الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

الدليل الإرشادي لتطبيق ضوابط الأمن السيبراني للبيانات

Guide to Data Cybersecurity Controls Implementation (GDCC – 1 : 2023)

إشارة المشاركة: أبيض
تصنيف الوثيقة: عام

إخلاء مسؤولية: طُور هذا الدليل الإرشادي عن طريق الهيئة الوطنية للأمن السيبراني لتمكين الجهات من تطبيق ضوابط الأمن السيبراني للبيانات، كما تخلي الهيئة الوطنية للأمن السيبراني مسؤوليتها من الاعتماد على هذه الوثيقة فقط؛ وتؤكد على ضرورة الأخذ بعين الاعتبار المتطلبات الخاصة بالجهة وبيئتها؛ وتؤكد الهيئة الوطنية للأمن السيبراني بأن هذه الوثيقة ماهي إلا دليل إرشادي يمكن استخدامه كمثال ولا تعني بالضرورة أن تكون الطريقة الوحيدة لتطبيق الضوابط على ألا تتعارض الطرق الأخرى مع متطلبات الهيئة الوطنية للأمن السيبراني. تحتوي هذه الوثيقة على بعض الأمثلة للمخرجات ذات العلاقة بتطبيق الضوابط، ويحق للمقيم أو المدقق أن يطلب أدلة أخرى حسب ما يراه المقييم أو المدقق لضمان التأكد من تطبيق جميع الضوابط.

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 للإستلام.

برتقالي – مشاركة محدودة

المستلم بالإشارة البرتقالية يمكنه مشاركة المعلومات في نفس المنشأة مع الأشخاص المعنين 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

قائمة المحتويات

مقدمة 5
الهدف 5
نطاق العمل 5
مكونات وهيكلية ضوابط الأمن السيبراني للبيانات 5
هيكلية الدليل الإرشادي 7
إرشادات عامة لتطبيق ضوابط الأمن السيبراني للبيانات 8
إرشادات تطبيق ضوابط الأمن السيبراني للبيانات 9

قائمة الأشكال

شكل 1: المكونات الأساسية والفرعية لضوابط الأمن السيبراني للبيانات 6
شكل 2: هيكلية الدليل الإرشادي لضوابط الأمن السيبراني للبيانات 7

مقدمة

طورت الهيئة الوطنية للأمن السيبراني (ويشار لها في هذه الوثيقة بـ "الهيئة") الدليل الإرشادي لتطبيق ضوابط الأمن السيبراني المنصوص عليها في ضوابط الأمن السيبراني للبيانات (DCC-1:2022) (ويشار لها في هذه الوثيقة بـ "الضوابط")، وذلك للمساهمة في تمكين الجهات الوطنية من تطبيق متطلبات الالتزام بضوابط الأمن السيبراني للبيانات. حيث تم بناء هذا الدليل الإرشادي بالاعتماد على المعلومات والخبرات التي قامت الهيئة بجمعها وتحليلها منذ نشر الضوابط ومواءمة هذا الدليل الإرشادي مع أفضل الممارسات الرائدة في الأمن السيبراني لتسهيل تطبيق الضوابط في الجهات الوطنية.

الهدف

الهدف الرئيسي من هذا الدليل الإرشادي هو المساهمة في تمكين الجهات الوطنية لتحقيق متطلبات الالتزام بتطبيق ضوابط الأمن السيبراني للبيانات في الجهة، وذلك بهدف رفع وتعزيز مستوى الأمن السيبراني لديها، وتقليل مخاطر الأمن السيبراني التي تنشأ من التهديدات السيبرانية الداخلية.

نطاق العمل

نطاق العمل لهذا الدليل مطابق لما هو مذكور في ضوابط الأمن السيبراني للبيانات (DCC-1: 2022) وهو:

- تطبق هذه الضوابط على الجهات الحكومية في المملكة العربية السعودية (وتشمل الوزارات والهيئات والمؤسسات وغيرها) والجهات والشركات التابعة لها، وتطبق على جهات القطاع الخاص التي تمتلك بنى تحتية وطنية حساسة أو تقوم بتشغيلها أو استضافتها، ويشار لها جميعاً في هذه الوثيقة بـ(الجهة) بالإضافة إلى شركات الخدمات الاستشارية العاملة ضمن المشاريع الاستراتيجية ذات الحساسية العالية.

- تطبق الضوابط على جميع أشكال البيانات المادية والرقمية، والتي تشمل البيانات المهيكلة (مثل قواعد البيانات، وجداول البيانات) والبيانات غير المهيكلة (مثل الوثائق والمستندات).

- تشجع الهيئة الجهات الأخرى في المملكة وبشدة على الاستفادة من هذه الضوابط لتطبيق أفضل الممارسات في ما يتعلق بتحسن الأمن السيبراني وتطويره داخل الجهة.

مكونات وهيكلية ضوابط الأمن السيبراني للبيانات

يوضح الشكل رقم (1) أدناه المكونات الأساسية والفرعية لضوابط الأمن السيبراني للبيانات.

1	حوكمة الأمن السيبراني Cybersecurity Governance	1-1	المراجعة والتدقيق الدوري للأمن السيبراني Periodical Cybersecurity Review and Audit	2-1	الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources
		3-1	برنامج التوعية والتدريب بالأمن السيبراني Cybersecurity Awareness and Training Program		
2	تعزيز الأمن السيبراني Cybersecurity Defense	1-2	إدارة هويات الدخول والصلاحيات Identity and Access Management	2-2	حماية الأنظمة وأجهزة معالجة المعلومات Information System and Processing Facilities Protection
		3-2	أمن الأجهزة المحمولة Mobile Devices Security	4-2	حماية البيانات والمعلومات Data and Information Protection
		5-2	التشفير Cryptography	6-2	الإتلاف الآمن للبيانات Secure Data Disposal
		7-2	الأمن السيبراني للطابعات والماسحات الضوئية وآلات التصوير Cypersecurity for Printers, Scanners and Copy Machines		
3	الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية Third-Party and Cloud Computing Cybersecurity	1-3	الأمن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity		

هيكلية الدليل الإرشادي

يوضح الشكل رقم (2) أدناه هيكلية الدليل الإرشادي لتطبيق ضوابط الأمن السيبراني للبيانات.

1	اسم المكون الأساسي
الرقم المرجعي للمكون الأساسي	
الرقم المرجعي للمكون الفرعي	اسم المكون الفرعي
الهدف	
الضوابط	
الرقم المرجعي للضابط	بنود الضابط
إرشادات تطبيق الضوابط:	
المخرجات المتوقعة:	

شكل 1: هيكلية الدليل الإرشادي لتطبيق ضوابط الأمن السيبراني للبيانات

إرشادات عامة لتطبيق ضوابط الأمن السيبراني للبيانات

إرشادات عامة
• تحديد بيانات الجهة وملّاكها والعمل على تصنيفها وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة، ومراجعتها بشكل دوري. • تحديد الأصول التقنية والأنظمة التي تنتج أو تعالج أو تخزن بيانات الجهة، ومراجعتها بشكل دوري. • تحديد وتوثيق متطلبات الأمن السيبراني للبيانات للجهة والأدوار والمسؤوليات المتعلقة بها، واعتمادها من قبل صاحب الصلاحية ومراجعتها بشكل دوري. • مراجعة الدليل الإرشادي لتطبيق الضوابط الأساسية للأمن السيبراني والعمل على تطبيق الضوابط ذات العلاقة بضوابط الأمن السيبراني للبيانات. • وضع خطة ضوابط الأمن السيبراني للبيانات، ومتابعتها بشكل مستمر.

إرشادات تطبيق ضوابط الأمن السيبراني للبيانات

1 حوكمة الأمن السيبراني (Cybersecurity Governance)

1-1	المراجعة والتدقيق الدوري للأمن السيبراني (Periodical Cybersecurity Review and Audit)
الهدف	ضمان التأكد من أن ضوابط الأمن السيبراني لدى الجهة مطبقة وتعمل وفقاً للسياسات والإجراءات التنظيمية للجهة, والمتطلبات التشريعية والتنظيمية الوطنية ذات العلاقة, والمتطلبات الدولية المقرة تنظيمياً على الجهة
الضوابط	
1-1-1	رجوعاً للضابط 1-8-1 في الضوابط الأساسية في الأمن السيبراني, فإنه يجب على الإدارة المعنية بالأمن السيبراني في الجهة مراجعة تطبيق ضوابط الأمن السيبراني للبيانات حسب المدة المحددة لكل مستوى.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج إجراء تدقيق الأمن السيبراني • نموذج سياسة مراجعة وتدقيق الأمن السيبراني • نموذج سجل خطة تدقيق الأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • مراجعة تطبيق جميع متطلبات الأمن السيبراني للبيانات في الجهة حسب مستوى تصنيف البيانات. • إجراء المراجعة كل سنة على الأقل لجميع مستويات تصنيف البيانات. • تنفيذ المراجعة لتطبيق ضوابط الأمن السيبراني للبيانات كل سنة على الأقل لجميع مستويات تصنيف البيانات. • توثيق واعتماد خطة مراجعة بناءً على الفترة الزمنية المحددة لضمان تطبيق ضوابط الأمن السيبراني بفعالية والعمل وفقًا للسياسات والإجراءات التنظيمية ، بالاضافة إلى القوانين واللوائح والاتفاقيات الوطنية والدولية ذات الصلة.
	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • تقرير مراجعة لجميع مستويات تصنيف البيانات كل سنة على الأقل.
1-2-1	رجوعاً للضابط 2-8-1 في الضوابط الأساسية في الأمن السيبراني, فإنه يجب أن تتم مراجعة تطبيق ضوابط الأمن السيبراني للبيانات من قبل أطراف مستقلة عن الإدارة المعنية بالأمن السيبراني من داخل الجهة حسب المدة المحددة لكل مستوى.

