وزارة الاتصالات وتقنية المعلومات
MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY

سياسات الأمن الرقمي لقطاع الاتصالات وتقنية المعلومات

مايو 2019

قائمة المحتويات

قائمة الأشكال

قائمة الجداول

المقدمة

اعتمد مجلس الوزراء رؤية 2030 عام 2016 لتكون المملكة العربية السعودية "مركزًا حيويًا للعالمين العربي والإسلامي وقوة استثمارية رائدة ومحور ربط القارات الثلاث"، وهذه الرؤية الطموحة والجديرة بالثناء تدعمها ثلاثة محاور تتمثل في "مجتمع حيوي واقتصاد مزدهر ووطن طموح"، ولتحقيق رؤية 2030، وضعت سبعة برامج شاملة تعمل على الاستثمار في عوامل التمكين مثل التحول الرقمي على مستوى المملكة والاقتصاد والمجتمع لتعزيز منظومة القيم الوطنية.

إن هذا التحول الرقمي على مستوى كل الأنظمة بأكملها يزيد من المخاطر ذات الصلة. وبناءً على برنامج التحول الوطني وبهدف الحد من آثار هذه المخاطر، فقد استهدفت إحدى المبادرات الاستراتيجية للمملكة تعزيز الأمن الرقمي في قطاع الاتصالات وتقنية المعلومات داخل المملكة، ووفقًا لبرنامج التحول الوطني، فإن أهداف هذه المبادرة تشمل وضع الاستراتيجيات والسياسات وبناء الشراكات الخاصة بالأمن الرقمي في قطاع الاتصالات وتقنية المعلومات.

تعد وزارة الاتصالات وتقنية المعلومات الجهة المشرفة على قطاع الاتصالات وتقنية المعلومات في المملكة وهي المعنية بإعداد سياسات ومتطلبات للأمن الرقمي وتهيئة الظروف المناسبة لتطويرها وحوكمتها في القطاع، وعليه أعدت وزارة الاتصالات وتقنية المعلومات الحد الأدنى من السياسات الأساسية للأمن الرقمي التي ستساعد بشكل استباقي إذا ما تم تنفيذها بفعالية في تخفيف أثر التهديدات الأمنية الرقمية في قطاع الاتصالات وتقنية المعلومات.

الهدف

تهدف هذه الوثيقة إلى وضع الحد الأدنى من السياسات الأساسية للأمن الرقمي التي تساعد في تخفيف أثر التهديدات الأمنية الرقمية في قطاع الاتصالات وتقنية المعلومات إذا ما تم تطبيقها بفعالية..

النطاق

توضح هذه الوثيقة تفاصيل السياسات الأساسية التي تحتاجها الشركات العاملة في قطاع الاتصالات وتقنية المعلومات لتطوير وتنفيذ وتحسين الأمن الرقمي في هذه الشركات إضافة إلى السياسات الخاصة بخدمات الاتصالات وتقنية المعلومات التي تقدمها.

التطبيق

تطبق **السياسات الأساسية للأمن الرقمي لقطاع الاتصالات وتقنية المعلومات** على جميع الشركات العاملة في قطاع الاتصالات وتقنية المعلومات.
تطبق **سياسات الأمن الرقمي الخاصة بخدمات قطاع الاتصالات وتقنية المعلومات** على جميع الشركات العاملة في قطاع الاتصالات وتقنية المعلومات التي تقدم خدمات ذات علاقة.

المصطلحات

المصطلح	المعنى/ الاستخدام
يجب	يستخدم هذا المصطلح لتحديد المتطلبات الإلزامية لهذه السياسات.

المراجع

السياسات	المراجع
الأساسية	— الضوابط الأساسية للأمن السيبراني الوطني (NCA Essential Cybersecurity Controls) — ISO 27001:2013
الخاصة	— ITU-T SG 17 — GSMA — 3GPP — ISO 27001:27011 — Cloud Security Alliance (OWASP - IOT Security guidelines)

الجدول 1: مراجع السياسات

الأطراف المعنية (مصفوفة توزيع المسؤوليات)

تشمل عملية إعداد الوثيقة على تصميم سياسات الأمن الرقمي للاتصالات وتقنية المعلومات وإدارتها ونشرها، وإدارة هذه الوثيقة لها نشاطان رئيسيان، أحدهما المراجعة والتحديث، والآخر التنفيذ. تشير أنشطة التحديث والمراجعة إلى التحسينات والمراجعات المستمرة لسياسات الأمن الرقمي للاتصالات وتقنية المعلومات، ويعنى نشاط التنفيذ بتطبيق سياسات الأمن الرقمي للاتصالات وتقنية المعلومات.

الأطراف المعنية:

- الهيئة الوطنية للأمن السيبراني (NCA)
- وزارة الاتصالات وتقنية المعلومات (MCIT)
- هيئة الاتصالات وتقنية المعلومات (CITC)
- شركات خدمات الاتصالات وتقنية المعلومات

يلخص الجدول 2 جميع أدوار الأطراف المعنية في إدارة الوثيقة.

	أنشطة مرتبطة بسياسات الأمن الرقمي لقطاع الاتصالات وتقنية المعلومات	
الأطراف المعنية	المراجعة والتحديث	التنفيذ
الهيئة الوطنية للأمن السيبراني	C + I	I
وزارة الاتصالات وتقنية المعلومات	R + A	A
هيئة الاتصالات وتقنية المعلومات	C + I	A
شركات خدمات الاتصالات وتقنية المعلومات	I	R

المفتاح: R= مسؤولية تنفيذية، A= مسؤولية إشرافية، C = للاستشارة، I= للإبلاغ

الجدول 2: مصفوفة توزيع المسؤوليات

إعداد سياسات الأمن الرقمي لقطاع الاتصالات وتقنية المعلومات

استخدمت الضوابط الأساسية للأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني والمعايير الرائدة وأفضل ممارسات الأمن الرقمي لقطاع الاتصالات وتقنية المعلومات المطبقة دوليًا في إعداد سياسات الأمن الرقمي للقطاع، وتشكل هذه السياسات إحدى مراجع إعداد تنظيمات وقواعد الأمن الرقمي التي تصدر من هيئة الاتصالات وتقنية المعلومات.

يوضح الشكل رقم 1 رسم تصوري لسياسات الأمن الرقمي لقطاع الاتصالات وتقنية المعلومات

الشكل 1: رسم تصوري لسياسات الأمن الرقمي لقطاع الاتصالات وتقنية المعلومات

تمّ إعداد سياسات الأمن الرقمي لقطاع الاتصالات وتقنية المعلومات من منظورين:

1. **السياسات الأساسية للأمن الرقمي لقطاع الاتصالات وتقنية المعلومات** من خلال دمج الضوابط الأساسية للأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني ومعايير ISO 27001:2013 والتي تنطبق على كافة الشركات العاملة في قطاع الاتصالات وتقنية المعلومات. يرجى الرجوع إلى الملحق (أ) الذي يحدد السياسة الأساسية لقطاع الاتصالات وتقنية المعلومات والضوابط الأساسية للأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني ومعايير ISO 27001:2013.

2. **سياسات الأمن الرقمي الخاصة بخدمات قطاع الاتصالات وتقنية المعلومات** من خلال اعتماد أفضل الممارسات من معايير: ITU-T SG 17 والمنظمة الدولية لقطاع الاتصالات المتنقلة ومشروع شراكة الجيل الثالث وISO 27011 وتحالف أمن الحوسبة السحابية ومشروع أمن تطبيق الويب المفتوح -الإرشادات الأمنية لإنترنت الأشياء والتي تنطبق على الشركات التي تقدم خدمات الاتصالات وتقنية المعلومات. يرجى الرجوع إلى الملحق (ب) للاطلاع على السياسات الخاصة بقطاع الاتصالات وتقنية المعلومات والمعايير التي كانت مستخدمة للإشارة إلى السياسات المنصوص عليها.

تشمل سياسات الأمن الرقمي لقطاع الاتصالات وتقنية المعلومات مبادئ ونطاقات ونصوص:

- مبدأ السياسة: يلخص هدف الأمن الرقمي المطلوب ضمن كل سياسة.
- نطاق السياسة: يحتوي على أحكام نصوص الأمن الرقمي الإلزامية والتي يجب أن تلتزم بها الشركات العاملة في قطاع الاتصالات وتقنية المعلومات.
- تم ترقيم مبدأ ونطاق ونص كل سياسة وفقًا لنظام الترقيم الموضح أدناه:

الشكل 2: نظام ترقيم السياسات الأساسية والخاصة

التطبيق والالتزام

تطور هيئة الاتصالات وتقنية المعلومات تنظيمات وقواعد منبثقة من سياسات الأمن الرقمي لقطاع الاتصالات وتقنية المعلومات، كما تقوم الهيئة بمتابعة تطبيق السياسات والالتزام بها لمزودي خدمات الاتصالات وتقنية المعلومات، وترفع التقارير إلى الجهة المعنية بالأمن الرقمي في وزارة الاتصالات وتقنية المعلومات بشكل دوري ومتى دعت الحاجة بما يساهم في تحقيق مؤشرات الأهداف الاستراتيجية لمبادرة تعزيز الأمن الرقمي في قطاع الاتصالات وتقنية المعلومات كجزء من برنامج التحول الوطني "2.0" وهو أحد برامج رؤية 2030.

السياسات الأساسية للأمن الرقمي لقطاع الاتصالات وتقنية المعلومات

A.I مبدأ السياسات الأساسية للأمن الرقمي لقطاع الاتصالات وتقنية المعلومات

يتمثل في توفير الحد الأدنى لحوكمة وتعزيز وصمود الأمن الرقمي بالإضافة الى الحوسبة السحابية والأطراف الخارجية للشركات العاملة في قطاع الاتصالات وتقنية المعلومات. يوضح الجدول 3 الوارد أدناه نطاقات السياسات الأساسية للأمن الرقمي الخاص بقطاع الاتصالات وتقنية المعلومات التي يجب أن يتم تنفيذها.

A.I.1	حوكمة الأمن الرقمي Digital Security Governance	A.I.13	إدارة أمن الشبكات Networks Security Management
A.I.2	إدارة مخاطر الأمن الرقمي Digital Security Risk Management	A.I.14	أمن الأجهزة المحمولة Mobile Devices Security
A.I.3	الأمن الرقمي في إدارة التغيير Digital Security in Change Management	A.I.15	حماية البيانات والمعلومات Data and Information Protection
A.I.4	الأمن الرقمي ضمن إدارة مشاريع الأصول المعلوماتية Digital Security for Information Asset Project Management	A.I.16	التشفير Cryptography
A.I.5	الأمن الرقمي ضمن إدارة مشاريع النظم المعلوماتية Digital Security for Information Systems Project Management	A.I.17	إدارة النسخ الاحتياطية والاستعادة Backup and Recovery Management
A.I.6	إدارة الألتزام بتشريعات الأمن الرقمي Digital Security Compliance Management	A.I.18	إدارة ثغرات الأمن الرقمي واختبار الاختراق Digital Security Vulnerabilities Management and Penetration Testing
A.I.7	الأمن الرقمي المتعلق بالموارد البشرية Digital Security in Human Resource	A.I.19	إدارة سجلات الأحداث ومراقبة الأمن الرقمي Digital Security Events Logging and Monitoring
A.I.8	التوعية والتدريب بالأمن الرقمي Digital Security Awareness and Training	A.I.20	إدارة تهديدات وحوادث الأمن الرقمي Digital Security Incident and Threat Management
A.I.9	إدارة الأصول Asset Management	A.I.21	الأمن المادي Physical Security
A.I.10	إدارة هويات الدخول والصلاحيات Identity and Access Management	A.I.22	أمن التطبيقات للويب والأجهزة الذكية Web Application Security
A.I.11	أمن النظم المعلوماتية ومرافق معالجة المعلومات Information Systems and Processing Facilities Security	A.I.23	إدارة استمرارية الأعمال Business Continuity Management
A.I.12	الأمن الرقمي للبريد الإلكتروني Email Digital Security	A.I.24	الأمن الرقمي المتعلق بالأطراف الخارجية Third –Party Management

الجدول 3: نطاقات السياسات الأساسية للأمن الرقمي الخاص بقطاع الاتصالات وتقنية المعلومات

نصوص نطاق السياسات الأساسية لقطاع الاتصالات وتقنية المعلومات

A.I.1 حوكمة الأمن الرقمي

1. يجب إعداد استراتيجية للأمن الرقمي وتوثيقها وفقًا للمتطلبات التشريعية والتنظيمية ذات الصلة.
2. يجب إنشاء لجنة إشرافية لحوكمة الأمن الرقمي وتفويض مسؤولية ضمان تنفيذ أهداف الأمن الرقمي على النحو الموضح في الاستراتيجية، وتوفر الدعم للإدارة المعنية بالأمن الرقمي.
3. يجب إنشاء إدارة معنية بالأمن الرقمي مستقلة عن إدارة تقنية المعلومات، وتفويض المهام ذات الصلة للحفاظ على العمليات المتعلقة بالأمن الرقمي، ويفضل ارتباطها برئيس الشركة أو من ينيبه.
4. يجب أن تعمل الإدارة المعنية بالأمن الرقمي على إعداد سياسات ومعايير وإجراءات الأمن الرقمي.
5. يجب اعتماد سياسات ومعايير الأمن الرقمي وتنفيذها بواسطة الإدارة المعنية بالأمن الرقمي ونشرها على الأطراف المعنية.
6. يجب مراجعة استراتيجية وسياسات ومعايير الأمن الرقمي والأدوار والمسؤوليات ذات الصلة بشكل دوري أو عند إجراء تغييرات للمواءمة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

A.I.2 إدارة مخاطر الأمن الرقمي

1. يجب إعداد منهجية لإدارة مخاطر الأمن الرقمي وتوثيقهما ودمجهما في خطة الشركة لإدارة المخاطر.
2. يجب اعتماد منهجية إدارة مخاطر الأمن الرقمي وذلك وفقا لاعتبارات سرية وتوافر وسلامة الأصول والنظم المعلوماتية.
3. يجب على الإدارة المعنية بالأمن الرقمي تطبيق منهجية وإجراءات إدارة مخاطر الأمن الرقمي في الشركة.
4. يجب مراجعة منهجية إدارة مخاطر الأمن الرقمي بشكل دوري أو عند إجراء تغييرات للمواءمة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

A.I.3 الأمن الرقمي في إدارة التغيير

1. يجب إعداد منهجية إدارة تغيير الأمن الرقمي وتوثيقها واعتمادها وتنفيذها من خلال الإدارة المعنية بالأمن الرقمي.
2. يجب إدراج متطلبات الأمن الرقمي ضمن منهجية إدارة التغيير المعتمدة.
3. يجب دمج متطلبات إدارة تغيير الأمن الرقمي مع جميع خطط المشاريع واعتمادها من قبل الإدارات المختصة، للتعرف على مخاطر الأمن الرقمي وإدارتها من خلال دورة حياة المشروع.
4. يجب مراجعة متطلبات الأمن الرقمي لمنهجية إدارة التغيير بشكل دوري أو عند إجراء تغييرات للمواءمة مع سياسات الشركة.

