عملية إدارة الثغرات الأمنية وتوثيقها واعتمادها وتنفيذها لتحديد الثغرات الأمنية في التطبيقات والبنية التحتية والتخفيف من آثارها، وقياس مدى فعالية هذه العملية، وتقييم تأثيرها بشكل دوري.
الضوابط	
2-8-1	تحديد عملية إدارة الثغرات، وتوثيقها، واعتمادها، وتنفيذها. وتشمل:
	2-8-1-1 إدارة حزم التحديثات الأمنية وأساليب تطبيقها.
	2-8-1-2 إجراء فحص الثغرات بشكل دوري.
	2-8-1-3 تحديد جداول زمنية لمعالجة الثغرات بناء على تصنيفها.
2-8-2	يجب تطبيق متطلبات الأمن السيبراني لإدارة الثغرات التقنية.
2-9	**اختبار الاختراق**
الهدف	تحديد عملية اختبار الاختراق للتطبيقات وتوثيقها واعتمادها وتنفيذها؛ لاختبار مدى فعالية تعزيز الأمن السيبراني في الجهة من خلال محاكاة لتقنيات الهجوم السيبراني الفعلية واكتشاف نقاط الضعف الغير معروفة. كذلك يجب قياس مدى فعالية هذه العملية وتقييمها بشكل دوري.
الضوابط	
2-9-1	تحديد عملية اختبار الاختراق، وتوثيقها، واعتمادها، وتنفيذها.
2-9-2	تنفيذ اختبارات الاختراق لجميع الخدمات المقدمة خارجيًا (عن طريق الإنترنت) سنويًا بحد أدنى.
2-10	**إدارة سجلات أحداث الأمن**
الهدف	تحديد عملية إدارة سجلات أحداث الأمن السيبراني وتوثيقها واعتمادها وتنفيذها لتحليل التسجيل الأمني والتشغيلي والتعامل مع أحداث الأمن السيبراني. كذلك يجب قياس مدى فعالية

	هذه العملية وتقييمها بشكل دوري؛ لضمان التعرف على الأحداث المشتبه فيها المتعلقة بأصول المعلومات، والاستجابة لها في الوقت المناسب.
الضوابط	
2-10-1	تحديد عملية إدارة سجلات الأمن السيبراني، وتوثيقها، واعتمادها، وتنفيذها.
2-10-2	تحديد معايير الأحداث الواجب مراقبتها بناء على تصنيف أصول المعلومات أو ملف المخاطر، بحيث يتم تفعيل سجلات الأحداث على الأصول المعلوماتية الحساسة.
2-10-3	الاشتراك لدى مقدم خدمة مركز العمليات الأمنية "SOC".
2-10-4	قياس مدى فعالية ضوابط الأمن السيبراني في عملية إدارة سجلات أحداث الأمن السيبراني، وتقييمها بشكل.
2-11	**إدارة حوادث الأمن السيبراني**
الهدف	تحديد عملية إدارة حوادث الأمن السيبراني التي تتوافق مع إدارة حوادث الجهة وتوثيقها واعتمادها وتنفيذها لتحديد حوادث الأمن السيبراني والاستجابة لها والتغلب عليها. كذلك قياس مدى فعالية هذه العملية، وتقييمها بشكل دوري؛ وذلك لضمان تحديد حوادث الأمن السيبراني ومعالجتها في الوقت المناسب للحد من التأثير السلبي المحتمل للحادث في الجهة.
الضوابط	
2-11-1	تطوير عملية إدارة حوادث الأمن السيبراني، وتوثيقها، واعتمادها، وتنفيذها، ومواءمتها مع عملية إدارة حوادث الجهة.
2-11-2	قياس مدى فعالية ضوابط الأمن السيبراني في عملية إدارة حوادث الأمن السيبراني، وتقييمها بشكل دوري.
2-11-4	التعاون في مشاركة معلومات الأمن السيبراني مع الاتحاد.
2-12	**الأمن المادي**
الهدف	الحماية المادية لجميع مرافق الجهة لمنع الوصول المادي غير المصرح به وضمان حماية الجهة.
الضوابط	
2-12-1	تحديد ضوابط الأمن المادي، وتوثيقها، واعتمادها، وتنفيذها.
2-12-2	مراقبة مدى فعالية ضوابط الأمن المادي، وقياسها، وتقييمها بشكل دوري.
2-12-3	حماية غرف تقنية المعلومات الأجهزة الإلكترونية الحساسة والأجهزة الطرفية المحمولة، أو الوثائق من الوصول غير المصرح به.
2-12-4	تحديد معايير وإجراءات الإتلاف الآمن، وتوثيقها، واعتمادها، وتنفيذها، بحيث النسخ الرقمية والورقية وإعادة استخدام الأصول