	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة مراجعة وتدقيق الأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • تحديد الأطراف المستقلة عن الإدارة المعنية بالأمن السيبراني للجهة، مثل إدارة التدقيق الداخلي أو مدققي الطرف الخارجي، لمراجعة تطبيق ضوابط الأمن السيبراني للبيانات في الجهة. • إجراء المراجعة كل سنتين على الأقل لمستوى البيانات المصنفة عام أو مقيد و سنوياً على الأقل لمستوى البيانات المصنفة سري أو سري للغاية. • تنفيذ وتطبيق ضوابط الأمن السيبراني للبيانات من قبل أطراف مستقلة عن الإدارة المعنية بالأمن السيبراني من داخل الجهة حسب المدة المحددة لكل مستوى. • توثيق خطة مراجعة تطبيق معتمدة بناءً على الفترة الزمنية المحددة للتأكد من أن ضوابط الأمن السيبراني للبيانات يتم تطبيقها بشكل فعال وتعمل بما يتماشى مع السياسات والإجراءات التنظيمية للجهة والمتطلبات القانونية والتنظيمية الوطنية ذات الصلة والمتطلبات الدولية .
	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • تقرير مدققي الأطراف المستقلة الذي تم إجراؤه على جميع متطلبات الأمن السيبراني للبيانات في الجهة.
2-1	**الأمن السيبراني المتعلق بالموارد البشرية (Cybersecurity in Human Resources)**
الهدف	ضمان التأكد من أن مخاطر ومتطلبات الأمن السيبراني المتعلقة بالعاملين (موظفين ومتعاقدين) في الجهة تعالج بفاعلية قبل وأثناء وعند إنتهاء/إنهاء عملهم, وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة, والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
1-2-1	بالإضافة للضوابط الفرعية ضمن الضابط 3-9-1 في الضوابط الأساسية للأمن السيبراني يجب أن تغطي متطلبات الأمن السيبراني المتعلقة بالموارد البشرية لتشمل خلال وبعد إنتهاء/إنهاء العلاقة الوظيفية في الجهة بحد أدنى ما يلي:
1-1-2-1	إجراء مسح أمني (Screening and vetting) للعاملين في الوظائف ذات العلاقة بالتعامل مع البيانات.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للموارد البشرية **إرشادات تطبيق الضوابط:**

		• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • تحديد المرشحين المناسبين لوظائف معالجة البيانات السرية والسرية للغاية بناءً على مجموعة المهارات والكفاءات اللازمة. • مراجعة وتقييم مهارات وكفاءات المرشحين باستخدام منهجيات مختلفة بما في ذلك المقابلات والاختبارات الشفوية أو التحريرية. أيضًا ، تطوير عملية المسح الأمني على المرشحين الذين تم اختيارهم إما عن طريق فريق داخلي أو طرف ثالث. • تطوير وتوثيق واعتماد خطة عمل لمنح صلاحيات الوصول للمرشحين وفقًا للأدوار والصلاحيات المطلوبة . • تطوير عملية مراجعة دورية لإزالة الأدوار والصلاحيات غير المستخدمة وغير المبررة بعد انقضاء حاجتها أو مدتها.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • عملية التوظيف والإعداد التي تشمل المسح الأمني حسب مهارات المرشح. • اختيار الفريق المختص بالمسح الأمني إما عن طريق فريق داخلي أو طرف ثالث. • قائمة المستخدمين التي تم التحقق منها والموافقة عليها بشكل دوري مع صلاحياتهم (مثل مسؤول الخصوصية / حماية البيانات). • مراجعة سياسة الأمن السيبراني للموارد البشرية بما يتماشى مع سياسات الأمن السيبراني للبيانات.
	2-1-2-1	تعهد العاملين في الجهة بعدم إستخدام تطبيقات التراسل أو التواصل الإجتماعي أوخدمات التخزين السحابية الشخصية لإنشاء أو تخزين أومشاركة البيانات الخاصة بالجهة، بإستثناء تطبيقات التراسل الآمنة المعتمدة من الجهات ذات العلاقة.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للموارد البشرية • نموذج الالتزام بسياسات الأمن السيبراني • نموذج اتفاقية السرية **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • تحديد الموظفين الذين سيعملون على البيانات المقيدة أو السرية أو السرية للغاية، بناءً على التصنيف. • مراجعة وتطوير وتوثيق عقود التوظيف للموظفين بمساعدة الإدارة المعنية بالقانون داخل الجهة، للتعهد بعدم استخدام أنظمة الذكاء الاصطناعي التوليدي ووسائل التواصل الاجتماعي

		وتطبيقات التواصل والتراسل لإنشاء أو تخزين أو مشاركة بيانات الجهة، باستثناء أنظمة الذكاء الاصطناعي التوليدي وتطبيقات التراسل الآمنة المعتمدة من الجهات ذات العلاقة.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • توقيع اتفاقية من قبل الموظفين فيما يخص استخدام أنظمة الذكاء الاصطناعي التوليدي ووسائل التواصل الاجتماعي ، واستخدام تطبيقات التراسل الآمنة.
3-1	**برنامج التوعية والتدريب بالأمن السيبراني (Cybersecurity Awareness and Training Program)**	
الهدف	ضمان التأكد من أن العاملين بالجهة لديهم التوعية الأمنية اللازمة وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني والتأكد من تزويد العاملين بالجهة بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة والقيام بمسؤولياتهم تجاه الأمن السيبراني.	
الضوابط		
1-3-1	بالإضافة للضوابط الفرعية ضمن الضابط 3-10-1 في الضوابط الأساسية للأمن السيبراني، فإنه يجب أن يغطي برنامج التوعية بالأمن السيبراني المحاور المتعلقة بحماية البيانات، بما في ذلك:	
	1-1-3-1 مخاطر تسريب والوصول غير المصرح به للبيانات خلال دورة حياتها.	**أدوات الأمن السيبراني ذات العلاقة:** • خطة برنامج التوعية بالأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • يجب أن يخضع جميع الموظفين في الجهة لبرنامج التوعية بالأمن السيبراني لحماية وتصنيف البيانات ، مع جلسات توعية مخصصة للموظفين الجدد قبل منح الوصول إلى بيانات الجهة. • تطوير وتوثيق برنامج توعية للأمن السيبراني لحماية البيانات ، والذي يجب أن يشمل موضوعات مثل مقدمة عن تسريب البيانات ، وما يعتبر تسرباً للبيانات مثل استخدام أنظمة الذكاء الاصطناعي التوليدي غير المعتمدة، والمخاطر المرتبطة بتسريب البيانات ، وخطة العمل التي يجب اتباعها في حالة حدوث تسرب أو الوصول غير المصرح به إلى البيانات أثناء دورة حياتها. • تنفيذ برنامج التوعية بالأمن السيبراني لحماية البيانات بشكل دوري والاحتفاظ بسجل للتدريب.

		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • برنامج توعية مخصص وموثق ومعتمد لحماية البيانات والذي يتضمن مخاطر تسريب البيانات والوصول غير المصرح به إلى البيانات خلال دورة حياتها. • عينة من مكونات برنامج التوعية ذات الصلة (رسائل البريد الإلكتروني التوعوية ، وجلسات التوعية ، وحملات اختبار الوعي ، وما إلى ذلك).
	2-1-3-1	التعامل الآمن مع البيانات المصنفة خلال السفر والتواجد خارج مكان العمل.
		أدوات الأمن السيبراني ذات العلاقة: • خطة برنامج التوعية بالأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • يجب أن يخضع جميع العاملين في الجهة لبرنامج التوعية بالأمن السيبراني لحماية البيانات. • تطوير وتوثيق برنامج توعية للأمن السيبراني لحماية البيانات ، والذي يجب أن يتضمن موضوعات مثل إدخال البيانات لتصنيف البيانات ، وسياسة تصنيف البيانات ، والتعامل الآمن مع البيانات السرية أثناء التواجد خارج مكان العمل والسفر. • إجراء برنامج التوعية بالأمن السيبراني لحماية البيانات بشكل دوري والاحتفاظ بسجل للتدريب.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • برنامج توعية مخصص وموثق ومعتمد لحماية البيانات والذي يتضمن التعامل الآمن مع البيانات المصنفة خلال السفر والتواجد خارج مكان العمل. • عينة من مكونات برنامج التوعية ذات الصلة (رسائل البريد الإلكتروني التوعوية ، وجلسات التوعية ، وحملات اختبار الوعي ، وما إلى ذلك).
	3-1-3-1	التعامل الآمن مع البيانات خلال الإجتماعات (الإفتراضية والحضورية).
		أدوات الأمن السيبراني ذات العلاقة: • خطة برنامج التوعية بالأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • يجب أن يخضع جميع العاملين في الجهة لبرنامج التوعية بالأمن السيبراني لحماية البيانات.

		• تطوير وتوثيق برنامج توعية بالأمن السيبراني لحماية البيانات ، والذي يجب أن يتضمن تبادل البيانات مع جمهور أوسع ، والتخلص المناسب من المعلومات بعد تسجيل البيانات أثناء الاجتماعات. • تنفيذ برنامج التوعية بالأمن السيبراني لحماية البيانات بشكل دوري والاحتفاظ بسجل للتدريب.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • برنامج توعية موثق ومعتمد مخصص لحماية البيانات والذي يتضمن التعامل الآمن مع البيانات أثناء الاجتماعات. • عينة من مكونات برنامج التوعية ذات الصلة (رسائل البريد الإلكتروني التوعوية ، وجلسات التوعية ، وحملات اختبار الوعي ، وما إلى ذلك).
	4-1-3-1	الإستخدام الآمن للطابعات والماسحات الضوئية وآلات التصوير.
		أدوات الأمن السيبراني ذات العلاقة: • خطة برنامج التوعية بالأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • يجب أن يخضع جميع العاملين في الجهة لبرنامج التوعية بالأمن السيبراني لحماية البيانات. • تطوير وتوثيق برنامج توعية بالأمن السيبراني لحماية البيانات ، والذي يجب أن يتضمن موضوعات مثل تقييد استخدام الطابعة من الوصول غير المصرح به ، إعدادات الوصول عن بُعد للطابعات والماسحات الضوئية ، التنبه للبيانات المطبوعة والتخلص المناسب إذا لم تعد البيانات مطلوبة. • إجراء برنامج التوعية بالأمن السيبراني لحماية البيانات بشكل دوري والاحتفاظ بسجل للتدريب.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • برنامج توعية مخصص وموثق ومعتمد لحماية البيانات يتضمن الاستخدام الآمن للطابعات والماسحات الضوئية وآلات التصوير. • عينة من مكونات برنامج التوعية ذات الصلة (رسائل البريد الإلكتروني التوعوية ، وجلسات التوعية ، وحملات اختبار الوعي ، وما إلى ذلك).
	5-1-3-1	إجراءات الإتلاف الآمن للبيانات.
		أدوات الأمن السيبراني ذات العلاقة: • خطة برنامج التوعية بالأمن السيبراني **إرشادات تطبيق الضوابط:**

		• العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • يجب أن يخضع جميع العاملين في الجهة لبرنامج التوعية بالأمن السيبراني لحماية البيانات. • تطوير وتوثيق برنامج توعية للأمن السيبراني لحماية البيانات ، وسياسة الإتلاف الآمن للبيانات ، وعملية الإتلاف الآمن للبيانات ، والتمزيق أو الإتلاف ، ومعلومات حول الطرف الخارجي المختص بإتلاف البيانات ، إن وجد. • إجراء برنامج التوعية بالأمن السيبراني لحماية البيانات بشكل دوري والاحتفاظ بسجل للتدريب.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • برنامج توعية مخصص وموثق ومعتمد لحماية البيانات يتضمن إجراءات الإتلاف الآمن للبيانات. • عينة من مكونات برنامج التوعية ذات الصلة (رسائل البريد الإلكتروني التوعوية ، وجلسات التوعية ، وحملات اختبار الوعي ، وما إلى ذلك).
	6-1-3-1	مخاطر مشاركة الوثائق والمعلومات من خلال قنوات تواصل غير مؤمنة.
		أدوات الأمن السيبراني ذات العلاقة: • خطة برنامج التوعية بالأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • يجب أن يخضع جميع العاملين في الجهة لبرنامج التوعية بالأمن السيبراني لحماية البيانات. • تطوير وتوثيق برنامج توعية بالأمن السيبراني لحماية البيانات ، والذي يجب أن يتضمن موضوعات مثل القنوات المناسبة لمشاركة المستندات في الشركة ، والمخاطر المرتبطة بتسريب البيانات مثل استخدام أنظمة الذكاء الاصطناعي التوليدي غير المعتمدة، والعقوبات المرتبطة بمشاركة المستندات من خلال قنوات غير آمنة. • إجراء برنامج التوعية بالأمن السيبراني لحماية البيانات بشكل دوري والاحتفاظ بسجل للتدريب.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • برنامج توعية مخصص وموثق ومعتمد لحماية البيانات يتضمن مخاطر مشاركة الوثائق والمعلومات من خلال قنوات تواصل غير مؤمنة. • عينة من مكونات برنامج التوعية ذات الصلة (رسائل البريد الإلكتروني التوعوية ، وجلسات التوعية ، وحملات اختبار الوعي ، وما إلى ذلك).
	7-1-3-1	المخاطر السيبرانية المتعلقة بإستخدام وسائط التخزين الخارجية.

		أدوات الأمن السيبراني ذات العلاقة: • خطة برنامج التوعية بالأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • يجب أن يخضع جميع العاملين في الجهة لبرنامج التوعية بالأمن السيبراني لحماية البيانات. • تطوير وتوثيق برنامج توعية للأمن السيبراني لحماية البيانات ، والذي يجب أن يتضمن موضوعات مثل سياسة وسائط التخزين ، واستخدام وحدات وسائط التخزين الخارجية في الجهة ، والمخاطر المرتبطة بتسريب البيانات من جهاز التخزين ، وعملية الموافقة على استخدام وسائط التخزين الخارجية ، إذا لزم الأمر. • إجراء برنامج التوعية بالأمن السيبراني لحماية البيانات بشكل دوري والاحتفاظ بسجل للتدريب.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • برنامج توعية مخصص موثق ومعتمد لحماية البيانات يتضمن المخاطر السيبرانية المتعلقة باستخدام وسائط التخزين الخارجية. • عينة من مكونات برنامج التوعية ذات الصلة (رسائل البريد الإلكتروني التوعوية ، وجلسات التوعية ، وحملات اختبار الوعي ، وما إلى ذلك).



2 تعزيز الأمن السيبراني (Cybersecurity Defense)

1-2	إدارة هويات الدخول والصلاحيات (Identity and Access Management)	
الهدف	ضمان حماية الأمن السيبراني للوصول المنطقي (Logical Access) إلى الأصول المعلوماتية والتقنية للجهة؛ من أجل منع الوصول غير المصرح به، وتقييد الوصول إلى ما هو مطلوب؛ لإنجاز الأعمال المتعلقة بالجهة.	
الضوابط		
1-1-2	بالإضافة للضوابط الفرعية ضمن الضابط 2-2-3 في الضوابط الأساسية للأمن السيبراني, يجب أن تغطي متطلبات الأمن السيبراني المتعلقة بإدارة هويات الدخول والصلاحيات، بحد أدنى؛ مايلي:	
	1-1-1-2	التقييد الحازم بالسماح للحد الأدنى من العاملين للوصول والاطلاع ومشاركة البيانات بناء على قوائم صلاحيات مقتصرة على موظفين سعوديين إلا بموجب استثناء من قبل صاحب الصلاحية (رئيس الجهة أو من يفوضه) وعلى أن يتم إعتماد هذه القوائم من قبل صاحب الصلاحية.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار إدارة هويات الدخول والصلاحيات، بحيث يشمل إدارة كلمات المرور • نموذج سياسة إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • تحديد قائمة الموظفين المعتمدة في الجهة الذين لديهم حق الوصول إلى البيانات السرية والسرية للغاية والتحقق ان يكونوا سعودين. • يجب اعتماد قائمة الصلاحيات الحساسة على البيانات السرية والسرية للغاية والمحافظة عليها ومراجعتها من قبل صاحب الصلاحية (رئيس الجهة أو من يفوضه).
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • سياسة إدارة الصلاحيات الهامة والحساسة الموثقة والمعتمدة. • قائمة الامتيازات المعتمدة للبيانات السرية والسرية للغاية من قبل صاحب الصلاحية (رئيس الجهة أو من يفوضه).

		• مراجعة سياسة الأدوار والمسؤوليات بما يتماشى مع سياسات الأمن السيبراني للبيانات.
	2-1-1-2	منع مشاركة قوائم الصلاحيات المعتمدة مع الأشخاص غير المصرح لهم.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار إدارة هويات الدخول والصلاحيات، بحيث يشمل إدارة كلمات المرور • نموذج سياسة إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • حصر قوائم الصلاحيات المعتمدة والعمل على منع مشاركة هذه القوائم مع الأشخاص غير المصرح لهم • مراجعة عملية منح الصلاحيات لقائمة الصلاحيات المعتمدة والتحقق من وجود آلية الموافقة المناسبة. • يجب إجراء مراجعة دورية على الصلاحيات المعتمدة إلى البيانات السرية والسرية للغاية.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • سياسة إدارة هويات الدخول والصلاحيات الموثقة والمعتمدة. • الاحتفاظ بقائمة من المستخدمين الذين لديهم صلاحيات هامة وحساسة.
	2-1-2	إدارة هويات الدخول وصلاحيات الاطلاع على البيانات بإستخدام أنظمة إدارة الصلاحيات الهامة والحساسة (Privileged Access Management).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار إدارة هويات الدخول والصلاحيات، بحيث يشمل إدارة كلمات المرور • نموذج سياسة إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • تتم إدارة الوصول إلى البيانات المقيدة والسرية والسرية للغاية باستخدام نظام إدارة الصلاحيات الهامة والحساسة. • تحديد وتطبيق نظام إدارة الصلاحيات الهامة والحساسة ، وفقًا لمتطلبات الجهة ، لإدارة الهويات الذين لديهم حق الوصول للاطلاع على البيانات. • التحقق من أن تقنيات إدارة الوصول المناسبة مطبقة وفعالة لادارة الصلاحيات الهامة والحساسة.

	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • سجلات تتبع الهويات التي لديها حق الوصول إلى البيانات المقيدة والسرية والسرية للغاية. • وثائق توضح إجراءات المراجعة والتقييم الدوري. • امتثال نظام PAM لمتطلبات الجهة. • إجراء اختبارات منتظمة لنظام PAM لضمان فعاليته. • وثائق توضح كيفية استخدام تقنيات إدارة الوصول لإدارة الصلاحيات الهامة والحساسة. • وثائق توضح إجراءات الصيانة والمراقبة لتقنيات إدارة الوصول.
3-1-2	بالإضافة للضابط الفرعي 2-2-3-5 في الضوابط الأساسية للأمن السيبراني، يجب مراجعة قوائم الصلاحيات المعتمدة والصلاحيات المستخدمة للتعامل مع البيانات حسب المدة المحددة لكل مستوى.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار إدارة هويات الدخول والصلاحيات، بحيث يشمل إدارة كلمات المرور • نموذج سياسة إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • تطوير وتوثيق الإجراءات وخطة العمل للمراجعة الدورية لقوائم الصلاحيات الهامة والحساسة للمستخدمين في حالة تغيير أدوار الموظفين. • يجب إجراء المراجعة سنوياً على الأقل لمستوى تصنيف البيانات العامة أو المقيدة وكل ثلاثة أشهر على الأقل لمستوى تصنيف البيانات السرية أو السرية للغاية.
	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • خطة عمل للمراجعة الدورية لهويات المستخدمين وحق الوصول. • تقارير للمراجعة الدورية لهويات المستخدمين وحقوق الوصول التي تم إجراؤها.
2-2	**حماية الأنظمة وأجهزة معالجة المعلومات (Information System and Processing Facilities Protection)**
الهدف	ضمان حماية الأنظمة وأجهزة معالجة المعلومات بما في ذلك أجهزة المستخدمين والبنى التحتية للجهة من المخاطر السيبرانية.
الضوابط	
1-2-2	بالإضافة للضوابط الفرعية ضمن الضابط 2-3-2 في الضوابط الأساسية للأمن السيبراني، يجب أن تشمل متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات، بحد أدنى، مايلي:

	1-1-2-2	تطبيق حزم التحديثات والإصلاحات الأمنية من وقت إطلاقها للأنظمة المستخدمة للتعامل مع البيانات حسب المدة المحددة لكل مستوى.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة حزم التحديثات والإصلاحات • نموذج معيار إدارة التحديثات والإصلاحات **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • تحديد الأنظمة والخدمات التي تتعامل مع البيانات بجميع التصنيفات. • مراجعة إرشادات الاصلاحات والتحديثات فيما يتعلق بالأنظمة والخدمات المستخدمة وتوثيق إجراءات التحديثات التي يجب اتباعها بما يتماشى مع الإرشادات. • يجب إجراء الاصلاحات والتحديثات الأمنية الدورية كل شهر على الأقل وذلك للأنظمة والخدمات التي تتعامل مع البيانات العامة أو المقيدة ، وعلى الفور للأنظمة والخدمات التي تتعامل مع البيانات السرية أو السرية للغاية.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • إجراءات الاصلاحات والتحديثات الأمنية الموثقة للأنظمة والخدمات التي تتعامل مع البيانات. • تقرير مراجعة الاصلاحات والتحديثات بشكل دوري.
	2-1-2-2	مراجعة إعدادات الحماية والتحصين للأنظمة المستخدمة للتعامل مع البيانات (Security Configuration and Hardening) حسب المدة المحددة لكل مستوى.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة حزم التحديثات والإصلاحات • نموذج سياسة الإعدادات والتحصين • نموذج معايير الإعدادات والتحصين الآمن **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • تحديد الأنظمة المستخدمة للتعامل مع البيانات. • مراجعة إرشادات إعدادات الحماية والتحصين فيما يتعلق بالأنظمة المستخدمة وتوثيق إجراءات التحصين التي يجب اتباعها بما يتماشى مع الإرشادات.