A.I.4 الأمن الرقمي ضمن إدارة مشاريع الأصول المعلوماتية

1. يجب إعداد متطلبات الأمن الرقمي لإدارة مشاريع الأصول المعلوماتية واعتمادها وتنفيذها ودمجها في منهجية إدارة التغيير للأمن الرقمي.
2. يجب أن تشمل متطلبات الأمن الرقمي لإدارة مشاريع الأصول المعلوماتية عملية إجراء التقييمات ووضع خطط المعالجة.
3. يجب أن تتضمن متطلبات الأمن الرقمي لإدارة مشاريع الأصول المعلوماتية التأكد من وجود نسخ احتياطية للأصول المعلوماتية قبل بدء أي مشروع أو عند إجراء تغييرات أوتحديثات.
4. يجب مراجعة متطلبات الأمن الرقمي لإدارة الأصول المعلوماتية بشكل دوري أو عند إجراء تغييرات للمواءمة مع سياسات الشركة.

A.I.5 الأمن الرقمي ضمن إدارة مشاريع النظم المعلوماتية

1. يجب إعداد متطلبات الأمن الرقمي لإدارة مشاريع النظم المعلوماتية واعتمادها وتنفيذها ودمجها في منهجية إدارة التغيير للأمن الرقمي.
2. يجب أن تتضمن متطلبات الأمن الرقمي لإدارة مشاريع النظم المعلوماتية تطبيق ممارسات التطوير الآمن للبرامج.
3. يجب أن تتضمن متطلبات الأمن الرقمي لإدارة النظم المعلوماتية التأكد من أن مصادر نظم المعلومات موثوقة ومرخصة.
4. يجب أن تتضمن متطلبات الأمن الرقمي لإدارة تغيير النظم المعلوماتية إنشاء خط أساس للإعدادات الحالية قبل بدء أي مشروع أو عند إجراء تغييرات أوتحديثات.
5. يجب مراجعة متطلبات الأمن الرقمي لإدارة النظم المعلوماتية بشكل دوري أو عند إجراء تغييرات للمواءمة مع سياسات الشركة.

A.I.6 إدارة الالتزام بتشريعات الأمن الرقمي

1. يجب وضع متطلبات الالتزام بتشريعات الأمن الرقمي بما يتماشى مع المتطلبات التشريعية والتنظيمية ذات العلاقة والقابلة للتطبيق.
2. يجب متابعة التطبيق والالتزام لتشريعات الأمن الرقمي وتوثيق النتائج من خلال الإدارة المعنية بشكل دوري.

A.I.7 الأمن الرقمي المتعلق بالموارد البشرية

1. يجب توثيق متطلبات الأمن الرقمي للعاملين واعتمادها ودمجها في شروط التوظيف ودورة التوظيف بأكملها.

2. يتم تنفيذ متطلبات الأمن الرقمي للعاملين بالتعاون مع إدارة الموارد البشرية.
3. يجب أن يكون جميع العاملين على دراية بمتطلبات الأمن الرقمي والشروط المرتبطة بها.
4. يجب التأكد أن متطلبات الأمن الرقمي تتضمن مراجعة صلاحيات الوصول الخاصة بالعاملين واتخاذ الإجراءات اللازمة بناءً على حالتهم الوظيفية.
5. يجب مراجعة متطلبات الأمن الرقمي للعاملين بشكل دوري أو عند إجراء تغييرات للمواءمة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

A.I.8 التوعية والتدريب بالأمن الرقمي

1. يجب إعداد متطلبات الأمن الرقمي الخاصة بالتوعية والتدريب وتوثيقها واعتمادها وتنفيذها.
2. يجب تطوير برنامج للتدريب والتوعية بالأمن الرقمي بما يتوافق مع متطلبات الأمن الرقمي.
3. يجب نشر برنامج التوعية والتدريب بالأمن الرقمي باستخدام وسائل تواصل متعددة.
4. يجب إجراء التوعية بالأمن الرقمي مع جميع المستخدمين والأطراف المعنية.
5. يجب مراجعة برنامج التوعية والتدريب بالأمن الرقمي للعاملين بشكل دوري أو عند إجراء تغييرات للمواءمة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

A.I.9 إدارة الأصول

1. يجب إعداد متطلبات الأمن الرقمي لإدارة واستخدام الأصول والنظم المعلوماتية وتوثيقها واعتمادها وتنفيذها.
2. يجب تحديد الأصول والنظم المعلوماتية وتوثيقها وتصنيفها وحمايتها بناءً على متطلبات الأمن الرقمي ودمجها في سجل الأصول.
3. يجب مراجعة متطلبات الأمن الرقمي لإدارة الأصول والنظم المعلوماتية بشكل دوري أو عند إجراء تغييرات للمواءمة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

A.I.10 إدارة هويات الدخول والصلاحيات

1. يجب إعداد متطلبات الأمن الرقمي لإدارة هويات الدخول والصلاحيات وتوثيقها واعتمادها وتنفيذها.
2. يجب أن تتضمن النظم المعلوماتية التعرف على المستخدمين بشكل فريد من خلال تطبيق آليات المصادقة وإعطاء الصلاحيات وفقًا لسياسات ومعايير التحكم في الوصول ذات العلاقة.
3. يجب الموافقة على طلبات صلاحيات الوصول إلى الأصول والنظم المعلوماتية وتنفيذها بناءً على المهام والوظيفية وإدارتها ومراجعتها بشكل آمن.
4. يجب اتباع مبدأ أقل الصلاحيات اللازمة لتنفيذ الأعمال للمستخدمين.
5. يجب إدارة التحكم في الوصول والصلاحيات الخاصة بحسابات المستخدمين بشكلٍ آمن.
6. يجب مراجعة أنشطة المستخدمين والمحافظة عليها بشكل دوري.
7. يجب مراجعة تنفيذ متطلبات الأمن الرقمي لإدارة هويات الدخول والصلاحيات بشكل دوري أو عند إجراء تغييرات للمواءمة مع المتطلبات التشريعية أو التنظيمية ذات العلاقة.

A.I.11 أمن النظم المعلوماتية ومرافق معالجة المعلومات

1. يجب إعداد متطلبات الأمن الرقمي لتأمين النظم المعلوماتية ومرافق معالجة المعلومات وتوثيقها واعتمادها وتنفيذها.
2. يجب أن تشمل متطلبات الأمن الرقمي على الإدارة الآمنة للبرامج الضارة وحماية الفيروسات.
3. يجب أن تشمل متطلبات الأمن الرقمي على الإدارة الآمنة لوسائط التخزين الداخلية والخارجية.
4. يجب أن تشمل متطلبات الأمن الرقمي على الإدارة الآمنة لحزم التحديثات والإصلاحات.
5. يجب دمج متطلبات الأمن الرقمي لمرافق معالجة المعلومات في منهجية إدارة مشاريع ذات العلاقة.
6. يجب مراجعة متطلبات الأمن الرقمي لتأمين النظم المعلوماتية ومرافق معالجة المعلومات بشكل دوري أو عند إجراء تغييرات للمواءمة مع المتطلبات التشريعية أو التنظيمية ذات العلاقة.

A.I.12 الأمن الرقمي للبريد الإلكتروني

1. يجب إعداد متطلبات الأمن الرقمي للبريد الإلكتروني وتوثيقها واعتمادها وتنفيذها.
2. يجب أن تتضمن متطلبات الأمن الرقمي الكشف عن مخاطر أمن البريد الإلكتروني والوقاية منها وإدارتها.
3. يجب أن تشمل متطلبات الأمن الرقمي للبريد الإلكتروني على التوعية بتهديدات الهندسة الاجتماعية، وكذلك طرق التعرف على البريد العشوائي والرسائل الإلكترونية المشتبه بها.
4. يجب مراجعة متطلبات الأمن الرقمي لحماية البريد الإلكتروني بشكل دوري أو عند إجراء تغييرات للمواءمة مع المتطلبات التشريعية أو التنظيمية ذات العلاقة.

A.I.13 إدارة أمن الشبكات

1. يجب تحديد متطلبات الأمن الرقمي لإدارة أمن الشبكات وتوثيقها واعتمادها وتنفيذها.
2. يجب أن تشمل متطلبات الأمن الرقمي على تصميم وتنفيذ بنية شبكات آمنة متعددة المستويات.
3. يجب أن تشمل متطلبات الأمن الرقمي على أنظمة تمنع الوصول غير المصرح به إلى الشبكة ومواردها ومكوناتها ووسائط التخزين المتصلة بها.
4. يجب أن تشمل متطلبات الأمن الرقمي الحفاظ على مخططات بنية الشبكة الحالية وتصميمها وتدفق البيانات.
5. يجب أن تشمل متطلبات الأمن الرقمي إدارة ومراجعة اتفاقيات خدمات الشبكة مع الأطراف ذات العلاقة.
6. يجب مراجعة متطلبات الأمن الرقمي لإدارة أمن الشبكات بشكل دوري أو عند إجراء تغييرات للمواءمة مع المتطلبات التشريعية أو التنظيمية ذات العلاقة.

A.I.14 أمن الأجهزة المحمولة

1. يجب إعداد متطلبات الأمن الرقمي للأجهزة المحمولة وتوثيقها واعتمادها وتنفيذها.
2. يجب أن تشمل متطلبات الأمن الرقمي على حلول آمنة تتيح التحكم بمعلومات الشركة وتشفيرها وحذفها عند الحاجة.
3. يجب مراجعة متطلبات الأمن الرقمي الخاصة بأمن الأجهزة المحمولة بشكل دوري أو عند إجراء تغييرات للمواءمة مع المتطلبات التشريعية أو التنظيمية ذات العلاقة.

A.I.15 حماية البيانات والمعلومات

1. يجب إعداد متطلبات الأمن الرقمي لحماية وإدارة البيانات والمعلومات وتوثيقها واعتمادها وتنفيذها.
2. يجب أن تشمل متطلبات الأمن الرقمي للبيانات والمعلومات الملكية والتصنيف والخصوصية.
3. يجب أن تشمل متطلبات الأمن الرقمي للبيانات والمعلومات التدابير المناسبة لحماية المعلومات الشخصية من الضياع وإساءة الاستخدام والوصول غير المصرح به.
4. يجب مراجعة متطلبات الأمن الرقمي لحماية وإدارة البيانات والمعلومات بشكل دوري أو عند إجراء أي تغييرات للمواءمة مع المتطلبات التشريعية أو التنظيمية ذات العلاقة.