2.3. الأمن السيبراني المتعلق بالأطراف الخارجية والموردين

3-1	**الأمن السيبراني المتعلق بالأطراف الخارجية والموردين**
الهدف	حماية أصول الجهة من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية والموردين بما في ذلك موفرو خدمات الإسناد ومقدمو الخدمات الخارجية.
الضوابط	
3-1-1	تحديد ضوابط ومتطلبات الأمن السيبراني بين الجهة والأطراف الخارجية، وتوثيقها، واعتمادها، وتنفيذها، ومراقبتها.
3-1-2	تحديد اتفاقية المحافظة على سرية البيانات
3-2	**الحوسبة السحابية**
الهدف	تحديد ضوابط الأمن السيبراني في استخدام الحوسبة السحابية وعملية الخدمات السحابية والاستضافة وتوثيقها واعتمادها وتنفيذها ومراقبتها، وقياس مدى فعالية ضوابط الأمن السيبراني المحددة وتقييمها.
الضوابط	

1-2-3	تحديد ضوابط الأمن السيبراني ضمن سياسة الحوسبة السحابية للخدمات السحابية والاستضافة، وتوثيقها، واعتمادها، وتنفيذها، ونشرها داخل الجهة
2-2-3	مراقبة الالتزام بسياسة الحوسبة السحابية.
3-2-3	قياس ضوابط الأمن السيبراني المتعلقة بسياسة الحوسبة السحابية وعملية الخدمات السحابية والاستضافة، وتقييمها بشكل دوري.
4-2-3	تتضمن ضوابط الأمن السيبراني لسياسة الحوسبة السحابية للخدمات السحابية التالي:
	1-4-2-3 عملية اعتماد الخدمات السحابية، وتشمل: • إجراء تقييم لمخاطر الأمن من السيبراني تجاه مزود الخدمة السحابية والخدمات السحابية؛ • إبرام عقد يشمل ضوابط الأمن السيبراني، وذلك قبل استخدام الخدمات السحابية؛
	2-4-2-3 إجراء تصنيف البيانات قبل استضافتها؛
	3-4-2-3 موقع البيانات، ويشمل الالتزام باستخدام الخدمات السحابية حسب ضوابط الجهات المشرعة بالدولة
	4-4-2-3 قيود استخدام البيانات، وتشمل عدم استخدام مزود الخدمة السحابية بيانات الجهة لأغراض أخرى؛
	5-4-2-3 الحماية، ويجب على مزود الخدمة السحابية تطبيق ضوابط الأمن السيبراني ومراقبتها على النحو المحدد في تقييم المخاطر؛ وذلك من أجل حماية سرية بيانات الجهة وسلامتها وضمان توافرها؛
	6-4-2-3 فصل البيانات، ويشمل فصل بيانات الجهة عن البيانات الأخرى التي يحتفظ بها مزود الخدمة السحابية بشكل ملائم، بحيث يكون مزود الخدمة السحابية قادرا على تحديد بيانات الجهة في جميع الأوقات وتمييزها عن البيانات الأخرى.
	7-4-2-3 استمرارية الأعمال، ويتضمن ذلك تلبية متطلبات استمرارية الأعمال وفقا لسياسة استمرارية الأعمال المعتمدة لدى الجهة؛
	8-4-2-3 أحقية الجهة في إجراء مراجعة وتدقيق وفحص الأمن السيبراني لدى مزود الخدمة السحابية؛
	9-4-2-3 الإنهاء، ويشمل: • حقوق الجهة في الأنهاء؛ • حقوق الجهة باستعادة بياناتها من قبل مزود الخدمة السحابية عند الإنهاء في صيغة مناسبة يمكن استخدامها؛ • حقوق الجهة بالمطالبة بحذف بياناتها من قبل مزود الخدمة السحابية عند الإنهاء بشكل غير قابل للاستعادة .