		• يجب إجراء إعدادات الحماية والتحصين بشكل سنوي على الأقل وذلك للأنظمة التي تتعامل مع البيانات العامة أو المقيدة ، وكل ستة أشهر على الأقل للأنظمة والخدمات التي تتعامل مع البيانات السرية أو السرية للغاية.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • معيار معتمد لمراجعة إعدادات الحماية والتحصين لأنظمة معالجة البيانات (على سبيل المثال نسخة معتمدة ورقية أو إلكترونية). • التقارير التي تفيد بأن إعدادات الحماية والتحصين للأنظمة المستخدمة للتعامل مع البيانات حسب المدة المحددة لكل مستوى تتم مراجعتها.
	3-1-2-2	مراجعة وتحصين الإعدادات المصنعية (مثل كلمة المرور الثابتة، والخلفية الافتراضية) للأصول التقنية المستخدمة للتعامل مع البيانات.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة حزم التحديثات والإصلاحات **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • تحديد الأصول التقنية وأنظمة معالجة البيانات على جميع التصنيفات. • مراجعة الإعدادات الافتراضية التي تشمل ، على سبيل المثال لا الحصر: كلمات المرور الافتراضية وحسابات الزوار وحسابات الخدمة والخلفيات والمسؤولين الافتراضيين والبروتوكولات القديمة والمنافذ المفتوحة في النظام. • التحقق والتأكد من أن الإعدادات الأمنية لن يتم تعيينها على أنها افتراضية للأصول التقنية.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • تقرير مراجعة الإعدادات الافتراضية للأصول التقنية.
	4-1-2-2	تعطيل خاصية تصوير الشاشة (Print Screen or Screen Capture) للأجهزة التي تنشئ أوتعالج الوثائق.

		إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • تحديد الأجهزة التي تعالج البيانات السرية والسرية للغاية للجهة. • المراجعة والتحقق من أن ميزات(Print Screen أو Screen Capture) تصوير الشاشة على الأجهزة تم تعطيلها.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • تقرير المراجعة والتحقق من تعطيل ميزات تصوير شاشة الأجهزة التي تنشئ وتعالج الوثائق السرية والسرية للغاية. • عينة من الإعدادات الأمنية للنظام.
3-2	أمن الأجهزة المحمولة (Mobile Devices Security)	
الهدف	ضمان حماية أجهزة الجهة المحمولة (بما في ذلك أجهزة الحاسب المحمول والهواتف الذكية والأجهزة الذكية اللوحية) من المخاطر السيبرانية. وضمان التعامل بشكل آمن مع المعلومات الحساسة والمعلومات الخاصة بأعمال الجهة وحمايتها أثناء النقل والتخزين والمعالجة عند استخدام الأجهزة الشخصية للعاملين في الجهة (مبدأ "BYOD").	
الضوابط		
1-3-2	بالإضافة للضوابط الفرعية ضمن الضابط 2-6-3 في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة, بحد أدنى؛ ما يلي:	
	1-1-3-2	إدارة الأجهزة المحمولة المملوكة للجهة مركزياً بإستخدام نظام إدارة الأجهزة المحمولة (Mobile Device Management - MDM) وتفعيل خاصية الحذف عن بعد.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية • نموذج معيار أمن الأجهزة المحمولة **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • تحديد قائمة الأجهزة المحمولة في الجهة التي تخزن وتستخدم وتعالج بيانات الجهة.

		• تحديد وتطبيق نظام إدارة الأجهزة المحمولة (MDM) ، وفقًا لمتطلبات الجهة، لإدارة الأجهزة المحمولة التي يمكنها الوصول إلى البيانات. • مراجعة أن نظام MDM يجب أن يكون به خاصية الحذف عن بعد وتمكينها على جميع الأجهزة.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • قائمة موثقة بجميع الأجهزة المحمولة في الجهة التي تتعامل مع البيانات. • خطة تطبيق نظام إدارة الأجهزة المحمولة (MDM). • لقطة شاشة لنظام إدارة الأجهزة المحمولة (MDM) قيد الاستخدام. • عينة من إعدادات نظام إدارة الأجهزة المحمولة (MDM).
	2-1-3-2	إدارة أجهزة (BYOD) مركزياً بإستخدام نظام إدارة الأجهزة المحمولة (Mobile Device Management - MDM) وتفعيل خاصية الحذف عن بعد.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • تحديد قائمة الأجهزة المحمولة للموظفين خارج الجهة التي تخزن وتستخدم وتعالج بيانات الجهة. • تحديد وتطبيق نظام إدارة الأجهزة المحمولة (MDM) ، وفقًا لمتطلبات الجهة ، لإدارة الأجهزة المحمولة التي يمكنها الوصول إلى البيانات العامة والسرية للجهة. • مراجعة أن نظام إدارة الأجهزة المحمولة يحتوي على وظيفة السحب / الحذف عن بُعد ممكّنة في جميع أجهزة (BYOD). • التحقق من أن أجهزة (BYOD) لا يحق لها الوصول إلى أي بيانات سرية أو سرية للغاية للجهة. • التأكد من عدم استخدام أجهزة (BYOD) للبيانات السرية والسرية للغاية.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • قائمة موثقة بجميع الأجهزة المحمولة للموظفين خارج الجهة التي تتعامل مع بيانات الجهة. • خطة تطبيق نظام إدارة الأجهزة المحمولة (MDM) لأجهزة BYOD.
4-2	حماية البيانات والمعلومات (Data and Information Protection)	

الهدف	ضمان حماية السرية وسلامة بيانات ومعلومات الجهة ودقتها وتوافرها، وذلك وفقًا للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.	
الضوابط		
1-4-2	بالإضافة للضوابط الفرعية ضمن الضابط 2-7-3 في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بحماية البيانات والمعلومات، بحد أدنى، ما يلي:	
	1-1-4-2	إستخدام خاصية العلامات المائية لترميز كامل الوثيقة عند الإنشاء والتخزين والطباعة وعلى الشاشة وعلى كل نسخة بحيث يكون الرمز يمكن تتبعه على مستوى المستخدم أو الجهاز. **أدوات الأمن السيبراني ذات العلاقة:** • نموذج سياسة الأمن السيبراني للبيانات • نموذج معيار الأمن السيبراني للبيانات **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • مراجعة واختيار البرنامج أو النظام المستخدم في إنشاء وتخزين وطباعة وعرض البيانات في الجهة ، والتي لديها القدرة على ترميز البيانات باستخدام العلامة المائية وفقًا لتصنيف البيانات والرقم الفريد الذي يمكن تتبعه طوال دورة حياة المستند. • تطبيق الميزات المذكورة أعلاه لجميع مستندات البيانات السرية والسرية للغاية أثناء إنشاء المستند أو تخزينه أو طباعته أو عرضه. • تحديد وتعريف سياسة تصنيف البيانات لتشمل وضع العلامات المائية والترميز التي يمكن تتبعها لوثائق الجهة. **المخرجات المتوقعة:** • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • خطة تطبيق للعلامة المائية والترميز لتمكين تتبعها في برنامج أو نظام المستند. • سياسة الأمن السيبراني للبيانات الموثقة والمعتمدة والتي تتضمن ميزات التوثيق للبيانات السرية والسرية للغاية. • عينة من وثيقة عليها علامة مائية.
	2-1-4-2	إستخدام تقنيات منع تسريب البيانات (Data Leakage Prevention) وتقنيات إدارة الصلاحيات (Rights Management).

		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للبيانات • نموذج معيار الحماية من فقدان البيانات **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • تحديد وتوثيق معايير منع تسريب البيانات (DLP) ومعايير إدارة الصلاحيات. • تحديد وتطبيق أنظمة منع تسريب البيانات (DLP) وإدارة الصلاحيات وفقًا لمتطلبات البيانات المقيدة والسرية والسرية للغاية. • مراجعة تقنيات منع تسريب البيانات التي يجب أن تشمل ، على سبيل المثال لا الحصر: قاعدة تحديد الحوادث وآلية تصفية الرسائل ومنع تسريب البيانات للأجهزة والشبكة والحوسبة السحابية \ أو التخزين وإمكانيات تصفية المحتوى والاستجابة للحوادث والمعالجة. • مراجعة تقنيات إدارة الصلاحيات التي يجب أن تشمل على سبيل المثال لا الحصر: التزويد الآلي ومراقبة النشاط المميز وتدقيق تسجيل الدخول وأدوات إدارة كلمات المرور وإدارة إدخال (LDAP) والتحقق من الهوية متعدد العناصر.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • معيار موثق لمنع تسريب البيانات. • خطة تطبيق نظام منع تسريب البيانات (DLP). • خطة تنفيذية لنظام إدارة الصلاحيات. • لقطة شاشة لمنع تسريب البيانات (DLP) وأنظمة إدارة الصلاحيات قيد الاستخدام. • عينة من إعدادات أنظمة منع تسريب البيانات (DLP) وأنظمة إدارة الصلاحيات.
	3-1-4-2	حظر إستخدام البيانات في أي بيئة غير بيئة الإنتاج (Production Environment) إلا بعد إجراء تقييم للمخاطر وتطبيق ضوابط لحماية تلك البيانات, مثل تقنيات تعتيم البيانات (Data Masking) أو تقنيات مزج البيانات (Data Scrambling).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للبيانات **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • تحديد والاحتفاظ بسجل لجميع البيئات بخلاف بيئة الإنتاج. • المراجعة والتحقق من أن ترحيل البيانات المقيدة والسرية والسرية للغاية في بيئة الإنتاج غير مسموح به في البيئات غير الإنتاجية. ومع ذلك ، في حالة حاجة العمل ، يجب تطبيق الضوابط