A.I.16 التشفير

1. يجب إعداد متطلبات الأمن الرقمي الخاصة بالتشفير وتوثيقها واعتمادها وتنفيذها.
2. يجب أن تشمل متطلبات الأمن الرقمي الخاصة بالتشفير على معايير آمنة ومعتمدة لإدارة أنظمة ومفاتيح التشفير.
3. يجب مراجعة متطلبات الأمن الرقمي الخاصة بالتشفير بشكل دوري أو عند إجراء تغييرات للمواءمة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

A.I.17 إدارة النسخ الاحتياطية والاستعادة

1. يجب إعداد متطلبات الأمن الرقمي الخاصة بالنسخ الاحتياطية والاستعادة وتوثيقها واعتمادها وتنفيذها.
2. يجب أن تشمل متطلبات الأمن الرقمي على خطط النسخ الاحتياطي والاستعاده والاختبار بشكل دوري للأصول والنظم المعلوماتية.
3. يجب مراجعة متطلبات الأمن الرقمي لإدارة النسخ الاحتياطية والاستعادة بشكل دوري أو عند إجراء تغييرات للمواءمة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

A.I.18 إدارة ثغرات الأمن الرقمي واختبار الاختراق

1. يجب إعداد متطلبات الأمن الرقمي الخاصة بإدارة الثغرات واختبار الاختراق وتوثيقها واعتمادها وتنفيذها.
2. يجب أن تشمل متطلبات الأمن الرقمي لإدارة الثغرات الأمنية عمليات التقييم والتصنيف والمعالجة بشكل دوري.
3. يجب أن تشمل متطلبات الأمن الرقمي لإدارة اختبار الاختراق عمليات التقييم والتصنيف والمعالجة بنطاق عمل محدد وبشكل دوري.
4. يجب مراجعة متطلبات الأمن الرقمي الخاصة بإدارة الثغرات الأمنية واختبار الاختراق بشكل دوري أو عند إجراء تغييرات للمواءمة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

A.I.19 إدارة سجلات الأحداث ومراقبة الأمن الرقمي

1. يجب إعداد متطلبات الأمن الرقمي الخاصة بتسجيل الأحداث ومراقبتها وتوثيقها واعتمادها وتنفيذها.
2. يجب أن تشمل متطلبات الأمن الرقمي تفعيل تسجيل الأحداث ومراقبتها للأصول والنظم المعلوماتية وسجلات الوصول بناءً على احتياج العمل والمتطلبات التشريعية والتنظيمية ذات العلاقة.
3. يجب أن تتضمن متطلبات الأمن الرقمي لتسجيل الأحداث ومراقبتها أنظمة آمنة يمكنها الاحتفاظ بسجلات الأحداث لفترة محددة بناءً على احتياج العمل والمتطلبات التشريعية والتنظيمية ذات العلاقة.

4. يجب مراجعة متطلبات الأمن الرقمي الخاصة بتسجيل الأحداث ومراقبتها بشكل دوري أو عند إجراء تغييرات للمواءمة بناءً على احتياج العمل والمتطلبات التشريعية والتنظيمية ذات العلاقة.

A.I.20 إدارة تهديدات وحوادث الأمن الرقمي

1. يجب إعداد متطلبات الأمن الرقمي الخاصة بإدارة التهديدات والحوادث وتوثيقها واعتمادها وتنفيذها.
2. يجب أن تشمل متطلبات الأمن الرقمي الخاصة بإدارة التهديدات والحوادث على مراقبة حوادث الأمن الرقمي وتسجيلها وتقييمها ومعالجتها.
3. يجب أن تشمل متطلبات الأمن الرقمي الخاصة بإدارة التهديدات والحوادث على تصنيف أولويات حوادث الأمن الرقمي المحددة وترتيبها ومشاركتها مع الأطراف المعنية عند الحاجة.
4. يجب مراجعة متطلبات الأمن الرقمي الخاصة بإدارة التهديدات والحوادث بشكل دوري أو عند إجراء تغييرات للمواءمة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

A.I.21 الأمن المادي

1. يجب إعداد متطلبات الأمن الرقمي الخاصة بالأمن المادي وتوثيقها واعتمادها وتنفيذها.
2. يجب دمج متطلبات الأمن الرقمي الخاصة بالأمن المادي والإجراءات التصحيحية في خطة استمرارية أعمال الشركة.
3. يجب أن تشمل متطلبات الأمن الرقمي الخاصة بالأمن المادي على الحماية المادية للمباني ومراكز البيانات التي تحتوي على الأصول والنظم المعلوماتية الخاصة بالشركة.
4. يجب أن تشمل متطلبات الأمن الرقمي الخاصة بالأمن المادي على آليات تحكم وتسجيل ومراقبة دخول العاملين والزوار.
5. يجب أن تشمل متطلبات الأمن الرقمي حماية ومراقبة موارد وإمدادات الطاقة من انقطاع التيار الكهربائي والحرائق والفيضانات والمخاطر البيئية والطبيعية.
6. يجب مراجعة متطلبات الأمن الرقمي الخاصة بالأمن المادي بشكلٍ دوري أو عند إجراء تغييرات للمواءمة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

A.I.22 أمن التطبيقات للويب والأجهزة الذكية

1. يجب إعداد متطلبات الأمن الرقمي لتطبيقات الويب والأجهزة الذكية وتوثيقها واعتمادها وتنفيذها.
2. يجب أن تشمل متطلبات الأمن الرقمي أنظمة حماية متعددة المستويات باستخدام البروتوكولات الآمنة.
3. يجب أن تشمل متطلبات الأمن الرقمي إجراء تقييم الثغرات واختبار الاختراق ومعالجة الثغرات حسب تصنيفها قبل إطلاق التطبيقات.
4. يجب مراجعة متطلبات الأمن الرقمي بشكل دوري أو عند إجراء تغييرات للمواءمة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

A.I.23 إدارة استمرارية الأعمال

1. يجب إعداد متطلبات الأمن الرقمي الخاصة بخطط استمرارية الأعمال والتعافي من الكوارث وتوثيقها واعتمادها وتنفيذها.
2. يجب تضمين متطلبات الأمن الرقمي في خطة استمرارية العمل الخاصة بالشركة.
3. يجب تنفيذ متطلبات الأمن الرقمي من خلال الإدارة المعنية بالتعاون مع الأطراف ذات العلاقة.
4. يجب أن تشمل متطلبات الأمن الرقمي اختبارات لخطط استمرارية الأعمال والتعافي من الكوارث بشكل دوري بالتعاون مع الأطراف ذات العلاقة.
5. يجب مراجعة متطلبات الأمن الرقمي الخاصة باستمرارية الأعمال والتعافي من الكوارث بشكلٍ دوري أو عند إجراء تغييرات للمواءمة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

A.I.24 إدارة الأمن الرقمي المتعلق بالأطراف الخارجية

1. يجب إعداد متطلبات الأمن الرقمي المتعلقة بالأطراف الخارجية وتوثيقها واعتمادها وتنفيذها.
2. يجب أن تشمل متطلبات الأمن الرقمي بنودًا مفصلة ومحددة تركز على المخاطر الرقمية وإدارة الأصول والنظم المعلوماتية والوصول إليها وتطبيق ذلك طوال فترة العلاقة التعاقدية.
3. يجب تضمين متطلبات الأمن الرقمي الخاصة بوصول الطرف الخارجي إلى المعلومات وإدارتها في العقود والاتفاقيات المعتمدة مع هذه الأطراف.
4. يجب مراجعة متطلبات الأمن الرقمي المتعلقة بالأطراف الخارجية بشكل دوري أو عند إجراء تغييرات للمواءمة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

سياسات الأمن الرقمي الخاصة بخدمات قطاع الاتصالات وتقنية المعلومات

تتمثل مبادئ هذه السياسة في توفير سياسات أمنية رقمية محددة للشركات العاملة في قطاع الاتصالات وتقنية المعلومات التي تقدم خدمات الاتصالات وتقنية المعلومات التالية وفقًا للمتطلبات التشريعية والتنظيمية المتبعة.

تتألف سياسات الأمن الرقمي الخاصة بخدمات قطاع الاتصالات وتقنية المعلومات من سبع خدمات لقطاع الاتصالات وتقنية المعلومات:

- **خدمات صوتية:** شركات تقدم خدمات صوتية تقليدية، مثل الخدمات الصوتية الأرضية والقائمة على بروتوكول الإنترنت كخدمات الصوت عبر الإنترنت (VoIP).
- **خدمات الرسائل القصيرة:** شركات تقدم خدمات الرسائل القصيرة.
- **خدمات الإنترنت:** شركات تقدم خدمات الإنترنت.
- **خدمات الاتصال:** شركات تقدم خدمات الاتصال مثل محطات طرفية (VSAT) والهواتف المحمولة والمايكرويف والألياف البصرية.
- **الحوسبة السحابية:** شركات تقدم خدمات سحابية، مثل البنية التحتية كخدمة والبرمجيات كخدمة والمنصة كخدمة.
- **التقنيات الناشئة:** شركات تقدم حلول التقنيات الناشئة، مثل إنترنت الأشياء وخدمات الذكاء الصناعي وخدمات تقنية "البلوك تشين" والواقع المعزز/ الافتراضي.
- **الخدمات المدارة:** شركات تقدم مجموعة من خدمات الاتصالات وتقنية المعلومات المخصصة والمحددة زمنيًا لعملائها على أساس تعاقدي.

تتكون سلسلة خدمات الاتصالات وتقنية المعلومات من المكونات الأربعة التالية:

- **البنية التحتية الغير نشطة:** شركات تصميم البنية التحتية الغير نشطة وبنائها وتشغيلها.
- **البنية التحتية النشطة:** شركات تصميم البنية التحتية النشطة وبنائها وتشغيلها.
- **مطورو البرامج والتطبيقات:** شركات إعداد برامج مثل التطبيقات والأنظمة الأساسية.
- **مزودو خدمات الاتصالات وتقنية المعلومات (مزودو الخدمة):** شركات تقدم خدمات الاتصالات وتقنية المعلومات للمستخدمين النهائيين.

B.II مبدأ سياسة الأمن الرقمي الخاصة بالخدمات الصوتية

تحدد سياسة الأمن الرقمي الخاصة بالخدمات الصوتية الحد الأدنى من متطلبات الأمن الرقمي لشركات خدمات الاتصالات وتقنية المعلومات التي تقدم خدمات صوت تقليدية، وتشمل هذه الخدمات الخطوط الأرضية والخدمات الصوتية القائمة على الإنترنت، مثل خدمات الصوت عبر الإنترنت (VOIP). كما تحدد متطلبات تأمين الوصول إلى خدمات الاتصالات الهاتفية ومقاسم الهاتف وشبكات إصدار الإشارات والبنية التحتية التقنية للخدمات الصوتية عبر الإنترنت.

B.II.1	متطلبات الأمن الرقمي الخاصة بالخدمات الصوتية
خدمات صوتية: البنية التحتية النشطة	
B.II.2	إدارة هويات الدخول والصلاحيات الخاصة بالخدمات الصوتية
B.II.3	إدارة أمن الشبكات الخاصة بالخدمات الصوتية
B.II.4	إدارة ثغرات الأمن الرقمي واختبار الاختراق الخاصة بالخدمات الصوتية
B.II.5	إدارة مكافحة الرسائل الاقتحامية الخاصة بالخدمات الصوتية
خدمات صوتية: مزودو الخدمة	
B.II.6	حماية البيانات والمعلومات الخاصة بالخدمات الصوتية
B.II.7	التوعية والتدريب بالأمن الرقمي الخاص بالخدمات الصوتية

الجدول 4: نطاقات سياسة الأمن الرقمي الخاصة بالخدمات الصوتية

نصوص نطاق سياسة الأمن الرقمي الخاصة بالخدمات الصوتية

B.II.1. متطلبات الأمن الرقمي الخاصة بالخدمات الصوتية

1. يجب إعداد متطلبات الأمن الرقمي الخاصة بالخدمات الصوتية وتوثيقها واعتمادها وتنفيذها.
2. يجب مراجعة متطلبات الأمن الرقمي للخدمات الصوتية بشكلٍ دوري أو عند إجراء تغييرات للمواءمة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

نصوص السياسة الخاصة بالبنية التحتية النشطة

B.II.2. إدارة هويات الدخول والصلاحيات الخاصة بالخدمات الصوتية

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. استخدام آلية مصادقة فعالة للتحقق من مشتركي الخدمات الصوتية.
2. تنفيذ آلية تحكم آمنة لمنع سرقة الهوية الرقمية لمشتركي الخدمات الصوتية.

B.II.3. إدارة أمن الشبكات الخاصة بالخدمات الصوتية

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. حماية الخوادم وشبكة خدمات الاتصالات الهاتفية التقليدية أو القائمة على الإنترنت.
2. حماية أنظمة ومقاسم الهاتف.
3. حماية شبكات إصدار الإشارات لحمايتها من أي تهديدات قد تؤدي إلى إساءة استخدام المعلومات.
4. حماية شبكات الصوت عبر بروتوكول الإنترنت (VOIP) لمنع أي اعتراض للمعلومات.

B.II.4. إدارة ثغرات الأمن الرقمي واختبار الاختراق الخاصة بالخدمات الصوتية

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. تقييم الثغرات الأمنية واختبار الاختراق وتصنيف ومعالجة الثغرات للأصول والنظم المعلوماتية الخاصة بالخدمات الصوتية بشكل دوري.
2. تقييم وتصنيف ومعالجة الثغرات الأمنية الخاصة بشبكات إصدار الإشارة بشكل دوري.

B.II.5. إدارة مكافحة الرسائل الاقتحامية الخاصة بالخدمات الصوتية

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. تنفيذ آلية تحكم لمكافحة الرسائل الاقتحامية الخاصة بالخدمات الصوتية.

نصوص السياسة لمزودي الخدمة

B.II.6. حماية البيانات والمعلومات الخاصة بالخدمات الصوتية

يجب على مزودي الخدمات:

1. التأكد من أن الاتفاقيات ونماذج الثقة بين الأطراف المعنية تشمل منهجية تحمي وتحافظ على الخصوصية كجزء من تصميمها.

B.II.7. التدريب والتوعية بالأمن الرقمي الخاص بالخدمات الصوتية

يجب على مزودي الخدمات:

1. توفير توعية للمستخدمين تركز على اكتشاف المكالمات الهاتفية المشبوهة أو حوادث سرقة المعلومات الشخصية المهمة عبر الاتصال.

C.III مبدأ سياسة الأمن الرقمي الخاصة بخدمات الرسائل القصيرة

توفر سياسة الأمن الرقمي الخاصة بخدمات الرسائل القصيرة الحد الأدنى من متطلبات الأمن الرقمي لشركات خدمات الاتصالات وتقنية المعلومات التي تقدم خدمات الرسائل القصيرة، وتتناول سياسة الرسائل القصيرة تأمين الوصول إلى عمليات البنية التحتية للرسائل القصيرة وخدماتها، وتحدد تدابير لإدارة الرسائل القصيرة الاقتحامية وخصوصية البيانات.

C.III.1	متطلبات الأمن الرقمي الخاصة بخدمات الرسائل القصيرة
رسائل قصيرة: البنية التحتية النشطة	
C.III.2	إدارة هويات الدخول والصلاحيات الخاصة بخدمات الرسائل القصيرة
C.III.3	إدارة أمن الشبكات الخاصة بخدمات الرسائل القصيرة
C.III.4	إدارة ثغرات الأمن الرقمي واختبار الاختراق الخاصة بخدمات الرسائل القصيرة
C.III.5	إدارة مكافحة الرسائل الاقتحامية الخاصة بخدمات الرسائل القصيرة
رسائل قصيرة: مزودو الخدمة	
C.III.6	حماية البيانات والمعلومات الخاصة بخدمات الرسائل القصيرة
C.III.7	التوعية الأمنية والتدريب الخاص بخدمات الرسائل القصيرة

الجدول 5: نطاقات سياسة الأمن الرقمي الخاصة بخدمات الرسائل القصيرة

نصوص نطاق سياسة الأمن الرقمي الخاصة بخدمات الرسائل القصيرة

C.III.1 متطلبات الأمن الرقمي الخاصة بخدمات الرسائل القصيرة

1. يجب إعداد متطلبات الأمن الرقمي الخاصة بخدمات الرسائل القصيرة وتوثيقها واعتمادها وتنفيذها.
2. يجب مراجعة متطلبات الأمن الرقمي الخاصة بخدمات الرسائل القصيرة بشكلٍ دوري أو عند إجراء تغييرات للمواءمة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

نصوص السياسة الخاصة بالبنية التحتية النشطة

C.III.2 إدارة هويات الدخول والصلاحيات الخاصة بخدمات الرسائل القصيرة

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. استخدام آلية مصادقة فعالة للتحقق من مشتركي خدمات الرسائل القصيرة.
2. تنفيذ آلية تحكم آمنة لمنع سرقة الهوية الرقمية لمشتركي خدمات الرسائل القصيرة.

C.III.3 إدارة أمن الشبكات الخاصة بخدمات الرسائل القصيرة

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. حماية خوادم وشبكات الاتصال والتأكد من موثوقيتها لخدمات الرسائل القصيرة.
2. وضع آلية تحكم للحد من حوادث اعتراض الرسائل القصيرة.
3. وضع آلية تحكم للحد من حوادث حجب الخدمة وانتحال الهوية عبر بوابات الرسائل القصيرة.

C.III.4 إدارة ثغرات الأمن الرقمي واختبار الاختراق الخاصة بخدمات الرسائل القصيرة

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. تقييم الثغرات الأمنية واختبار الاختراق وتصنيف ومعالجة الثغرات للأصول والنظم المعلوماتية الخاصة بخدمات الرسائل القصيرة بشكل دوري.
2. تقييم وتصنيف ومعالجة الثغرات الأمنية للكود المصدري الخاص بتطبيقات خدمات الرسائل القصيرة بشكل دوري.

C.III.5 إدارة مكافحة الرسائل الاقتحامية الخاصة بخدمات الرسائل القصيرة

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. تطبيق أنظمة تصفية للرسائل الاقتحامية التي يمكنها التكيف مع تفضيلات المستخدمين المحددة مسبقًا لمنع تلقي رسائل اقتحامية غير مرغوب فيها.

نصوص السياسة لمزودي الخدمة

C.III.6. حماية البيانات والمعلومات الخاصة بخدمات الرسائل القصيرة

يجب على مزودي الخدمات:

1. التأكد من أن الاتفاقيات ونماذج الثقة بين الأطراف المعنية تشمل منهجية تحمي وتحافظ على الخصوصية كجزء من تصميمها.

C.III.7. التدريب والتوعية بالأمن الرقمي الخاص بخدمات الرسائل القصيرة

يجب على مزودي الخدمات:

1. توفير برامج التدريب والتوعية بالأمن الرقمي لمستخدمي الرسائل القصيرة تركز على حوادث الخداع الإلكتروني عبر الرسائل القصيرة.

D.IV مبدأ سياسة الأمن الرقمي الخاصة بخدمات الإنترنت

توفر سياسة الأمن الرقمي الخاصة بخدمات الإنترنت الحد الأدنى من متطلبات الأمن الرقمي للشركات المقدمة لخدمات الإنترنت، وتشمل خدمات الإنترنت عادةً الوصول إلى الإنترنت والنفاذ إليه وتسجيل اسم النطاق واستضافة الويب والوصول إلى البنية التحتية والخدمات عبر الإنترنت.

D.IV.1	متطلبات الأمن الرقمي الخاصة بخدمات الإنترنت
خدمات الإنترنت: البنية التحتية النشطة	
D.IV.2	إدارة هويات الدخول والصلاحيات الخاصة بخدمات الإنترنت
D.IV.3	حماية البيانات والمعلومات الخاصة بخدمات الإنترنت
D.IV.4	إدارة ثغرات الأمن الرقمي واختبار الاختراق الخاصة بخدمات الإنترنت
D.IV.5	إدارة أمن الشبكات الخاصة بخدمات الإنترنت
D.IV.6	إدارة الإعدادات الآمنة الخاصة بخدمات الإنترنت
D.IV.7	الأمن المادي الخاص بخدمات الإنترنت
D.IV.8	حماية الاتصال الخاص بخدمات الإنترنت
D.IV.9	إدارة أمن البيانات الرقمية الخاصة بخدمات الإنترنت
D.IV.10	إدارة الأصول الخاصة بخدمات الإنترنت
خدمات الإنترنت: مزودو الخدمة	
D.IV.11	إدارة هويات الدخول والصلاحيات الخاصة بخدمات الإنترنت
D.IV.12	حماية الاتصال الخاص بخدمات الإنترنت
D.IV.13	إدارة الحوادث الخاصة بخدمات الإنترنت
D.IV.14	حماية البيانات والمعلومات الخاصة بخدمات الإنترنت
D.IV.15	التدريب والتوعية بالأمن الرقمي الخاص بخدمات الإنترنت

الجدول 6: نطاقات سياسة الأمن الرقمي الخاصة بخدمات الإنترنت

نصوص نطاق سياسة الأمن الرقمي الخاصة بخدمات الإنترنت

D.IV.1. متطلبات الأمن الرقمي الخاصة بخدمات الإنترنت

1. يجب إعداد متطلبات الأمن الرقمي الخاصة بخدمات الإنترنت وتوثيقها واعتمادها وتنفيذها.
2. يجب مراجعة متطلبات الأمن الرقمي الخاصة بخدمات الإنترنت بشكلٍ دوري أو عند إجراء تغييرات للمواءمة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

نصوص السياسة الخاصة بالبنية التحتية النشطة

D.IV.2. إدارة هويات الدخول والصلاحيات الخاصة بخدمات الإنترنت

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. استخدام آلية مصادقة فعالة لموردي الأصول والنظم المعلوماتية لخدمات الإنترنت.
2. إدارة صلاحيات الموردين الذين يديرون الأصول والنظم المعلوماتية التي تتيح خدمات الإنترنت.

D.IV.3. حماية البيانات والمعلومات الخاصة بخدمات الإنترنت

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. استخدم آليات تحكم لحماية خصوصية معلومات المستخدمين ومواقعهم.

D.IV.4. إدارة ثغرات الأمن الرقمي واختبار الاختراق الخاصة بخدمات الإنترنت

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. تقييم الثغرات الأمنية واختبار الاختراق وتصنيف ومعالجة الثغرات للأصول والنظم المعلوماتية الخاصة بخدمات الإنترنت بشكل دوري.
2. تقييم وتصنيف ومعالجة الثغرات الأمنية للكود المصدري الخاص بتطبيقات خدمات الإنترنت بشكل دوري.

D.IV.5. إدارة أمن الشبكات الخاصة بخدمات الإنترنت

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. تضمين بنود في اتفاقيات خدمات الشبكة لحماية الخدمات والأجهزة التي يديرها الموردون.
2. حماية خوادم وشبكات الاتصال والتأكد من موثوقيتها لخدمات الإنترنت.
3. وضع آلية تحكم للحد من حوادث اعتراض تدفق بيانات خدمات الإنترنت.
4. وضع آلية تحكم للحد من حوادث حجب الخدمة وانتحال الهوية عبر خدمات الإنترنت.

D.IV.6. إدارة الإعدادات الآمنة الخاصة بخدمات الإنترنت

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. الحفاظ على الإعدادات الأساسية للأصول والنظم المعلوماتية التي توفر خدمات الإنترنت وتأمينها.

D.IV.7. الأمن المادي الخاص بخدمات الإنترنت

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. التأكد من أن مراكز تشغيل خدمات الإنترنت مجهزة بأنظمة كشف مادية.
2. التأكد من توفير طاقة غير منقطعة للأجهزة المهمة في المناطق النائية.
3. إجراء عمليات تدقيق منتظمة للكابلات للكشف عن أي تغيير أو تلف.

D.IV.8. حماية الاتصال الخاص بخدمات الإنترنت

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. تطبيق حلول تقنية آمنة لترشيح الوصول إلى محتوى أو خدمات الإنترنت الضارة.
2. تطبيق حلول تقنية آمنة للحد من التنمر والابتزاز الإلكتروني عبر خدمات وتطبيقات الإنترنت.

D.IV.9. إدارة أمن البيانات الرقمية الخاصة بخدمات الإنترنت

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. حماية الأصول المعلوماتية بآليات تحكم مناسبة على عدة مستويات.
2. التأكد من حماية وتحصين النظم المعلوماتية الافتراضية باستخدام الحد الأدنى من متطلبات الأمن الرقمي.

D.IV.10. إدارة الأصول الخاصة بخدمات الإنترنت

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. الإعداد والاحتفاظ بسجل أصول يحوي تفاصيل الأصول المستخدمة في خدمات الإنترنت.

نصوص السياسة لمزودي الخدمة

D.IV.11. إدارة هويات الدخول والصلاحيات الخاصة بخدمات الإنترنت

يجب على مزودي الخدمات:

1. استخدام آلية مصادقة فعالة للتحقق من مشتركي خدمات الإنترنت.
2. تنفيذ آلية تحكم آمنة لمنع سرقة الهوية الرقمية لمشتركي خدمات الإنترنت.

D.IV.12. حماية الاتصال الخاص بخدمات الإنترنت

يجب على مزودي الخدمات:

1. التأكد من وجود آليات تمكن المستخدمين من الإبلاغ عن سوء استخدام الإنترنت من قِبل مستخدمين آخرين.

D.IV.13. إدارة الحوادث الخاصة بخدمات الإنترنت

يجب على مزودي الخدمات:

1. التأكد من وجود آليات تمكن المستخدمين من الإبلاغ عن حوادث أمنية رقمية.

D.IV.14. حماية البيانات والمعلومات الخاصة بخدمات الإنترنت

يجب على مزودي الخدمات:

1. التأكد من أن الاتفاقيات ونماذج الثقة بين الأطراف المعنية تشمل منهجية تحمي وتحافظ على الخصوصية كجزء من تصميمها.

D.IV.15. التدريب والتوعية بالأمن الرقمي الخاص بخدمات الإنترنت

يجب على مزودي الخدمات:

1. إجراء حملات توعية لتزويد مستخدمي الإنترنت بالمعلومات والإرشادات اللازمة للاستخدام الآمن والمسؤول لخدمات الإنترنت.

E.V مبدأ سياسة الأمن الرقمي الخاصة بخدمات الاتصال

توفر سياسة الأمن الرقمي الخاصة بخدمات الاتصال الحد الأدنى من متطلبات الأمن الرقمي للشركات المقدمة لخدمات الاتصال، والغرض من هذه السياسة هو تحديد نطاق أمن رقمي إضافي يجب على شركات خدمات الاتصالات وتقنية المعلومات تطبيقها عند تقديم خدمات الاتصال، وتغطي السياسة أمن خدمات الاتصال عبر وسائط مختلفة مثل المحطات الطرفية (VSAT) والهواتف المحمولة والمايكرويف والألياف البصرية.

E.V.1	متطلبات الأمن الرقمي الخاصة بخدمات الاتصال
خدمات الاتصال: البنية التحتية الغير نشطة	
E.V.2	الأمن المادي الخاص بخدمات الاتصال
خدمات الاتصال: البنية التحتية النشطة	
E.V.3	إدارة هويات الدخول والصلاحيات الخاصة بخدمات الاتصال
E.V.4	إدارة أمن الشبكات الخاصة بخدمات الاتصال
E.V.5	إدارة أمن البيانات الرقمية الخاصة بخدمات الاتصال
E.V.6	إدارة ثغرات الأمن الرقمي واختبار الاختراق الخاصة بخدمات الاتصال
E.V.7	التسجيل والمراقبة الخاصة بخدمات الاتصال
خدمات الاتصال: مزودو الخدمة	
E.V.8	حماية البيانات والمعلومات الخاصة بخدمات الاتصال
E.V.9	التدريب والتوعية بالأمن الرقمي الخاص بخدمات الاتصال

الجدول 7: نطاقات سياسة الأمن الرقمي الخاصة بخدمات الاتصال

نصوص نطاق سياسة الأمن الرقمي الخاصة بخدمات الاتصال

E.V.1. متطلبات الأمن الرقمي الخاصة بخدمات الاتصال

1. يجب إعداد متطلبات الأمن الرقمي لخدمات الاتصال وتوثيقها واعتمادها وتنفيذها.
2. يجب مراجعة متطلبات الأمن الرقمي لخدمات الاتصال بشكلٍ دوري أو عند إجراء تغييرات للمواءمة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

نصوص السياسة الخاصة بالبنية التحتية الغير نشطة

E.V.2. الأمن المادي الخاص بخدمات الاتصال

يجب على الشركات المقدمة لخدمات البنية التحتية الغير نشطة:

1. حماية منظومة أجهزة الأقمار الصناعية والمايكرويف والألياف البصرية.
2. حماية وظائف القياس عن بُعد والتتبع والتحكم (TT&C).
3. حماية وضمان عمليات الإرسال والاستقبال في اتصالات القمر الصناعي.
4. تطبيق إجراءات لحماية المحطات الرئيسية لخدمات الاتصالات المتنقلة.