		المناسبة ، والتي تشمل ، على سبيل المثال لا الحصر: تعتيم البيانات / مزج البيانات ، وتطهير البيانات ، وإخفاء هوية البيانات ، وتشفير البيانات ، وتقييم الإدارة المعنية بالأمن السيبراني للمخاطر. • تطوير وتوثيق ضوابط الأمن السيبراني التي تشمل تقييم مخاطر ترحيل البيانات ، وحماية البيانات أثناء الترحيل من خلال تقنيات الحماية (مثل تعتيم البيانات ، ومزج البيانات ، وما إلى ذلك). • تطوير وتوثيق الإجراءات المتعلقة بترحيل بيانات الإنتاج في البيئات غير الإنتاجية.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • إجراءات وضوابط موثقة حول ترحيل بيانات الإنتاج إلى بيئات اخرى.
	4-1-4-2	إستخدام خدمة حماية العلامة التجارية لحماية هوية الجهة من الإنتحال (Brand Protection).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار الحماية من فقدان البيانات **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • تحديد والاحتفاظ بسجل لجميع الهويات بالعلامة التجارية للجهة على الإنترنت والتي قد تكون عرضة لانتحال الهوية. • مراجعة الموردين المتاحين الذين يقدمون خدمات حماية العلامة التجارية وتحليل مدى ملاءمة الخدمة بناءً على متطلبات الجهة. • مراجعة وتطبيق خدمة حماية العلامة التجارية لهوية الجهة.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • قائمة موثقة من الهويات في الجهة المعرضة لانتحال الهوية. • خطة تطبيق خدمة حماية العلامة التجارية للمورد. • عينة من تقارير وتنبيهات حماية العلامة التجارية.
5-2	التشفير (Cryptography)	

الهدف	ضمان الاستخدام السليم والفعال للتشفير؛ لحماية الأصول المعلوماتية الإلكترونية للجهة، وذلك وفقًا للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.	
الضوابط		
1-5-2	بالإضافة للضوابط الفرعية ضمن الضابط 2-8-3 في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني للتشفير في الجهة، بحد أدنى؛ ما يلي:	
	1-1-5-2	استخدام طرق وخوارزميات محدثة وآمنة للتشفير عند الإنشاء والتخزين والمشاركة وعلى كامل الاتصال الشبكي المستخدم لنقل البيانات وفقاً للمستوى المتقدم (Advanced) ضمن المعايير الوطنية للتشفير (NCS-1:2020).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار التشفير • نموذج سياسة التشفير • نموذج معيار إدارة مفاتيح التشفير **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • تحديد وتوثيق جميع خوارزميات التشفير أثناء النقل وأثناء التخزين للبيانات السرية والسرية للغاية للجهة. • المراجعة والتحقق من أن خوارزميات التشفير المستخدمة في الجهة للبيانات المذكورة أعلاه متوافقة مع متطلبات "المستوى المتقدم" في معايير التشفير الوطنية (NCS-1: 2020). **المخرجات المتوقعة:** • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • تقنيات التشفير الموثقة المستخدمة للبيانات السرية والسرية للغاية الخاصة بالجهة. • عينة من إعدادات نظام التشفير.
	2-1-5-2	استخدام طرق وخوارزميات محدثة وآمنة للتشفير عند الإنشاء والتخزين والمشاركة وعلى كامل الاتصال الشبكي المستخدم لنقل البيانات وفقاً للمستوى المتوسط (Moderate) ضمن المعايير الوطنية للتشفير (NCS-1:2020).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة التشفير • نموذج معيار إدارة مفاتيح التشفير

		إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • تحديد وتوثيق جميع خوارزميات التشفير أثناء النقل وأثناء التخزين للبيانات المقيدة للجهة. • المراجعة والتحقق من أن خوارزميات التشفير المستخدمة في الجهة للبيانات المذكورة أعلاه متوافقة مع متطلبات "المستوى المتوسط" في معايير التشفير الوطنية (NCS-1: 2020). **المخرجات المتوقعة:** • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • تقنيات التشفير الموثقة المستخدمة للبيانات السرية للجهة.
6-2	الإتلاف الآمن للبيانات (Secure Data Disposal)	
الهدف	ضمان تنفيذ عمليات إتلاف البيانات بشكل آمن, وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة , والمتطلبات التشريعية والتنظيمية ذات العلاقة.	
الضوابط		
1-6-2	يجب أن تغطي متطلبات الإتلاف الآمن للبيانات في الجهة بحد أدنى، ما يلي:	
	1-1-6-2 تحديد التقنيات والأدوات والإجراءات اللازمة لتنفيذ عمليات الإتلاف الآمن للبيانات حسب مستوى تصنيف البيانات.	
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعلق بالأمن المادي • نموذج معيار الأمن المادي **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • تحديد قائمة الأصول المادية للتخزين الداخلي والمتنقل مثل محركات الأقراص الصلبة الخارجية ومحركات الأشرطة وأجهزة التخزين الضوئية وتخزين الفلاش وما إلى ذلك المستخدمة لتخزين البيانات المقيدة والسرية والسرية للغاية الخاصة بالجهة. • تحديد وتوثيق خطة إتلاف البيانات من أجهزة التخزين المذكورة أعلاه بطريقة آمنة.

		• مراجعة آلية الإتلاف الآمن للبيانات والتي يجب أن تشمل ، على سبيل المثال لا الحصر: حذف البيانات باستخدام برامج مقدمة من طرف خارجي ، والكتابة ، وإعادة التنسيق ؛ التخلص من البيانات باستخدام الإتلاف المادي لأصول التخزين أو بالاستعانة بخدمات الاطراف الخارجية.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • قائمة موثقة بأصول التخزين التي تتعامل مع بيانات مقيدة أو سرية أو سرية للغاية. • خطة إتلاف البيانات الموثقة لأدوات التخزين.
	2-1-6-2	عند إنتهاء الحاجة لإستخدام وسائط التخزين بشكل نهائي, يجب أن يتم الإتلاف الآمن (Secure Disposal) لوسائط التخزين وذلك بإستخدام التقنيات والأدوات وبإتباع الإجراءات التي تم تحديدها في الضابط 2-6-1-1.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار الأمن المادي **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • تطبيق وتنفيذ الإتلاف الآمن لوسائط التخزين عند إنتهاء الحاجة لإستخدام وسائط التخزين بشكل نهائي. • تحديد و توثيق خطة إتلاف البيانات لأجهزة التخزين المذكورة أعلاه بطريقة آمنة. • مراجعة وتطبيق آلية التخلص من الجهاز المستخدم في عملية الإتلاف والتي تضمن الإتلاف النهائي بعد الاستعادة. علاوة على ذلك ، في حالة استخدام خدمة طرف خارجي ، يتم مراجعتها والتحقق منها والموافقة عليها وفقًا لمتطلبات الجهة.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • قائمة موثقة بالأصول المادية للتخزين الداخلي والمتنقل المستخدمة لتخزين البيانات المقيدة والسرية والسرية للغاية الخاصة بالجهة. • الاجراء المعتمد للاتلاف الآمن للبيانات الموثقة ولوسائط التخزين. • خطة تطبيق خدمة الطرف الخارجي من جهاز إتلاف البيانات ، إذا لزم الأمر. • عينة من سجلات / تقارير الإتلاف.
	3-1-6-2	عند الحاجة لإعادة إستخدام وسائط التخزين, يجب أن يتم الحذف الآمن للبيانات (Secure Erasure), بحيث لايمكن إسترجاعها.

		أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار الأمن المادي **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • تحديد وتوثيق خطة إتلاف البيانات المذكورة أعلاه بطريقة آمنة. • مراجعة وتطبيق تقنيات حذف البيانات المستخدمة في عملية حذف البيانات التي تضمن الحذف الدائم للبيانات بعد الاسترداد ، دون أي ضرر على قابلية استخدام الجهاز. علاوة على ذلك ، في حالة استخدام برنامج أو خدمة تابعة لطرف خارجي ، يتم مراجعتها والتحقق منها والموافقة عليها وفقًا لمتطلبات الجهة.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • قائمة موثقة بأصول التخزين التي تتعامل مع بيانات مقيدة أو سرية أو سرية للغاية. • خطة حذف البيانات الموثقة لأدوات التخزين. • خطة تطبيق حذف البيانات ، بما في ذلك إجراءات لبرامج أو خدمة الطرف الخارجي لحذف البيانات ، إذا لزم الأمر.
	4-1-6-2	يجب أن يتم التحقق من تنفيذ عمليات الإتلاف أو الحذف الآمن للبيانات المشار إليها في الضابطين رقم 2-6-1-2 و 2-6-1-3.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار الأمن المادي **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • مراجعة خطة التنفيذ لعمليات الإتلاف الآمن للبيانات في الجهة لوسائط التخزين التي تتعامل مع بيانات مقيدة أو سرية أو سرية للغاية. • تحقق من جميع وسائط التخزين تتبع خطة التنفيذ المناسبة وفقًا لمتطلبات حذف البيانات أو التخلص من الوسائط. علاوة على ذلك ، تحقق من تقديم جميع الموافقات المناسبة والتوقيعات قبل التسليم والتأكد من الإتلاف الآمن للبيانات.