نصوص السياسة الخاصة بالبنية التحتية النشطة

E.V.3. إدارة هويات الدخول والصلاحيات الخاصة بخدمات الاتصال

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. التحقق من المصادقة واعطاء الصلاحيات المناسبة للعاملين للوصول إلى شبكات الهواتف المحمولة وخدماتها.
2. التحقق من المصادقة واعطاء الصلاحيات المناسبة للعاملين للوصول إلى المحطات الطرفية (VSAT).
3. التحقق من المصادقة واعطاء الصلاحيات المناسبة للعاملين للوصول إلى شبكة الإرسال بالمايكرويف.
4. استخدام آلية مصادقة فعالة لموردي الأصول والنظم المعلوماتية لخدمات الاتصال.
5. إدارة صلاحيات الموردين الذين يديرون الأصول والنظم المعلوماتية التي تتيح خدمات الاتصال.

E.V.4. إدارة أمن الشبكات الخاصة بخدمات الاتصال

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. حماية بيانات الإشارة والترددات ومعلومات المستخدم من خلال تطبيق التشفير بما يتوافق مع التشريعات والتنظيمات ذات العلاقة.

2. تطبيق آليات لحماية الإرسال والاستقبال عبر بروتوكول الإنترنت (البث الأحادي والبث المتعدد) في اتصالات المحطات الطرفية (VSAT).
3. تمكين تشفير مناسب في الوصلة الصاعدة بترددات الراديو عالية القدرة المستخدمة في اتصالات المحطات الطرفية (VSAT).
4. تطبيق آليات لتمكين التشفير المناسب للوصلات التي تعمل بالمايكروويف.
5. تطبيق آليات لتقييد تغيير خوارزميات التشفير بين الأجهزة المحمولة وبرج الخدمة أثناء تحويل المكالمة.

E.V.5. إدارة أمن البيانات الرقمية الخاصة بخدمات الاتصال

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. عدم الكشف عن عناوين بروتوكولات الانترنت (IP) الداخلية للنظم المعلوماتية عبر الإنترنت.
2. تشفير معلومات الهوية الرقمية والعنوان الرقمي على الوصلات التي تعمل بالمايكروويف.

E.V.6. إدارة ثغرات الأمن الرقمي واختبار الاختراق الخاصة بخدمات الاتصال

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. تقييم الثغرات الأمنية واختبار الاختراق وتصنيف ومعالجة الثغرات للأصول والنظم المعلوماتية الخاصة بخدمات الاتصال بشكل دوري.

E.V.7. التسجيل والمراقبة الخاصة بخدمات الاتصال

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. التأكد من تسجيل ومراقبة جميع الأنشطة المتعلقة بالنظم المعلوماتية الخاصة بخدمات الاتصال.

نصوص السياسة لمزودي الخدمة

E.V.8. حماية البيانات والمعلومات الخاصة بخدمات الاتصال

يجب على مزودي الخدمات:

1. التأكد من أن الاتفاقيات ونماذج الثقة بين الأطراف المعنية تشمل منهجية تحمي وتحافظ على الخصوصية كجزء من تصميمها.

E.V.9. التدريب والتوعية بالأمن الرقمي الخاص بخدمات الاتصال

يجب على مزودي الخدمات:

1. تنظيم حملات توعية لتثقيف المشتركين حول الاستخدام الآمن لخدمات الاتصال.

F.VI مبدأ سياسة الأمن الرقمي الخاصة بخدمات الحوسبة السحابية

توفر سياسة الأمن الرقمي الخاصة بخدمات الحوسبة السحابية الحد الأدنى من متطلبات الأمن الرقمي للشركات المقدمة لخدمات الحوسبة السحابية، وتحدد السياسة التهديدات والمخاطر التقنية والضمانات الخاصة بالبيئات السحابية. تتناول سياسة الأمن الرقمي الخاصة بخدمات الحوسبة السحابية مناطق تأمين الوصول إلى برامج مراقبة الأجهزة الافتراضية (hypervisors) والأجهزة الافتراضية (virtual machines) والواجهة الوسيطة للتطبيقات (APIs) .

F.VI.1	متطلبات الأمن الرقمي الخاصة بخدمات الحوسبة السحابية
الحوسبة السحابية: البنية التحتية النشطة	
F.VI.2	إدارة الأصول الخاصة بخدمات الحوسبة السحابية
F.VI.3	إدارة هويات الدخول والصلاحيات الخاصة بخدمات الحوسبة السحابية
F.VI.4	إدارة أمن البيانات الرقمية الخاصة بخدمات الحوسبة السحابية
F.VI.5	إدارة ثغرات الأمن الرقمي واختبار الاختراق الخاصة بخدمات الحوسبة السحابية
F.VI.6	إدارة أمن الشبكات الخاصة بخدمات الحوسبة السحابية
F.VI.7	إدارة الإعدادات الأمنه الخاصة بخدمات الحوسبة السحابية
F.VI.8	إدارة استمرارية الأعمال الخاصة بخدمات الحوسبة السحابية
F.VI.9	أمن إدارة التغيير الخاصة بخدمات الحوسبة السحابية
F.VI.10	إدارة حوادث الأمن الرقمي الخاصة بخدمات الحوسبة السحابية
الحوسبة السحابية: مزودو الخدمة	
F.VI.11	حماية البيانات والمعلومات الخاصة بخدمات الحوسبة السحابية
F.VI.12	التدريب والتوعية بالأمن الرقمي الخاص بخدمات الحوسبة السحابية

الجدول 8: نطاقات سياسة الأمن الرقمي الخاصة بخدمات الحوسبة السحابية

نصوص نطاق سياسة الأمن الرقمي الخاصة بخدمات الحوسبة السحابية

F.VI.1. متطلبات الأمن الرقمي الخاصة بخدمات الحوسبة السحابية

1. يجب إعداد متطلبات الأمن الرقمي الخاصة بخدمات الحوسبة السحابية وتوثيقها واعتمادها وتنفيذها.
2. يجب مراجعة متطلبات الأمن الرقمي الخاصة بخدمات الحوسبة السحابية بشكلٍ دوري أو عند إجراء تغييرات للمواءمة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

نصوص السياسة الخاصة بالبنية التحتية النشطة

F.VI.2. إدارة الأصول الخاصة بخدمات الحوسبة السحابية

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. الإعداد والاحتفاظ بسجل أصول يحوي تفاصيل الأصول والنظم المعلوماتية المستخدمة أو التي يملكها أو يديرها عملاء أو مستأجرين لخدمات الحوسبة السحابية.
2. التأكد من تطبيق متطلبات تصنيف البيانات للبيئات الافتراضية متوائمة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

F.VI.3. إدارة هويات الدخول والصلاحيات الخاصة بخدمات الحوسبة السحابية

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. توفير الوصول المقيد عبر مصادقة الهوية متعددة العناصر (Multi-Factor Authentication) إلى وظائف برامج مراقبة الأجهزة الافتراضية (hypervisors) ووحدات التحكم الإدارية للأنظمة التي تستضيف الأنظمة الافتراضية.
2. تنشيط ومراقبة سجلات الوصول إلى الواجهة الوسيطة للتطبيقات (APIs) والاحتفاظ بها بما يتوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.
3. تنشيط ومراقبة سجلات الوصول الى وحدات التخزين والاحتفاظ بها بما يتوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

F.VI.4. إدارة أمن البيانات الرقمية الخاصة بخدمات الحوسبة السحابية

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. التأكد من وجود آليات التشفير لتأمين البيانات في البنية التحتية كخدمة (IaaS).

2. التأكد من وجود آليات التشفير لتأمين التطبيقات في نظام المنصة كخدمة (PaaS) .
3. التأكد من وجود آليات التشفير لتأمين قاعدة البيانات في نظام المنصة كخدمة (PaaS).
4. تطبيق آليات التشفير المناسبة للبيانات قبل إرسالها إلى نظام منصة البرمجيات كخدمة (SaaS).

F.VI.5. إدارة ثغرات الأمن الرقمي واختبار الاختراق الخاصة بخدمات الحوسبة السحابية

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. تقييم الثغرات الأمنية واختبار الاختراق وتصنيف ومعالجة الثغرات للأصول والنظم المعلوماتية الخاصة بخدمات الحوسبة السحابية بشكل دوري.

F.VI.6. إدارة أمن الشبكات الخاصة بخدمات الحوسبة السحابية

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. حماية بيانات ومعلومات الشبكات الخاصة بخدمات الحوسبة السحابية من خلال تطبيق التشفير بما يتوافق مع التشريعات والتنظيمات ذات العلاقة.
2. مراقبة الشبكات الخاصة بخدمات الحوسبة السحابية وتقييد تدفق البيانات بين الشبكات الموثوقة وغير الموثوق بها.

F.VI.7. إدارة الإعدادات الآمنه الخاصة بخدمات الحوسبة السحابية

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. التأكد من حماية وتحصين الإعدادات الأساسية للأصول والنظم المعلوماتية الافتراضية.
2. تحصين أنظمة الأجهزة الافتراضية من خلال إعداد واستخدام خط أساس أمني للإعدادات.

F.VI.8. إدارة استمرارية الأعمال الخاصة بخدمات الحوسبة السحابية

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. إعداد وتطبيق آليات للتأكد من توفر خدمات الحوسبة السحابية للعملاء وعدم إنقطاعها.

F.VI.9. أمن إدارة التغيير الخاصة بخدمات الحوسبة السحابية

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. إعداد منهجية إدارة التغييرات للعملاء.
2. إعداد منهجية إدارة التغييرات لتصاميم الواجهة الوسيطة للتطبيقات (API).
3. إعداد منهجية إدارة التغييرات لشبكة البنية التحتية لخدمات الحوسبة السحابية.

F.VI.10. إدارة حوادث الأمن الرقمي الخاصة بخدمات الحوسبة السحابية

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. التأكد من وجود آليات تمكن المستخدمين من الإبلاغ عن حوادث أمنية رقمية وأتمتتها.
2. التأكد من أن اتفاقية مستوى الخدمة مع كل عميل تضمن دعمًا لحل حوادث الأمن الرقمي.

نصوص السياسة لمزودي الخدمة

F.VI.11. حماية البيانات والمعلومات الخاصة بخدمات الحوسبة السحابية

يجب على مزودي الخدمات:

1. التأكد من حماية البيانات والمعلومات الخاصة بخدمات الحوسبة السحابية بما يتواءم مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

F.VI.12. التدريب والتوعية بالأمن الرقمي الخاص بخدمات الحوسبة السحابية

يجب على مزودي الخدمات:

1. القيام بحملات توعية لتثقيف المستخدمين حول الاستخدام الآمن لخدمات الحوسبة السحابية.

G.VII مبدأ سياسة الأمن الرقمي الخاصة بخدمات التقنيات الناشئة

توفر سياسة الأمن الرقمي الخاصة بخدمات التقنيات الناشئة الحد الأدنى من متطلبات الأمن الرقمي للشركات المقدمة لخدمات التقنيات الناشئة، كما توفر السياسة تدابير لإدارة الأمن عبر البيانات والشبكات وإعداد التطبيقات المتعلقة بحلول التقنيات الناشئة فضلًا عن خصوصية البيانات.

G.VII.1	متطلبات الأمن الرقمي الخاصة بخدمات التقنيات الناشئة
التقنيات الناشئة: البنية التحتية النشطة	
G.VII.2	إدارة هويات الدخول والصلاحيات الخاصة بخدمات التقنيات الناشئة
G.VII.3	إدارة أمن البيانات الخاصة بخدمات التقنيات الناشئة
G.VII.4	إدارة أمن الشبكات الخاصة بخدمات التقنيات الناشئة
التقنيات الناشئة: مطورو البرامج والتطبيقات	
G.VII.5	أمن التطبيقات الخاصة بالتقنيات الناشئة
التقنيات الناشئة: مزودو الخدمة	
G.VII.6	حماية البيانات والمعلومات الخاصة بخدمات التقنيات الناشئة
G.VII.7	التدريب والتوعية بالأمن الرقمي الخاص بخدمات التقنيات الناشئة

الجدول 9: نطاقات سياسة الأمن الرقمي الخاصة بخدمات التقنيات الناشئة

نصوص نطاق سياسة الأمن الرقمي الخاصة بخدمات التقنيات الناشئة

G.VII.1. متطلبات الأمن الرقمي الخاصة بخدمات التقنيات الناشئة

1. يجب إعداد متطلبات الأمن الرقمي لخدمات التقنيات الناشئة وتوثيقها واعتمادها وتنفيذها.
2. يجب مراجعة متطلبات الأمن الرقمي لخدمات التقنيات الناشئة بشكلٍ دوري أو عند إجراء تغييرات للمواءمة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

نصوص السياسة الخاصة بالبنية التحتية النشطة

G.VII.2. إدارة هويات الدخول والصلاحيات الخاصة بخدمات التقنيات الناشئة

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. إصدار معرفات للمستخدمين لاستخدامها في عمليات المصادقة وإعطاء الصلاحيات.
2. التأكد من تحديد أدوار وصلاحيات المستخدم بشكل صحيح في البيئات المتعددة.
3. التأكد من توفير خيار تغيير اسم المستخدم وكلمة المرور الافتراضيين للمستخدم.

G.VII.3. إدارة أمن البيانات الخاصة بخدمات التقنيات الناشئة

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. التأكد من حماية البيانات الخاصة بخدمات التقنيات الناشئة بما يتواءم مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

G.VII.4. إدارة أمن الشبكات الخاصة بخدمات التقنيات الناشئة

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. التأكد من تحديد منافذ وخدمات تواصل الشبكات الخاصة لخدمات التقنيات الناشئة بالإنترنت للحد الأدنى المطلوب لإتمام العمل.
2. تقييم الثغرات الأمنية واختبار الاختراق وتصنيف ومعالجة الثغرات للأصول والنظم المعلوماتية الخاصة بخدمات التقنيات الناشئة بشكل دوري.

نصوص السياسة الخاصة بمطوري البرامج والتطبيقات

G.VII.5. أمن التطبيقات الخاصة بالتقنيات الناشئة

يجب على المطورين:

1. التأكد من تطوير الكود المصدري لأجهزة التقنيات الناشئة بطريقة آمنة ومحمية.
2. حماية مجموعات البيانات المستخدمة لتدريب نماذج الذكاء الاصطناعي بما يتواءم مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

نصوص السياسة لمزودي الخدمة

G.VII.6. حماية البيانات والمعلومات الخاصة بخدمات التقنيات الناشئة

يجب على مزودي خدمات وحلول التقنيات الناشئة:

1. التأكد من جمع الحد الأدنى من المعلومات الشخصية اللازمة من العملاء.
2. التأكد من حماية البيانات الخاصة بخدمات التقنيات الناشئة بما يتواءم مع المتطلبات التشريعية والتنظيمية ذات العلاقة.
3. التأكد من وصول الأفراد المصرح لهم فقط إلى المعلومات الشخصية الخاصة بالعملاء.
4. التأكد من تطوير وتطبيق سياسة الاحتفاظ بالبيانات والمعلومات الخاصة بخدمات التقنيات الناشئة بما يتواءم مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

G.VII.7. التدريب والتوعية بالأمن الرقمي الخاص بخدمات التقنيات الناشئة

يجب على مزودي الخدمات:

1. القيام بحملات توعية لتثقيف المستخدمين حول الاستخدام الآمن لخدمات التقنيات الناشئة.

H.VIII مبدأ سياسة الأمن الرقمي الخاصة بالخدمات المدارة

توفر سياسة الأمن الرقمي الخاصة بالخدمات المدارة الحد الأدنى من متطلبات الأمن الرقمي للشركات المقدمة للخدمات المدارة. توفر السياسة تدابير لإدارة وصول الشركات إلى الخدمات المدارة وتأمين شبكاتها.

H.VIII.1	متطلبات الأمن الرقمي الخاصة بالخدمات المدارة
الخدمة المدارة: البنية التحتية النشطة	
H.VIII.2	إدارة أمن الأطراف الخارجية الخاص بالخدمات المدارة
H.VIII.3	إدارة هويات الدخول والصلاحيات الخاصة بالخدمات المدارة
H.VIII.4	إدارة أمن الشبكات الخاصة بالخدمات المدارة
H.VIII.5	إدارة ثغرات الأمن الرقمي واختبار الاختراق الخاصة بالخدمات المدارة
H.VIII.6	أمن تطبيقات الأجهزة المحمولة الخاصة بالخدمات المدارة
الخدمة المدارة: مطورو البرامج والتطبيقات	
H.VIII.7	أمن التطبيقات الخاصة بالخدمات المدارة
الخدمة المدارة: مزودو الخدمة	
H.VIII.8	حماية البيانات والمعلومات الخاصة بالخدمات المدارة

الجدول 10: نطاقات سياسة الأمن الرقمي الخاصة بالخدمات المدارة

نصوص نطاق سياسة الأمن الرقمي الخاصة بالخدمات المدارة

H.VIII.1. متطلبات الأمن الرقمي الخاصة بالخدمات المدارة

1. يجب إعداد متطلبات الأمن الرقمي للخدمات المدارة الخاصة وتوثيقها واعتمادها وتنفيذها.
2. يجب مراجعة متطلبات الأمن الرقمي للخدمات المدارة بشكلٍ دوري أو عند إجراء تغييرات للمواءمة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

نصوص السياسة الخاصة بالبنية التحتية النشطة

H.VIII.2. إدارة أمن الأطراف الخارجية الخاص بالخدمات المدارة

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. التأكد من تطوير وتطبيق اتفاقيات الإستخدام الآمن للخدمات المدارة مع الأطراف ذا العلاقة.

H.VIII.3. إدارة هويات الدخول والصلاحيات الخاصة بالخدمات المدارة

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. التأكد من إعدادات الوصول إلى وحدة إدارة التحكم للنظم المعلوماتية يتم عبر مصادقة الهوية متعددة العناصر (Multi-Factor Authentication).
2. التأكد من أن الوصول إلى النظم المعلوماتية الخاصة بالخدمات المدارة للعملاء يتم منحه بشكل مؤقت عندما يرتبط بطلب خدمة محدد ومعتمد.

H.VIII.4. إدارة أمن الشبكات الخاص بالخدمات المدارة

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. التأكد من فصل شبكات النظم المعلوماتية الخاصة بالخدمات المدارة عن شبكات النظم المعلوماتية الخاصة بالشركة.
2. السماح فقط بالاتصال الشبكي المعتمد والآمن مع النظم المعلوماتية للعملاء.

H.VIII.5. إدارة ثغرات الأمن الرقمي الخاصة بالخدمات المدارة

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. تقييم الثغرات الأمنية واختبار الاختراق وتصنيف ومعالجة الثغرات للأصول والنظم المعلوماتية الخاصة بالخدمات المدارة بشكل دوري.
2. إجراء تقييمات ثغرات الأمن الرقمي للنظم المعلوماتية التي ستتم إدارتها في مقرات العملاء بعد الحصول على الإذن منهم.
3. معالجة ثغرات الأمن الرقمي في بيئة اختبار قبل البدء بتطبيقها في بيئة الإنتاج الخاصة بالعملاء وبالتنسيق معهم.

H.VIII.6. أمن تطبيقات الأجهزة المحمولة الخاصة بالخدمات المدارة

يجب على الشركات المقدمة لخدمات البنية التحتية النشطة:

1. حماية التطبيق من تقنيات الهندسة العكسية.
2. التأكد من تفعيل الحماية الذاتية وقت تشغيل التطبيق (Runtime Application Self-Protection) وإجراءات الإصلاح الذاتي.
3. التأكد من حماية معلومات المستخدمين عند استخدام تطبيقات الأجهزة المحمولة.
4. التأكد من فحص منصات إدارة تطبيقات النظم المعلوماتية لتحديد التهديدات الأمنية المحتملة.
5. توفير آلية تمكن المستخدمين من التحكم في بياناتهم والوصول إليها بطريقة آمنة.
6. توفير آلية تنبه المستخدمين بوجود نشاط غير اعتيادي على التطبيق.

نصوص السياسة الخاصة بمطوري البرامج والتطبيقات

H.VIII.7. أمن التطبيقات الخاصة بالخدمات المدارة

يجب على المطورين:

1. التأكد من تطوير الكود المصدري للتطبيقات الخاصة بالخدمات المدارة بطريقة آمنة ومحمية.
2. حماية البيانات والمعلومات المستخدمة للتطبيقات الخاصة بالخدمات المدارة بما يتواءم مع المتطلبات التشريعية والتنظيمية ذات العلاقة.
3. تقييم الثغرات الأمنية واختبار الاختراق وتصنيف ومعالجة الثغرات للتطبيقات الخاصة بالخدمات المدارة بشكل دوري.
4. التأكد من فصل بيئة الإنتاج عن بيئات التطوير والاختبار.

نصوص السياسة لمزودي الخدمة

H.VIII.8. خصوصية البيانات الخاصة بالخدمات المدارة

يجب على مزودي الخدمات:

1. التأكد من أن الاتفاقيات ونماذج الثقة بين الأطراف المعنية تشمل منهجية تحمي وتحافظ على الخصوصية كجزء من تصميمها.

ملحق (أ)

يحدد هذا الجدول السياسة الأساسية والضوابط الأساسية للأمن السيبراني التابعة للهيئة الوطنية للأمن السيبراني (NCA-ECC) ومعايير منظمة المعايير الدولية (الأيزو 27001 إدارة أمن المعلومات).

الجدول أ-1: مطابقة السياسة الأساسية مع الضوابط والمعايير العالمية

السياسات الأساسية للأمن الرقمي لقطاع خدمات الاتصالات وتقنية المعلومات	الضوابط الأساسية للأمن السيبراني التابعة للهيئة الوطنية للأمن السيبراني (NCA –ECC)	معايير منظمة المعايير الدولية (الأيزو 27001 إدارة أمن المعلومات)
حوكمة الأمن الرقمي	1-1, 1-2,1-3,4-1	A.5.1, A.5.1.1 – A.5.1.2,A.6.1, A.6.1.1
إدارة مخاطر الأمن الرقمي	1-5	8.2,8.3
الأمن الرقمي في إدارة التغيير	1-6	أ-12-1-2
الأمن الرقمي ضمن إدارة مشاريع الأصول المعلوماتية		A.14, A.14.1, A.14.2, A.6.1.5, A.12.1.3
الامن الرقمي ضمن إدارة مشاريع النظم المعلوماتية		
إدارة الإلتزام بتشريعات الأمن الرقمي	1-7, 1-8	أ-18، أ-18-1، أ-18-2
الأمن الرقمي المتعلق بالموارد البشرية	1-9	A.7,A.7.1, 7.2, 7.3
التوعية والتدريب بالأمن الرقمي	1-10	7.3
إدارة الأصول	2-1	A.8.1.1, A.8.1.2, A.8.3.2, A.10.1.2
إدارة هويات الدخول والصلاحيات	2-2	A.9, A.9.1 – A.9.4, A.9.2.5
أمن النظم المعلوماتية ومرافق معالجة المعلومات	2-3	7.3
الأمن الرقمي للبريد الإلكتروني	2-4	أ-13-2-3
إدارة أمن الشبكات	2-5	A.13, A.13.1
أمن الأجهزة المحمولة	2-6	A.6.2, A.8.3.1
حماية البيانات والمعلومات	2-7	
التشفير	2-8	A.10, A.10.1.2, A.12.2
إدارة النسخ الاحتياطية والاستعادة	2-9	أ-12-3
إدارة ثغرات الأمن الرقمي واختبار الاختراق	2-10, 2-11	أ-12-6
إدارة سجلات الأحداث ومراقبة الأمن الرقمي	2-12	A.12.4, A.12.4.1 – A.12.4.4
إدارة تهديدات وحوادث الأمن الرقمي	2-13	أ-16
الأمن المادي	2-14	أ-11، أ-11-1، أ-11-4-1
أمن التطبيقات للويب والأجهزة الذكية	2-15	
إدارة استمرارية الأعمال	3-1	أ-17
إدارة الأمن الرقمي المتعلق بالأطراف الخارجية	4-1	A.15, A.15.2.1

راجع الرابط

يحدد هذا الجدول السياسة الأساسية ونطاقات الضوابط الأساسية للأمن السيبراني التابعة للهيئة الوطنية للأمن السيبراني-NCA) ECC) ومعايير منظمة المعايير الدولية (27001 إدارة أمن المعلومات).