		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • خطة تنفيذ حذف البيانات ، بما في ذلك إجراءات برامج أو خدمة الطرف الخارجي لحذف البيانات ، إذا لزم الأمر. • الحفاظ على مسار المستندات لخطوات إتلاف البيانات المناسبة.
	5-1-6-2	الإحتفاظ بسجل لعمليات الإتلاف أو الحذف الآمن للبيانات التي تم تنفيذها.
		إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • مراجعة خطة عمل إتلاف البيانات المعمول بها والتأكد من أنها ستشمل مراقبة وتسجيل البيانات والأجهزة في الجهة . يجب أن تحافظ أيضًا على حالة جميع أصول تخزين البيانات في النطاق وتسجيل أي تغييرات على الحالة وفقًا للقواعد المحددة من قبل الجهة. • مراجعة وتنفيذ أي برنامج أو خدمة خاصة بطرف خارجي لاستخدامها في مراقبة وتسجيل عمليات أصول تخزين البيانات.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • الاحتفاظ بقائمة لجميع أصول تخزين البيانات في الجهة مع وضعها والمعلومات الأخرى ذات الصلة. • خطة تنفيذ مراقبة الإتلاف الآمن للبيانات ، بما في ذلك إجراءات خدمة الطرف الخارجي لعمليات أصول تخزين البيانات ، إذا لزم الأمر. • عينة من إتلاف وحذف السجلات / التقارير.
	2-6-2	يجب مراجعة تطبيق متطلبات الإتلاف الآمن للبيانات في الجهة حسب المدة المحددة لكل مستوى.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعلق بالأمن المادي **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • مراجعة عملية وآلية الإتلاف الآمن للبيانات فيما يتعلق بخطة التنفيذ وسياسة الإتلاف الآمن للبيانات.

	• يجب إجراء مراجعة دورية لعملية الإتلاف الآمن لـ لبيانات لأجهزة التخزين سنوياً على الأقل أو أقل لمستوى تصنيف البيانات العامة أو المقيدة وكل ستة أشهر على الأقل أو أقل لمستوى تصنيف البيانات السرية أو السرية للغاية ، لضمان تطبيق المتطلبات بفعالية .
	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • تقرير مراجعة عملية الإتلاف الآمن للبيانات.
7-2	**الأمن السيبراني للطابعات والماسحات الضوئية وآلات التصوير (Cypersecurity for Printers, Scanners and Copy Machines)**
الهدف	ضمان التعامل الآمن مع البيانات عند إستخدام الطابعات والماسحات الضوئية وآلات التصوير.
الضوابط	
1-7-2	يجب تحديد وتوثيق وإعتماد متطلبات الأمن السيبراني لحماية الطابعات والماسحات الضوئية وآلات التصوير في الجهة.
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • مراجعة متطلبات الأمن السيبراني للطابعات والماسحات الضوئية وآلات التصوير التي تتعامل مع البيانات المقيدة والسرية والسرية للغاية الخاصة بالجهة. • تحديد وتوثيق واعتماد سياسة إعدادت الحماية والتحصين للجهة لضمان الاستخدام المناسب لطابعات الجهة والماسحات الضوئية وآلات التصوير من قبل الموظفين.
	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).
2-7-2	يجب تطبيق متطلبات الأمن السيبراني للطابعات والماسحات الضوئية وآلات التصوير في الجهة.
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • مراجعة متطلبات الأمن السيبراني للطابعات والماسحات الضوئية وآلات التصوير التي تتعامل مع البيانات المقيدة والسرية والسرية للغاية الخاصة بالجهة.

	• تطبيق سياسة إعدادت الحماية والتحصين للجهة لضمان الاستخدام المناسب لطابعات الجهة والماسحات الضوئية وآلات التصوير من قبل الموظفين المصرح لهم. يجب أن يشمل ذلك ، على سبيل المثال لا الحصر: وضع الأجهزة وإعداداتها وإدارة الوصول إلى الأجهزة والاصلاحات والتحديثات والتسجيل والمراقبة وتعطيل الإعدادت الافتراضية.	
	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • تطبيق متطلبات الأمن السيبراني للطابعات والماسحات الضوئية وآلات التصوير في الجهة.	
3-7-2	يجب أن تغطي الأمن السيبراني للطابعات والماسحات الضوئية وآلات التصوير بحد أدنى، ما يلي:	
1-3-7-2	تعطيل خاصية التخزين المؤقت.	
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • مراجعة وتطبيق إعدادات الطابعات والماسحات الضوئية وأجهزة التصوير للتخزين المؤقت والتأكد من تعطيل هذه الخاصية للأجهزة التي تتعامل مع البيانات السرية والسرية للغاية للجهة.	
	المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • تطبيق خاصية تعطيل التخزين المؤقت في الطابعات والماسحات الضوئية وآلات التصوير الخاصة بالجهة.	
2-3-7-2	تفعيل خاصية التحقق من الهوية في الطابعات والماسحات الضوئية وآلات التصوير المركزية قبل بدء عمليات الطباعة والتصوير والمسح الضوئي.	
	إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • مراجعة وتطبيق إعدادات المصادقة على الطابعات والماسحات الضوئية وأجهزة التصوير والتأكد من تمكينها لجميع الموظفين المصرح لهم بالوصول إلى البيانات السرية والسرية للغاية الخاصة بالجهة.	

		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • تطبيق تمكين المصادقة للطابعات والماسحات الضوئية وآلات التصوير المركزية.
	3-3-7-2	الإحتفاظ بطريقة آمنة بسجل إلكتروني للعمليات الخاصة بإستخدام الطابعات والماسحات الضوئية وآلات التصوير لفترة لاتقل عن 12 شهراً.
		إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • مراجعة وتطبيق إعدادات تسجيل الطابعات والماسحات الضوئية وأجهزة التصوير والتأكد من الاحتفاظ بسجلات للأجهزة التي تتعامل مع البيانات السرية والسرية للغاية للجهة لمدة لا تقل عن 12 شهراً. • أن يحتوي السجل الإلكتروني على ما تم طباعته أو مسحة أو تصويره :كما يمكن استخدام (Hash)لإنشاء توقيع رقمي للمستند أو الملف. أيضاً، يمكن استخدام (Hash) للتحقق من سلامة المستند أو الملف وتحديد ما إذا تم تغييره أو تعديله.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • تطبيق نظام الاحتفاظ بالسجلات للطابعات والماسحات الضوئية وآلات التصوير.
	4-3-7-2	تفعيل وحماية سجلات المراقبة لأنظمة CCTV على مواقع أجهزة الطباعة المركزية والماسحات الضوئية وآلات التصوير.
		إرشادات تطبيق الضوابط: • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • مراجعة وتطبيق إعداد وتركيب أنظمة (CCTV) في الجهة لضمان مراقبة الأصول المتعلقة بالبيانات السرية والسرية للغاية مثل: الطابعات المركزية والماسحات الضوئية وآلات النسخ. • التحقق من تسجيلات أنظمة (CCTV) للإعدادات المذكوره أعلاه وتخزينها وفقًا لسياسة الإتلاف الآمن للبيانات. • مراجعة صلاحيات الوصول إلى سجلات أنظمة (CCTV) والتحقق من أن صلاحيات الوصول مقتصره على الاشخاص المصرح لهم. • يجب إجراء مراجعة دورية للوصول إلى سجلات أنظمة (CCTV) للتأكد من أن الأشخاص المصرح لهم فقط هم من يمكنهم الوصول إليها.

		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • تطبيق تسجيل أنظمة (CCTV) لمراقبة الطابعات والماسحات الضوئية وآلات التصوير المركزية. • مراجعة الوصول إلى سجلات أنظمة (CCTV) للأشخاص المصرح لهم فقط.
	5-3-7-2	إستخدام أجهزة تمزيق الوثائق الورقية (Cross Shredding) لإتلاف الوثائق في حال الإنتهاء من إستخدامها نهائياً. **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني للإتلاف الآمن للبيانات بجميع الأشكال ، سواء الإلكترونية أو الورقية، واعتمادها من قبل صاحب الصلاحية. • التأكد من تمزيق الوثائق الورقية السرية والسرية للغاية بعد انقضاء الحاجة منها. • مراجعة سياسة حفظ البيانات لإتلاف الوثائق الورقية في حالة انتهاء فترة الاحتفاظ بالبيانات. **المخرجات المتوقعة:** • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • توفير أجهزة تمزيق في مباني الجهة للتخلص السليم من الوثائق الورقية.
4-7-2		يجب مراجعة تطبيق متطلبات الأمن السيبراني للطابعات والماسحات الضوئية وآلات التصوير في الجهة حسب المدة المحددة لكل مستوى. **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • يجب إجراء مراجعة دورية لمتطلبات الأمن السيبراني للطابعات والماسحات الضوئية وآلات التصوير سنوياً على الأقل للأجهزة التي تتعامل مع البيانات العامة والسرية ، وكل ثلاثة أشهر على الأقل للأجهزة التي تتعامل مع البيانات السرية والسرية للغاية. **المخرجات المتوقعة:** • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • تطبيق المراجعات الدورية للطابعات والماسحات الضوئية وآلات التصوير.

3 الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية (Third-Party and Cloud Computing Cybersecurity)

1-3	الأمن السيبراني المتعلق بالأطراف الخارجية (Third Party Cybersecurity)	
الهدف	ضمان حماية أصول الجهة من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية بما في ذلك خدمات الإسناد لتقنية المعلومات "Outsourcing" والخدمات المدارة "Managed Services" والخدمات الاستشارية "Consultancy Services" وفقًا للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.	
الضوابط		
1-1-3	بالإضافة للضوابط ضمن المكون الفرعي 1-4 في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني، المتعلقة بالأطراف الخارجية، بحد أدنى؛ ما يلي:	
	1-1-1-3	إجراء مسح أمني (Screening or Vetting) لموظفي الأطراف الخارجية الذين لديهم صلاحيات الإطلاع على البيانات.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • مراجعة وتقييم مهارات وكفاءات المرشحين باستخدام منهجيات مختلفة بما في ذلك المقابلات والاختبارات الشفوية أو التحريرية. أيضًا ، تطوير عملية المسح الأمني على المرشحين الذين تم اختيارهم إما عن طريق فريق داخلي أو طرف ثالث. • تطوير وتوثيق واعتماد خطة عمل لمنح وصول المرشحين الجدد وفقًا للأدوار والصلاحيات المطلوبة. • تطوير عملية مراجعة دورية لإزالة الأدوار والصلاحيات غير المستخدمة وغير المبررة بعد انقضاء حاجتها أو مدتها.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • عملية التوظيف والترتيبات التي تشمل المسح الأمني حسب مهارات موظفي الطرف الخارجي. • اختيار الفريق المختص من التحقق من المرشحين اما فريق داخلي او طرف خارجي. • قائمة المستخدمين المعتمدة المراجعة بشكل دوري مع صلاحياتهم. • مراجعة سياسة الأمن السيبراني للموارد البشرية بما يتماشى مع سياسات الأمن السيبراني للبيانات.