الجدول أ-2: مطابقة نطاق السياسة الأساسية مع الضوابط والمعايير العالمية

الضوابط الأساسية للأمن السيبراني التابعة للهيئة الوطنية للأمن السيبراني	السياسات الأساسية للأمن الرقمي لقطاع خدمات الاتصالات وتقنية المعلومات(NCA-ECC)	معايير منظمة المعايير الدولية (الأيزو)ISO 27001
حوكمة الأمن السيبراني	حوكمة الأمن الرقمي	A.6 تنظيم أمن المعلومات، A.5 سياسات أمن المعلومات البند 8 -عمليات التشغيل A.18 الالتزام A.14 الحصول على النظام وتطويره وصيانته A.7 أمن الموارد البشرية
	إدارة مخاطر الأمن الرقمي	
	الأمن الرقمي في إدارة التغيير	
	الأمن الرقمي ضمن إدارة مشاريع الأصول المعلوماتية	
	الامن الرقمي ضمن إدارة مشاريع النظم المعلوماتية	
	إدارة الالتزام بتشريعات الأمن الرقمي	
	الأمن الرقمي المتعلق بالموارد البشرية	
	التوعية والتدريب بالأمن الرقمي	
تعزيز الأمن السيبراني	إدارة الأصول	A.8 إدارة الأصول A.9 التحكم بالوصول A.10 التشفير A.12 الأمن التشغيلي A.6.2 عمل الأجهزة المحمولة عن بُعد A.13 أمن خدمات الاتصالات A.11 الأمن المادي والبيئي A.16 إدارة حوادث أمن المعلومات A.12.3 النسخ الاحتياطي A.12.4 التسجيل والمراقبة A.14 الحصول على النظام وتطويره وصيانته A.14.2.2 إجراءات التحكم في تغيير النظام
	إدارة هويات الدخول والصلاحيات	
	أمن النظم المعلوماتية ومرافق معالجة المعلومات	
	الأمن الرقمي للبريد الإلكتروني	
	إدارة أمن الشبكات	
	أمن الأجهزة المحمولة	
	حماية البيانات والمعلومات	
	التشفير	
	إدارة النسخ الاحتياطية والاستعادة	
	إدارة ثغرات الأمن الرقمي واختبار الاختراق	
	إدارة سجلات الأحداث ومراقبة الأمن الرقمي	
	إدارة تهديدات وحوادث الأمن الرقمي	
	الأمن المادي	
	أمن التطبيقات للويب والأجهزة الذكية	
صمود الأمن السيبراني	إدارة استمرارية الأعمال	A.17 جوانب أمن المعلومات لإدارة استمرارية العمل
الأمن السيبراني التابع للأطراف الخارجية والحوسبة السحابية	إدارة الأمن الرقمي المتعلق بالأطراف الخارجية	A.15 علاقات الموردين

راجع الرابط

ملحق (ب)

يحدد هذا الجدول السياسات الخاصة بالأمن الرقمي لقطاع خدمات الاتصالات وتقنية المعلومات مقابل المعايير الدولية وأفضل الممارسات.

الجدول ب-1: مطابقة نطاق السياسات الخاصة مع الضوابط والمعايير العالمية

سياسات الخدمات الخاصة بقطاع خدمات الاتصالات وتقنية المعلومات	المعايير		
سياسة الخدمات الصوتية	GSMA	ITU-T SG 17	
سياسة الرسائل القصيرة	GSMA	3GPP	
سياسة خدمات الإنترنت	ISO 27011	3GPP	GSMA
سياسة خدمات الاتصال	GSMA	ITU-T SG 17	
سياسة الحوسبة السحابية	Cloud Security Alliance		
سياسة التقنيات الناشئة	GSMA – IOT Security Guidelines	3GPP	OWASP – IOT Security Guidelines
سياسة الخدمات المدارة	ISO 27011	ITU-T SG 17	SANS – Practical Security Considerations for Managed Service Provider On-Premise Equipment

راجع الرابط

ملحق (ج)

ج-1 الاختصارات

الجدول ج-1: الاختصارات والتعريفات

الاختصار	التعريف
3GPP	مشروع شراكة الجيل الثالث
AI	الذكاء الصناعي
API	الواجهة الوسيطة للتطبيقات
Apps	تطبيقات
BYOD	استخدم جهازك الشخصي
CITC	هيئة الاتصالات وتقنية المعلومات
CRF	إطار تنظيم الأمن السيبراني
DNS	نظام أسماء النطاقات
DoS	الحرمان من الخدمة
DS	الأمن الرقمي
GDPR	اللائحة العامة لحماية البيانات
GSMA	المنظمة الدولية لقطاع الاتصالات المتنقلة
GTP	بروتوكول الاتصال النفقي اللاسلكي العام
IaaS	البنية التحتية كخدمة
ICT	الاتصالات وتقنية المعلومات
IMEI	الهوية الدولية للأجهزة المحمولة
IMSI	الهوية الدولية لمشترك الجوال
IOT	إنترنت الأشياء
IP	بروتوكول الإنترنت
ISO	المنظمة الدولية للمعايير
ITU-T	الاتحاد الدولي للاتصالات
KSA	المملكة العربية السعودية
LBS	خدمة تحديد المواقع
MAP	جزء تطبيقات الأجهزة المحمولة
MCIT	وزارة الاتصالات وتقنية المعلومات
MSISDN	رقم دليل المشترك الدولي في محطات الهواتف المحمولة
MSP	مزودو الخدمات المدارة
NCA	الهيئة الوطنية للأمن السيبراني
NCDC	المركز الوطني للتصديق الرقمي
NIST	المعايير الصادرة عن المعهد الوطني الأمريكي للمعايير والتقنية

الاختصار	التعريف
NTP	برنامج التحول الوطني
OWASP	مشروع أمن تطبيق الويب المفتوح
PaaS	منصة كخدمة
PBX	تبادل الفروع الخاصة
PII	معلومات التعرف الشخصية
PKI	البنية التحتية للمفاتيح العامة
PMI	البنية التحتية لإدارة الصلاحيات
RASP	حماية ذاتية وقت تشغيل التطبيق
SaaS	البرمجيات كخدمة
SBC	التحكم في بث الجلسات
SMS	خدمة الرسائل القصيرة
SPIT	البريد غير المرغوب فيه عبر الإنترنت
SS7	نظام الإشارات 7
URL	محدد موقع الموارد المُوحّد
VOIP	بروتوكول الصوت عبر الإنترنت
VSAT	محطة ذات فجوة متناهية الصغر

ج-2 المصطلحات

الجدول ج-2: مصطلحات وتفاصيل

المصطلحات	الوصف
إدارة صلاحيات الدخول	إدارة صلاحيات الدخول هي عملية منح المستخدمين المصرح لهم الحق في استخدام الخدمة مع منع دخول المستخدمين غير المصرح لهم، ويتمثل الغرض من إدارة صلاحيات الدخول في توفير الحق للمستخدمين لتمكين استخدام خدمة أو مجموعة من الخدمات.
الأصل	أي شيء ملموس أو غير ملموس له قيمة لدى الشركة، وتوجد أنواع كثيرة من الأصول؛ بعض هذه الأصول تتضمن أشياء واضحة مثل: الأشخاص والآلات والمرافق وبراءات الاختراع والبرمجيات والخدمات، ويمكن أن يشمل المصطلح أيضًا أشياء أقل وضوحًا مثل: المعلومات والخصائص (مثل: سمعة الشركة وصورتها العامة بجانب المهارة والمعرفة).
هجوم	أي نوع من الأنشطة الخبيثة التي تحاول الوصول بشكل غير مشروع أو جمع موارد النظم المعلوماتية أو المعلومات نفسها أو تعطيلها أو منعها أو تحطيمها أو تدميرها.
تدقيق	المراجعة المستقلة ودراسة السجلات والأنشطة لتقييم مدى فعالية ضوابط الأمن السيبراني ولضمان الالتزام بالسياسات والإجراءات التشغيلية والمعايير والمتطلبات التشريعية والتنظيمية ذات العلاقة.
واقع معزز	الواقع المعزز تركيب أو تداخل الأجسام الافتراضية في بيئة العالم الحقيقي، وفي الواقع المعزز يرى المستخدمون ويتفاعلون مع العالم الحقيقي بينما يتم إضافة المحتوى الرقمي إليه.
التحقق	التأكد من هوية المستخدم أو العملية أو الجهاز، وغالبًا ما يكون هذا الأمر شرطًا أساسيًا للسماح بالوصول إلى الموارد في النظام.
صلاحية المستخدم	خاصية تحديد والتأكد من حقوق/صلاحيات المستخدم للوصول إلى لموارد والأصول والنظم المعلوماتية للشركة والسماح له وفقًا لما حدد مسبقًا في حقوق/صلاحيات المستخدم.
توافر	ضمان الوصول إلى البيانات والمعلومات والأنظمة والتطبيقات واستخدامها في الوقت المناسب.
نسخ احتياطي	ملفات وأجهزة وبيانات وإجراءات متوفرة للاستخدام في حالة الأعطال أو الفقدان، أو في حالة مسح النسخ الأصلية أو تعطلها.
تقنية "البلوك تشين"	تقنية "البلوك تشين" هي قائمة متنامية من السجلات تسمى بالكتل التي يتم ربطها باستخدام التشفير، وهي عبارة عن سجل حسابات مفتوح وموزع يمكنه تسجيل المعاملات بين الطرفين بكفاءة وبطريقة آمنة ويمكن التحقق منها.

المصطلحات	الوصف
إدارة التغيير	نظام لإدارة الخدمة حيث يضمن منهجية نظاميًا واستباقيًا باستخدام أساليب وإجراءات معيارية فعالة (على سبيل المثال: التغيير في البنية التحتية للشركة وشبكاتها). تساعد إدارة التغيير جميع الأطراف المعنيين، بما في ذلك الأفراد والفرق على حدٍ سواء، على الانتقال من حالتهم الحالية إلى الحالة التالية المرغوب فيها، كما تساعد إدارة التغيير على تقليل تأثير الحوادث ذات الصلة على الخدمة.
الحوسبة السحابية	نموذج لتمكين الوصول إلى الشبكة عند الطلب لمجموعة مشتركة من قدرات/ موارد تقنية المعلومات (مثل: الشبكات والخوادم والتخزين والتطبيقات والخدمات) التي يمكن توفيرها بسرعة وإطلاقها بالحد الأدنى من الجهد الإداري التشغيلي أو التفاعل من مزود الخدمة، وتسمح الحوسبة السحابية للمستخدمين بالوصول إلى الخدمات القائمة على التقنية من خلال شبكة الحوسبة السحابية دون الحاجة إلى وجود معرفة لديهم أو خبرة أو تحكم في البنية التحتية التقنية التي تدعمهم، ويتألف نموذج الحوسبة السحابية من خمس خصائص أساسية: خدمة ذاتية حسب الطلب ووصول إلى الشبكة على نطاق واسع ومجمع الموارد المستقلة للموقع والمرونة السريعة والخدمة المقاسة، وهناك ثلاثة أنواع من نماذج تقديم خدمات الحوسبة السحابية وهي: البرمجيات كخدمة والمنصة كخدمة والبنية التحتية كخدمة؛ بناءً على وصول الشركة للحوسبة السحابية، وهناك أربعة نماذج: الحوسبة السحابية الخاصة والحوسبة السحابية المجتمعية والحوسبة السحابية العامة والحوسبة السحابية الهجينة.
المعلومات/ البيانات السرية	هي المعلومات (أو البيانات) المؤسسية التي تعتبر غاية في الحساسية والأهمية، حسب تصنيف الشركة والتي يتم إعدادها للاستخدام من قِبل الشركة نفسها أو شركات معينة أخرى، وإحدى الطرق التي يمكن استخدامها في تصنيف هذا النوع من المعلومات/ البيانات هو تقييم التأثير الناتج عن الإفصاح عنها أو الوصول إليها بشكلٍ غير مصرح به أو فقدها أو تلفها، وقد تكون التأثيرات مادية أو متعلقة بسمعة الشركة أو العملاء، التأثير على حياة الأشخاص المرتبطين بتلك المعلومات التي تم الإفصاح عنها، التأثير والضرر بالأمن أو الاقتصاد أو القدرات الوطنية، وتشمل البيانات/ المعلومات السرية كل المعلومات التي يترتب على الإفصاح عنها أو فقدها أو تلفها بشكلٍ غير مصرح به عواقب قانونية.
السرية	الاحتفاظ بقيود مصرح بها على الوصول إلى المعلومات والإفصاح عنها، بما في ذلك وسائل حماية معلومات الخصوصية/ المعلومات الشخصية.
البنية التحتية الوطنية الحساسة	هذه هي الأصول (أي المرافق والأنظمة والشبكات والعمليات والمشغلون الرئيسيون الذين يقومون بتشغيلها ومعالجتها)، التي قد يؤدي فقدانها أو تعرضها لاختراقات أمنية إلى: • تأثير سلبي كبير على توافر الخدمات الأساسية أو تكاملها أو تقديمها، بما في ذلك الخدمات التي يمكن أن تؤدي في حال تعرضت سلامتها للخطر إلى خسائر كبيرة في الممتلكات و/أو الأرواح و/أو الإصابات، مع مراعاة التأثيرات الاقتصادية و/أو الاجتماعية الكبيرة. • تأثير كبير على الأمن القومي و/أو الدفاع الوطني و/أو اقتصاد الدولة أو مقدراتها الوطنية.
التشفير	هذه هي القواعد التي تتضمن مبادئ وطرق ووسائل تخزين البيانات أو المعلومات ونقلها في شكل معين من أجل إخفاء محتواها الدلالي أو منع الاستخدام غير المصرح به أو منع التعديل غير المكتشف حتى يتمكن فقط الأشخاص المعنيون من قراءة ذلك ومعالجته.
التنمر السيبراني	يشير التنمر السيبراني إلى المعاملة السلبية والمدمرة التي يفرضها فرد على فرد آخر بطريقة تؤدي إلى معاناة الهدف وشعوره بالإهانة أو الضعف.
الاستدراج السيبراني	يشير الاستدراج السيبراني إلى حث أو إقناع يفرضه فرد على فرد آخر بطريقة تجعل الضحية يشعر بالراحة للتفاعل مع الجاني ومقابلته سرًا.
تصنيف البيانات والمعلومات	تعيين مستوى الحساسية للبيانات والمعلومات التي ينتج عنها ضوابط أمنية لكل مستوى من مستويات التصنيف، ويتم تعيين مستويات حساسية البيانات والمعلومات وفقًا لفئات محددة مسبقًا حيث يتم إنشاء البيانات والمعلومات أو تعديلها أو تحسينها أو تخزينها أو نقلها. كما أن مستوى التصنيف هو مؤشر على قيمة أو أهمية البيانات والمعلومات للشركة.

المصطلحات	الوصف
طبقات العمق	مفهوم لضمان المعلومات يتم فيه وضع طبقات متعددة من الضوابط الأمنية (تعزيز) عبر نظام تقنية المعلومات أو تقنية التشغيل.
الأمن الرقمي	يشتمل الأمن الرقمي على مجموعة من الأدوات والسياسات ومفاهيم الأمن ووسائل الوقاية الأمنية والأدلة وأساليب إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات والضمانات والتقنيات التي يمكن استخدامها لحماية أصول المعلومات التابعة للشركة من التهديدات السيبرانية الداخلية والخارجية.
حجب الخدمة	الحرمان من الخدمة هو هجوم سيبراني حيث يحاول المخترقون حجب المستخدمين المقصودين من الوصول إلى جهاز أو مصدر الشبكة عن طريق إعاقة الخدمات من مضيف متصل بالإنترنت بشكلٍ مؤقت أو دائم.
التقنيات الناشئة	تتضمن التقنيات الناشئة أي تقنيات جديدة تؤدي إلى اضطرابات لعمليات الأعمال بشكل إيجابي و/أو تحسين الكفاءة و/أو إضافة قيمة للأعمال.
دورة حياة التوظيف	تتضمن دورة حياة التوظيف المراحل السابقة لمشاركة العاملين ومرحلة التوظيف وأي تغيير في الدور والتعيين وإنهاء المشاركة في التوظيف والفترة التي تلي التوظيف.
إدارة الاحتيال	تتعلق إدارة الاحتيال بحصر البيانات المتكاملة وتحليلها وإجراء التحقيقات لتحليل السلوك بين المستخدمين والمحاسبين والقنوات ذات الصلة والكيانات الأخرى، وذلك لتحديد السلوك غير الطبيعي الذي قد يكون مؤشرًا على نشاط غير قانوني مثل الفساد أو الاحتيال.
المخترق	المخترق هو شخص يستخدم كمبيوتر أو شبكة أو مهارات أخرى للتغلب على مشكلة تقنية، وقد يشير مصطلح المخترق إلى أي شخص لديه مهارات تقنية يستخدمها للحصول على دخول غير مصرح به إلى الأنظمة أو الشبكات لارتكاب أنشطة غير مشروعة لتحقيق مكاسب شخصية.
منتجات خدمات الاتصالات وتقنية المعلومات	تشمل منتجات الاتصالات وتقنية المعلومات السلع والخدمات التي تمكّن خدمات الاتصالات وتقنية المعلومات.
إدارة الهوية	وسائل التأكد من هوية المستخدم أو العملية أو الجهاز، وغالبًا ما يكون هذا الأمر شرطًا أساسيًا للسماح بالوصول إلى الموارد في النظام.
إدارة الحوادث	تحديد واكتشاف حوادث الأمن الرقمي في الوقت المناسب وإدارتها بشكل فعّال والتعامل مع تهديدات الأمن الرقمي بشكل استباقي من أجل منع أو تقليل الآثار المترتبة على أعمال الشركة.

المصطلحات	الوصف
الأصول المعلوماتية	البيانات والمعلومات التي يتم تنظيمها وإدارتها ككيان واحد وتكون ذات قيمة.
صحة المعلومات	الحماية ضد تعديل أو تخريب المعلومات بشكل غير مصرح به، وتتضمن ضمان عدم الإنكار للمعلومات والموثوقية.
النظم المعلوماتية	الأجهزة (المحمولة وغير المحمولة) والخوادم والبرامج والتطبيقات (الويب وتطبيقات الأجهزة الذكية) ومكونات اتصالات الشبكة ووحدات التخزين والمستخدمين.
إنترنت الأشياء	إنترنت الأشياء هو نظام من أجهزة الحوسبة المترابطة والآلات الميكانيكية والرقمية والأشياء أو الحيوانات أو الأشخاص التي يتم توفيرها بمعرّفات فريدة من نوعها والقدرة على نقل البيانات عبر شبكة دون الحاجة إلى تفاعل إنسان مع إنسان أو إنسان مع كمبيوتر.
اعرف عميلك	معرفة العميل، يشار إليها أيضًا باسم اعرف عمليك، هي العملية التي تستخدمها الشركة للتحقق من هوية عملائها. كما تُستخدم أيضًا لتقييم مدى ملاءمتها والمخاطر المحتملة للنوايا غير القانونية تجاه علاقة العمل.
أمن ذو طبقات	يتم تعريف أمن الطبقات كطريقة لإنشاء طبقات أمنية متعددة وتضمينها لمنع حدوث انتهاكات أمنية محتملة في عدة مراحل.
تكامل الوسائط	تشير الوسائط إلى الجهاز الذي لديه القدرة على تخزين البيانات التي يمكن أن تتأثر بالأعطال الكهروميكانيكية وعيوب التصميم وإرهاق المواد وانقطاع التيار الكهربائي والمخاطر المادية الأخرى، ويشير تكامل الوسائط إلى تخزين البيانات واستعادتها بشكلٍ صحيح من الوسائط التي تخزّن البيانات.
تطبيقات الأجهزة المحمولة	تطبيق الأجهزة المحمولة هو برنامج كمبيوتر أو تطبيق برمجي مصمم للعمل على جهاز محمول مثل الهاتف أو الكمبيوتر اللوحي أو الساعة.
السجل الوطني لحظر المكالمات	السجل الوطني لحظر المكالمات هو قاعدة بيانات توفر للفرد حرية اختيار تضمينه في الحملات التسويقية عبر الهاتف أو استبعاده منها.
معلومات التعرف الشخصية	معلومات التعريف الشخصي هي أي بيانات يمكن أن تحدد هوية فرد معين. تتضمن هذه المعلومات الحيوية والطبية والمالية الشخصية والمعرّفات الفريدة مثل جواز السفر أو أرقام الهوية.

المصطلحات	الوصف
العاملون	الأشخاص الذين يعملون في شركة كموظفين أو متعاقدين.
التصيد	التصيد هو نوع من التهديدات، ويستخدم المخترقون وغيرهم من الأفراد الضارين هذه التقنية لخداع المستخدمين الشرعيين وأصحاب البنية التحتية في نقل المعلومات، وعادةً يتم هذا النوع من المخادعة بمهارة لتظهر كما لو أن مصدر طلب المعلومات حقيقي والطلب نفسه اعتيادي.
الأمن المادي	يصف الأمن المادي التدابير الأمنية التي تم تصميمها لمنع الوصول غير المصرح به إلى المرافق والمعدات والموارد التابعة للشركة، وحماية الأفراد والممتلكات من الضرر أو الأذى (مثل التجسس أو السرقة أو الهجمات الإرهابية)، وينطوي الأمن المادي على استخدام طبقات متعددة من الأنظمة المترابطة، تشمل نظام الدوائر التلفزيونية المغلقة وحراس الأمن والحدود الأمنية والأقفال وأنظمة التحكم في الوصول والعديد من التقنيات الأخرى.
السياسة	وثيقة تحدد بنودها التزامًا عامًا أو توجيهًا أو نية لشركة ما كما تم التعبير عن ذلك رسميًا من قِبل المسؤول المُصرّح لها.
خصوصية حسب التصميم	التحرر من التدخل غير المصرح به أو الكشف عن المعلومات الشخصية بشأن أحد الأفراد.
مرافق معالجة المعلومات	المرافق التي تحتوي على أجهزة وخوادم معالجة المعلومات والبنى التحتية التقنية.
دورة حياة العلاقات	مرحلة ما قبل تنفيذ الاتفاقية ومرحلة تقديم الخدمة وإنهاء الاتفاقية وفترة ما بعد الإنهاء.
الحفاظ على الخصوصية	ممنهجية الحفاظ على الخصوصية هو تدبير الأمن الإلزامي لتوفير الأمن للبيانات التي يتم نقلها أو التواصل بين مختلف الأطراف.
تأمين الإعدادات والتحصين	حماية وتحصين وضبط إعدادات جهاز الحاسب الآلي، والنظام، والتطبيق، وجهاز الشبكة، والجهاز الأمني لمقاومة الهجمات السيبرانية. مثل: إيقاف أو تغيير الحسابات المصنعية والافتراضية، إيقاف الخدمات غير المستخدمة، إيقاف منافذ الشبكة غير المستخدمة.
وحدة التحكم في حدود الجلسة	وحدة التحكم في حدود الجلسة هي إحدى وظائف الشبكة التي تقوم بتأمين البنية التحتية للصوت عبر بروتوكول الإنترنت مع توفير التشغيل البيني بين رسائل إشارات غير متوافقة وتدفقات الوسائط (الجلسات) من الأجهزة الطرفية أو خوادم التطبيقات.

المصطلحات	الوصف
البيانات الحساسة	المعلومات الحساسة هي البيانات التي يجب حمايتها من الوصول غير المصرح به لحماية الخصوصية أو أمن فرد أو شركة، وتُصنف البيانات الحساسة كما يلي: — المعلومات الشخصية: المعلومات الحساسة للتعريف بالشخصية هي البيانات التي يمكن تتبعها مرةً أخرى إلى الفرد والتي، إذا تم الكشف عنها، قد تؤدي إلى حدوث ضرر لهذا الشخص. — معلومات العمل: تتضمن معلومات الأعمال الحساسة أي معلومات تشكل خطرًا على الشركة وقد تؤدي إلى خسارة في القيمة. — المعلومات المصنَّفة: تتضمن المعلومات المصنَّفة أي معلومات تتطلب التخليص بناءً على مستوى الحساسية وتتعلق عمومًا بالأمن الوطني، وينطبق هذا عادةً على الكيان الحكومي فقط.
سلسة الخدمات	تشير سلسلة الخدمة إلى المراحل التي يتم من خلالها إنتاج منتج الاتصالات وتقنية المعلومات وتسليمه للمستهلك.
الخداع الإلكتروني	الخداع الإلكتروني هو هجوم أمني يتم فيه خداع المستخدم عن طريق رسالة قصيرة في تنزيل برامج ضارة مباشرةً على جهاز محمول أو بشكلٍ غير مباشر على أجهزة محمولة أخرى.
الرسائل القصيرة	الرسائل القصيرة هي مكون خدمة مراسلة نصية لمعظم أنظمة الهاتف والإنترنت والأجهزة المحمولة، وتستخدم بروتوكولات الاتصال الموحدة لتمكين الأجهزة المحمولة من تبادل الرسائل النصية القصيرة.
الهندسة الاجتماعية	الهندسة الاجتماعية عبارة تصف هجوم ضار مصمم للاستفادة من مستخدمي الكمبيوتر عديمي الخبرة، وتقوم متشركات الهجوم بإنشاء مسار يمكّن المتطفلين من استغلال ثغرات النظام، بما في ذلك العنصر البشري، وتسعى طريقة التطفل هذه إلى خداع الأفراد في التفكير في طلب لخدمة أو معلومات أصلية.
الاقتحامية	الاقتحامية مصطلح يشير عادةً إلى الاتصالات الرقمية التطفلية أو غير المرغوب فيها، مثل الإعلانات، ويستخدم المتسللون الاقتحامية لارتكاب الجرائم السيبرانية وإرسال بيانات غير مرغوب فيها مصممة لإلحاق الضرر بأي نظام معلومات.
الاقتحامية عبر خدمات الاتصال الهاتفي بالإنترنت	تشير الاقتحامية عبر الاتصال الهاتفي بالإنترنت، والمعروفة أيضًا باسم، الرسائل الاقتحامية الصوتية عبر بروتوكول الإنترنت، إلى الرسائل الجماعية غير المرغوب فيها التي يتم بثها عبر بروتوكول الصوت عبر الإنترنت إلى الهواتف المتصلة بالإنترنت.
الأطراف الخارجية	أي شركة تعمل كطرف في علاقة تعاقدية لتوفير السلع أو الخدمات (ويشمل ذلك الموردين ومزودي الخدمات).
تهديد	أي ظرف أو حدث من المحتمل أن يؤثر سلبًا على أعمال الشركة (بما في ذلك مهمتها أو وظائفها أو مكانتها أو سمعتها) أو أصولها التنظيمية أو أفرادها مستغلًا أحد النظم المعلوماتية عن طريق الوصول غير المصرح به إلى المعلومات أو تدميرها أو كشفها أو تعديلها و/أو الحرمان من الخدمة، وأيضًا، قدرة مصدر التهديد على النجاح في استغلال إحدى الثغرات الخاصة بنظام معلومات معين.
سرقة المعلومات الشخصية المهمة	سرقة المعلومات الشخصية المهمة هو شكل من أشكال الاحتيال غير القانوني عبر الهاتف يطبق الهندسة الاجتماعية على نظام الاتصال الهاتفي للوصول إلى المعلومات الشخصية والمالية الخاصة بغرض نهائي يتمثل في الاحتيال المالي للأفراد.

المصطلحات	الوصف
الواقع الافتراضي	الواقع الافتراضي يغمر المستخدمين في بيئة رقمية مصطنعة تمامًا، وهذه التقنية تغمر المستخدمين في بيئة افتراضية بالكامل يتم إنشاؤها بواسطة جهاز كمبيوتر.
الثغرة	أي نوع من الضعف في نظام الكمبيوتر أو البرامج أو التطبيقات أو مجموعة من الإجراءات أو في أي شيء يجعل الأمن السيبراني عرضة للتهديد.

نهاية الوثيقة