	2-1-1-3	وجود ضمانات تعاقدية للقدرة على حذف بيانات الجهة بطرق آمنة لدى الطرف الخارجي عند الإنتهاء/إنهاء العلاقة التعاقدية مع تقديم الأدلة على ذلك.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعّلق بالأطراف الخارجية **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • مراجعة اتفاقية مستوى الخدمة بين الجهة والأطراف الخارجية فيما يتعلق بمعالجة البيانات المقيدة والسرية والسرية للغاية للجهة. • التحقق من أن بند نهاية الخدمة في الاتفاقية يحدد ويوثق الإجراءات المناسبة للتخلص من بيانات الجهة وفقًا لسياسة الإتلاف الآمن للبيانات. أيضاً ، التحقق من أن الأطراف الخارجية تقدم أدلة للجهة على حذف بيانات الجهة بطرق آمنة.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • الإجراءات الموثقة للأطراف الخارجية في سياسة الإتلاف الآمن للبيانات الخاصة بالجهة فيما يتعلق بالبيانات المقيدة والسرية والسرية للغاية. • مراجعة اتفاقية مستوى الخدمة للإتلاف الآمن للبيانات في نهاية الخدمة.
	3-1-1-3	توثيق كافة عمليات مشاركة البيانات مع الأطراف الخارجية، على أن يشمل ذلك مبررات مشاركة البيانات.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعّلق بالأطراف الخارجية **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • مراجعة اتفاقية مستوى الخدمة بين الجهة والأطراف الخارجية فيما يتعلق بعمليات مشاركة البيانات المقيدة والسرية والسرية للغاية الخاصة. • تحديد وتطبيق البند المتعلق بمشاركة البيانات في الاتفاقية ، والتي يجب أن تشمل ، على سبيل المثال لا الحصر: وصف البيانات المشتركة ، وقيود استخدام البيانات ، وضمانات حماية البيانات المطلوبة ، والتبرير المتعلق بمشاركة البيانات. • التحقق من توثيق حركة نقل بيانات الجهة مع الأطراف الخارجية فقط بعد تقديم مبررات مشاركة البيانات.

		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • إجراء موثق لعمليات مشاركة البيانات مع الأطراف الخارجية. • مراجعة اتفاقية مستوى الخدمة للعملية المناسبة لعمليات مشاركة البيانات مع الأطراف الخارجية.
	4-1-1-3	عند مشاركة البيانات خارج المملكة يجب التحقق من قدرة الجهة المستضيفة على حماية تلك البيانات والحصول على موافقة صاحب الصلاحية بالإضافة إلى الإلتزام بالمتطلبات التشريعية والتنظيمية ذات العلاقة.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعّلق بالأطراف الخارجية **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • مراجعة اتفاقية مستوى الخدمة بين الجهة والأطراف الخارجية فيما يتعلق بنقل البيانات المقيدة والسرية والسرية للغاية خارج المملكة. • التحقق من معايير وقوانين حماية البيانات التي تتبعها الجهة المستضيفة خارج المملكة وتحديدها لحماية بيانات الجهة. أيضاً ، الحصول على موافقة خطية من المسؤول المفوض لنقل البيانات خارج المملكة ، وفقًا للأنظمة واللوائح ذات الصلة. • التحقق من المتطلبات التنظيمية الأخرى المطلوبة مثل متطلبات موافقة صاحب البيانات ، وتقييم الأثر لنقل البيانات خارج المملكة.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • إجراءات موثقة لنقل بيانات الجهة خارج المملكة. • مراجعة اتفاقية مستوى الخدمة للعملية المناسبة لنقل البيانات مع الأطراف الخارجية خارج المملكة.
	5-1-1-3	إلزام الأطراف الخارجية بإبلاغ الجهة مباشرةً عند حدوث حادثة أمن سيبراني قد تؤثر على بيانات الجهة التي تم مشاركتها أو إنشائها.

		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعّلق بالأطراف الخارجية **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • مراجعة اتفاقية مستوى الخدمة بين الجهة والأطراف الخارجية فيما يتعلق بالحوادث السيبرانية الذي قد يؤثر على البيانات السرية والسرية للغاية. • التحقق من الاتفاقيات وتحديدها لإبلاغ الجهة في حالة وقوع حادث للأمن السيبراني التي قد تتعرض لها بيانات الجهة. أيضاً، تحديد جداول زمنية محددة لاتفاقية مستوى الخدمة (SLA) بحيث يتعين على الأطراف الخارجية اتباعها للإبلاغ المباشر للجهة.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • إجراءات موثقة للإبلاغ بحوادث الأمن السيبراني المتعلقة ببيانات الجهة. • مراجعة اتفاقية مستوى الخدمة للعملية المناسبة للإبلاغ بحوادث الأمن السيبراني مع الأطراف الخارجية.
	6-1-1-3	إعادة تصنيف البيانات إلى أقل مستوى يحقق الهدف, قبل مشاركتها مع الأطراف الخارجية وذلك بإستخدام تقنيات تعتيم البيانات (Data Masking) أو تقنيات مزج البيانات (Data Scrambling).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعّلق بالأطراف الخارجية **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • التحقق من عملية إعادة تصنيف البيانات إلى أقل مستوى للتأكد من إرسال البيانات المطلوبة فقط الى الطرف الخارجي ويجب عدم إرسال أي بيانات غير مشار لها. يمكن تحقيق ذلك من خلال تقنيات إخفاء البيانات ، على سبيل المثال لا الحصر: إخفاء البيانات وتعتيم البيانات ومزج البيانات وتصفية البيانات.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية).

		• إجراء موثق لإخفاء البيانات المرسلة من الجهة.
2-1-3	بما يتوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة، وبالإضافة إلى ماينطبق من الضوابط الأساسية للأمن السيبراني ضمن المكونات الرئيسية (1) و (2) و (3) من هذه الوثيقة، يجب أن تغطي متطلبات الأمن السيبراني عند التعامل مع الجهات الاستشارية للمشاريع الإستراتيجية ذات الحساسية العالية على المستوى الوطني بحد أدنى، مايلي:	
	1-2-1-3	إجراء مسح أمني (Screening or Vetting) لموظفي شركات الخدمات الاستشارية الذين لديهم صلاحيات الإطلاع على البيانات.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعّلق بالأطراف الخارجية **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • على الجهة إلزام شركات الخدمات الاستشارية العاملة ضمن المشاريع الاستراتيجية بتقديم بيانات المسح الأمني لكافة الموظفين العاملين ضمن تلك المشاريع، وعلى شركات الخدمات الاستشارية التعاون في هذه المجال مع الجهة في استكمال هذا الإجراء. • مراجعة وتقييم ومهارات وكفاءات المرشحين باستخدام منهجيات مختلفة بما في ذلك المقابلات والاختبارات الشفوية أو التحريرية. أيضًا ، الأخذ بعين الاعتبار نتائج عملية المسح الأمني على المرشحين الذين تم اختيارهم إما عن طريق فريق داخلي أو طرف ثالث. • مراجعة المهارات باستخدام منهجيات مختلفة بما في ذلك طلبات تقديم العروض والسيرة الذاتية للمرشح. أيضًا ، تطوير عملية التحقق من الموظفين الذين تم اختيارهم من مصادر خارجية إما عن طريق فريق داخلي أو طرف خارجي. • تطوير وتوثيق واعتماد خطة عمل لمنح وصول للمرشحين الجدد وفقًا للأدوار والصلاحيات المطلوبة. • تطوير عملية مراجعة دورية لإزالة الأدوار والصلاحيات غير المستخدمة وغير المبررة بعد انقضاء حاجتها أو مدتها.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • وثيقة توضح تقديم شركة الخدمات الاستشارية بيانات الموظفين المطلوبة لإجراء المسح الأمني للعاملين على المشاريع الاستراتيجية في الجهة. • وثيقة توضح إتمام عملية المسح الأمني لموظفي شركات الخدمات الاستشارية من قبل الجهة.

		• عملية التوظيف والإعداد والتي تشمل الفحص والتدقيق حسب مهارات موظفي شركات الخدمات الاستشارية. • اختيار الفريق المختص بالتحقق من المرشحين. • قائمة المستخدمين المعتمدة مع صلاحياتهم. • مراجعة سياسة الأمن السيبراني للموارد البشرية بما يتماشى مع سياسات الأمن السيبراني للبيانات.
	2-2-1-3	وجود ضمانات تعاقدية تشمل إلزام موظفي شركات الخدمات الاستشارية بعدم إفشاء المعلومات وكذلك القدرة على حذف بيانات الجهة بطرق آمنة لدى شركات الخدمات الاستشارية عند الإنتهاء/إنهاء العلاقة التعاقدية مع تقديم الأدلة على ذلك.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعّلق بالأطراف الخارجية **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • على الجهة العمل على توقيع شركات الخدمات الاستشارية وموظفيها العاملين ضمن المشاريع الاستراتيجية ضمانات بعدم إفشاء المعلومات وكذلك القدرة على حذف بيانات الجهة بطرق آمنة عند الإنتهاء/ إنهاء العلاقة التعاقدية وعدم التصريح بأي بيانات قبل الحصول على موافقة خطية من الجهة، وعلى شركات الخدمات الاستشارية التعاون في هذه المجال مع الجهة في تطبيق هذا الإجراء. • مراجعة اتفاقية مستوى الخدمة بين الجهة وشركات الخدمات الاستشارية فيما يتعلق بمعالجة البيانات المقيدة والسرية والسرية للغاية للجهة. • التحقق من أن بند نهاية الخدمة في الاتفاقية يحدد ويوثق الإجراءات المناسبة للتخلص من بيانات الجهة وفقًا لسياسة الإتلاف الآمن للبيانات. أيضاً، التحقق من أن شركات الخدمات الاستشارية يجب أن تقدم دليلًا على الإتلاف الآمن للبيانات إلى الجهة.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • وثيقة توضح تضمين بنود المحافظة على سرية المعلومات وعدم إفشاء البيانات والحذف الآمن للبيانات لضمان عدم إفشاء المعلومات الخاصة بالجهة من قبل شركات الخدمات الاستشارية وموظفيها (نسخة ورقية أو إلكترونية). • الإجراءات الموثقة لشركات الخدمات الاستشارية في سياسة الإتلاف الآمن للبيانات الخاصة بالجهة للبيانات السرية والسرية للغاية. • مراجعة اتفاقية مستوى الخدمة للإتلاف الآمن للبيانات في نهاية الخدمة.
	3-2-1-3	توثيق كافة عمليات مشاركة البيانات مع شركات الخدمات الاستشارية، على أن يشمل ذلك مبررات مشاركة البيانات.

		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعّلق بالأطراف الخارجية **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • على الجهة العمل على توثيق عملية مشاركة البيانات مع شركات الخدمات الاستشارية العاملة ضمن المشاريع الاستراتيجية إستناداً على مبدأ الحاجة إلى المعرفة (Need-to- know) . • على شركات الخدمات الاستشارية العاملة ضمن المشاريع الاستراتيجية التأكد من توثيق مشاركة البيانات مع الموظفين المصرح لهم إستناداً على مبدأ الحاجة إلى المعرفة (Need-to- know) . • مراجعة اتفاقية مستوى الخدمة بين الجهة وشركات الخدمات الاستشارية فيما يتعلق بعمليات مشاركة البيانات المقيدة والسرية والسرية للغاية الخاصة. • تحديد وتطبيق البند المتعلق بمشاركة البيانات في الاتفاقية ، والتي يجب أن تشمل ، على سبيل المثال لا الحصر: وصف البيانات المشتركة ، وقيود استخدام البيانات ، وضمانات حماية البيانات المطلوبة ، والتبرير المتعلق بمشاركة البيانات. • التحقق من حركة بيانات الجهة إلى شركات الخدمات الاستشارية وتوثيقها فقط بعد تقديم التبرير المناسب لمشاركة البيانات.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • إجراء موثق لعمليات مشاركة البيانات مع شركات الخدمات الاستشارية. • مراجعة اتفاقية مستوى الخدمة للعملية المناسبة لعمليات مشاركة البيانات مع شركات الخدمات الاستشارية.
	4-2-1-3	إلزام شركات الخدمات الاستشارية بإبلاغ الجهة مباشرةً عند حدوث حادثة أمن سيبراني قد تؤثر على البيانات التي تمت مشاركتها أو إنشائها.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعّلق بالأطراف الخارجية **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • على الجهة إلزام شركات الخدمات الاستشارية العاملة ضمن المشاريع الاستراتيجية بإبلاغ الجهة عند حدوث حادثة أمن سيبراني على البيانات التي تمت مشاركتها، وعلى شركات الخدمات الاستشارية التعاون في هذه المجال مع الجهة في تطبيق هذا الإجراء. • مراجعة اتفاقية مستوى الخدمة بين الجهة وشركات الخدمات الاستشارية فيما يتعلق بالإبلاغ عن الحوادث التي قد تؤثر على البيانات المقيدة والسرية والسرية للغاية.

		• التحقق وتحديد عملية إبلاغ الجهة في حالة وقوع حادث أمن سيبراني قد يؤدي إلى تعرض بيانات الجهة للخطر. علاوة على ذلك، أيضًا تحديد جداول زمنية محددة لاتفاقية مستوى الخدمة (SLA) يجب على شركات الخدمات الاستشارية اتباعها للإبلاغ الفوري للجهة.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • إجراءات موثقة للإبلاغ بحوادث الأمن السيبراني المتعلقة ببيانات الجهة. • مراجعة اتفاقية مستوى الخدمة للعملية المناسبة للإبلاغ بحوادث الأمن السيبراني مع شركات الخدمات الاستشارية.
	5-2-1-3	إعادة تصنيف البيانات إلى أقل مستوى يحقق الهدف قبل مشاركتها مع شركات الخدمات الاستشارية وذلك باستخدام تقنيات تعتيم البيانات (Data Masking) أو تقنيات مزج البيانات (Data Scrambling).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • على الجهة إلزام شركات الخدمات الاستشارية العاملة ضمن المشاريع الاستراتيجية باستخدام البيانات ضمن النطاق المحدد من قبل الجهة، وعلى شركات الخدمات الاستشارية التعاون في هذه المجال مع الجهة في تطبيق هذا الإجراء. • على الجهة إلزام شركات الخدمات الاستشارية العاملة ضمن المشاريع الاستراتيجية باستخدام البيانات ضمن النطاق المحدد من قبل الجهة، وعلى شركات الخدمات الاستشارية التعاون في هذه المجال مع الجهة في تطبيق هذا الإجراء. • التحقق وتحديد عملية إعادة تصنيف البيانات إلى أدنى مستوى للتأكد من إرسال البيانات المطلوبة فقط الى شركات الخدمات الاستشارية ويجب عدم إرسال أي بيانات غير مشار لها. يمكن تحقيق ذلك من خلال تقنيات إخفاء البيانات المختلفة ، على سبيل المثال لا الحصر ، إخفاء البيانات وإخفاء هوية البيانات وخلط البيانات وتصفية البيانات.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • إجراء موثق لإعادة تصنيف البيانات لأقل مستوى يحقق الهدف قبل مشاركتها مثل استخدام تقنيات تعتيم البيانات وإخفاء البيانات ومزج البيانات.
	6-2-1-3	تخصيص قاعة مغلقة لموظفي شركات الخدمات الاستشارية لأداء أعمالهم, مع توفير أجهزة مخصصة مملوكة للجهة يتم من خلالها مشاركة البيانات ومعالجتها.

		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعّلق بالأطراف الخارجية **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • على الجهة إلزام شركات الخدمات الاستشارية العاملة ضمن المشاريع الاستراتيجية التي تتضمن بيانات سرية وسرية للغاية بعدم استخدام القاعات الغير مغلقة والغير مخصصة لموظفي الجهات الاستشارية بالإضافة إلى عدم استخدام الأجهزة الغير المخصصة والغير مملوكة للجهة، وعلى شركات الخدمات الاستشارية التعاون في هذه المجال مع الجهة في تطبيق هذا الإجراء. • مراجعة اتفاقية مستوى الخدمة بين الجهة وشركات الخدمات الاستشارية فيما يتعلق بالقاعة المغلقة المخصصة والأجهزة التي تستخدم بيانات الجهة السرية والسرية للغاية. • التحقق من تحديد القاعة المغلقة المخصصة حيث يمكن لموظفي شركات الخدمات الاستشارية تقديم الخدمة بشكل افضل. أيضاً ، توفير أجهزة الجهة لهم لمشاركة البيانات ومعالجتها.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • إجراء موثق للتعامل مع مساحة العمل في القاعة المغلقة وأجهزة معالجة البيانات لموظفي شركات الخدمات الاستشارية. • تقديم ما يثبت إلتزام شركات الخدمات الاستشارية بعدم استخدام القاعات الغير مخصصة لموظفي الجهات الاستشارية. • مراجعة اتفاقية مستوى الخدمة لاستخدام مساحة العمل والأجهزة المخصصة لموظفي شركات الخدمات الاستشارية.
	7-2-1-3	تفعيل أنظمة التحكم بالدخول والخروج من القاعة المغلقة، على أن يكون للمصرح لهم فقط.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعّلق بالأطراف الخارجية **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • على الجهة إلزام شركات الخدمات الاستشارية العاملة ضمن المشاريع الاستراتيجية التي تتضمن بيانات سرية وسرية للغاية باستخدام أنظمة الدخول والخروج من القاعات المغلقة والمخصصة لموظفي الشركات الاستشارية المصرح لهم وفق الصلاحيات. وعلى شركات الخدمات الاستشارية التعاون في هذه المجال مع الجهة في تطبيق هذا الإجراء. • مراجعة اتفاقية مستوى الخدمة بين الجهة وشركات الخدمات الاستشارية فيما يتعلق بالتحكم في الوصول إلى القاعة المغلقة للتعامل مع بيانات الجهة السرية والسرية للغاية.

		• التحقق وتحديد القاعة المغلقة المخصصة كمساحة يمكن التحكم في الوصول إليها حيث يمكن فقط لموظفي شركات الخدمات الاستشارية المعتمدين الوصول إلى بيانات الجهة وأجهزة تخزين البيانات.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • إجراء موثق لتفعيل نظام التحكم في الدخول إلى قاعة العمل المغلقة لموظفي شركات الخدمات الاستشارية. • مراجعة اتفاقية مستوى الخدمة لاستخدام مساحة عمل مخصصة للتحكم في الوصول لموظفي شركات الخدمات الاستشارية.
	8-2-1-3	منع خروج الأجهزة ووحدات التخزين والوثائق من القاعة المغلقة، ومن إدخال أي أجهزة إلكترونية للقاعة.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعّلق بالأطراف الخارجية **إرشادات تطبيق الضوابط:** • العمل على تحديد متطلبات هذا الضابط وتوثيقها في وثيقة متطلبات الأمن السيبراني، واعتمادها من قبل صاحب الصلاحية. • على الجهة إلزام شركات الخدمات الاستشارية وموظفيها العاملين ضمن المشاريع الاستراتيجية التي تتضمن بيانات سرية وسرية للغاية بمنع إدخال الأجهزة الغير مملوكة للجهة /إخراج الأجهزة ووحدات التخزين والوثائق من القاعات المغلقة والمخصصة لموظفي الشركات الاستشارية. • مراجعة اتفاقية مستوى الخدمة بين الجهة وشركات الخدمات الاستشارية فيما يتعلق بوسائط التخزين والجهاز المستخدم للتعامل مع بيانات الجهة السرية والسرية للغاية على أن تشمل منع إدخال الأجهزة الغير مملوكة للجهة /إخراج الأجهزة ووحدات التخزين والوثائق من القاعات المغلقة والمخصصة لموظفي الشركات الاستشارية . • التحقق وتحديد الإجراءات التي تمنع حمل أجهزة التخزين والوسائط التي تتعامل مع بيانات الجهة خارج الغرفة المغلقة. علاوة على ذلك ، تحقق من عدم السماح لأي وسائط تخزين أخرى بدخول القاعة المغلقة. يتم تطبيق ذلك باستخدام الفحوصات الأمنية عند الدخول والخروج من الغرفة المغلقة.
		المخرجات المتوقعة: • وثيقة توضح تحديد وتوثيق متطلبات هذا الضابط (مثل سياسة أو/و إجراء معتمد من قبل صاحب الصلاحية). • إجراء موثق للقيود المفروضة على أجهزة التخزين أثناء دخول وخروج من قاعة العمل المغلقة لموظفي شركات الخدمات الاستشارية. • مراجعة اتفاقية مستوى الخدمة للاستخدام المقبول لوسائط التخزين الخاصة بالجهة من قبل موظفي شركات الخدمات الاستشارية.



الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority