UNITED ARAB EMIRATES
MINISTRY OF CABINET AFFAIRS
PRIME MINISTER'S OFFICE

الإمارات العربية المتحدة
وزارة شؤون مجلس الوزراء
مكتب رئاسة مجلس الوزراء

السياسة الوطنية للأمن السحابي

الإصدار 1.0

مايو 2023

تنبيه

اعتُمدت هذه الوثيقة ووافق مجلس الوزراء في دولة الإمارات العربية المتحدة عليها، وهي ملكية حصرية وخاصة للمجلس الأمن السيبراني.

ويحتفظ مجلس الأمن السيبراني بحقه في تعديل، أو إضافة، أو حذف أي بند أو قسم من هذه السياسة.

ولا يُمكن استخدام هذه الوثيقة أو أي جزء منها دون الحصول على الموافقة الخطية المسبقة من مجلس الأمن السيبراني.

ضوابط الإصدار

النسخة	0.1
التاريخ:	21 فبراير 2022
جهة الإعداد:	مجلس الأمن السيبراني
التعديل:	مسودة أولية

النسخة	0.2
التاريخ:	28 مارس 2022
جهة الإعداد:	مجلس الأمن السيبراني
التعديل:	التحديثات حسب الجلسة المنعقدة بتاريخ 24 فبراير 2022 مع هيئة أبوظبي الرقمية

النسخة	0.3
التاريخ:	25 مايو 2022
جهة الإعداد:	مجلس الأمن السيبراني
التعديل:	التحديثات حسب مراجعة الملاحظات بشأن مسودة الوثيقة ضمن النسخة الثانية

	جهة المراجعة	جهة الموافقة
المسمى الوظيفي:	xxxxxxxxx	xxxxxxxxx
الاسم:	xxxxxxxxx	xxxxxxxxx
التوقيع:	xxxxxxxxx	xxxxxxxxx
التاريخ:	xxxxxxxxx	xxxxxxxxx

فهرس المحتويات

فهرس المحتويات

2. مستخدمو الخدمات السحابية

فهرس المحتويات

فهرس المحتويات

القسم 1

المقدّمة

المقدّمة

في الآونة الأخيرة، أحدثت الخدمات السحابية تطورات سريعة في الأساليب المتبعة لتقديم الخدمات الرقمية. كما أصبحت تعد قوة دافعة رئيسية لتحقيق إنجازات ضخمة في مجالات التكنولوجيا المستقبلية، وتحليلات البيانات الضخمة، وإنترنت الأشياء. كما أثرت تطبيقات الخدمات السحابية جذريًا على المجال، حيث أنها توفّر للمستخدمين خدمات تقنية فعالة من حيث التكلفة والمرونة وقابلية التطوير، ومثل: أي تقنية ناشئة، فقد صاحب الخدمات السحابية العديد من التعقيدات
والتحديات الجدية فيما يتعلق بالأمن السيبراني.

برزت دولة الإمارات العربية المتحدة كمركز إقليمي للخدمات السحابية والبيانات والذكاء الاصطناعي. وبسبب الاعتماد والاستخدام المتزايد للخدمات السحابية محلياً وعالمياً ازدياداً ملحوظاً في التهديدات العامة، مما يتطلب اتباع نهج شامل يعالج المخاطر ويدعم الابتكار للحفاظ على أمن التحوّل الرقمي لدولة الإمارات العربية المتحدة.

وضع المجلس هذه السياسة لتعزيز الأمن السحابي، بما يتماشى مع الأولوية الوطنية لدولة الإمارات العربية المتحدة بأن تصبح رائدة عالمية في مجال الأمن السيبراني، كما ستساعد هذه السياسة في تحسين الوضع الأمني للمؤسسات والأفراد الذين يستخدمون الخدمات السحابية داخل دولة الإمارات.

1.1 الهدف

تهدف هذه السياسة إلى تعزيز وضع الأمن السحابي لدولة الإمارات العربية المتحدة من خلال تحديد مبادئ اعتماد ممارسات الخدمات السحابية الآمنة ومعالجة التحديات التي تواجه مشهد الخدمات السحابية الحالي. وستوفّر أيضاً إرشادات للنظام البيئي السحابي في الدولة، وتعرف متطلبات الأمن السحابي، وتحدّد الجهات المسؤولة عن الإشراف على تشريعات أمن السحابة وإنفاذها.

ستساعد هذه السياسة في التأكد من التزام مزوّدي الخدمات السحابية (CSP) بمجموعة من المتطلبات الأمنية، كما ستضمن توفير مستوى حماية جيد لجميع مستخدمي الخدمات السحابية عند شراء الخدمات المذكورة واستخدامها. وتهدف هذه السياسة أيضاً إلى تجنب الآثار السلبية المحتملة التي يُمكن أن تنتج عن تطبيقها، مثل: تثبيط الاستثمار وإعاقة نمو قطاع الخدمات السحابية بسبب المتطلبات الصارمة للغاية.

1.2 النطاق ومدى قابلية التطبيق

يتطلب تحقيق وضع أمن سحابي مرن تحديد المسؤوليات الأمنية والتأكد من فهمها بوضوح من قبل الأطراف المعنية. ويدرك مجلس الأمن السيبراني أن الخدمات السحابية ليست أحادية البعد، كما يحرص على تحديد مسؤوليات مختلفة بناءً على نماذج الخدمة المعتمدة. ومع ذلك، ستقع مسؤولية تطبيق الضوابط الأمنية في النهاية على الجهة التي تستخدم الخدمات السحابية. تم إعداد نموذج يحدّد قابلية تطبيق المتطلبات بناءً على نموذج الخدمة.

وتُعرف الخدمات على النحو التالي:

البرمجيات كخدمة (SaaS)

يمتلك المستخدم صلاحية استخدام تطبيقات المزوّد التي تعمل على البنية التحتية السحابية. والتي يُمكن الوصول إليها عن بُعد من أجهزة مختلفة، مثل: الويب أو واجهة البرنامج. ويملك المستخدم صلاحية استخدام التطبيق فقط ولا يستطيع إدارة أو التحكم في البنية التحتية السحابية الأساسية المستخدمة.

المنصة كخدمة (PaaS)

يمتلك المستخدم صلاحية نشر تطبيقات من تطويره أو تطوير غيره على البنية التحتية السحابية، من خلال استخدام لغات البرمجة والمكتبات والخدمات والأدوات التي يدعمها المزوّد. ومع ذلك، لا يستطيع المستخدم إدارة البنية التحتية السحابية الأساسية المستخدمة أو التحكم فيها.

البنية التحتية كخدمة (IaaS)

يمتلك المستخدم صلاحية توفير موارد الحوسبة الأساسية، مثل: المعالجة والتخزين والشبكات، لنشر وتشغيل البرامج، بما يشمل أنظمة التشغيل والتطبيقات.

1.2 النطاق ومدى قابلية التطبيق

مستخدمو الخدمات السحابية:

جهات البنية التحتية للمعلومات الحيوية

تنطبق سياسة الأمن السحابي على الجهات التابعة لحكومة الإمارات العربية المتحدة، بالإضافة إلى جهات البنية التحتية الحيوية التي ترغب بشراء الخدمات السحابية واستخدامها داخل الدولة. يُرجى الرجوع إلى سياسة البنى التحتية للمعلومات الحيوية لدولة الإمارات العربية المتحدة للاطلاع على قائمة مفصّلة لقطاعات البنية التحتية للمعلومات الحيوية.

الجهات التجارية (غير التابعة لقطاع البنية التحتية للمعلومات الحيوية)

لا تلزم الجهات التجارية التي ترغب بشراء الخدمات السحابية واستخدامها داخل الدولة باتباع سياسة الأمن السحابي وستكون في هذه الحالة بمثابة دليل إرشادي.

مزوّدو الخدمات السحابية (CSP):

يجب أن تلتزم الجهات التي ترغب بتقديم الخدمات السحابية داخل الدولة بسياسة الأمن السحابي. ويجب على مزوّدي الخدمات السحابية الالتزام بالمتطلبات المنصوص عليها في هذه السياسة.

1.3 دورة حياة الاعتماد

يحدّد الإطار الوطني لحوكمة الأمن السيبراني (NCSGF) نهجاً متكاملاً ومشتركاً لإدارة واعتماد الأمن السيبراني على مستوى الجهة والقطاع والمستوى الوطني، لذا حدّد الإطار دورة حياة واضحة تُمكن من فهم وتقييم وتطبيق ومراقبة وتعزيز التعاون في مجال الأمن السيبراني داخل دولة الإمارات العربية المتحدة. وتضمن دورة الحياة هذه التطوير المستمر لقدرات الأمن السيبراني في الدولة من خلال توفير متطلبات محدّدة ومدارة ومعتمدة على نحوٍ جيدًا فيما يتعلق بالتقنيات الناشئة، مثل: الخدمات السحابية.

فهم الأسباب الدافعة للتحوّل إلى استخدام الخدمات السحابية، والمهارات المطلوبة وكيفية توافق استراتيجية العمل مع أهداف التحوّل الرقمي الشاملة.

تقييم المخاطر والفوائد بما يمكّن من تحديد التهديدات، بالإضافة إلى تحديد الأثر على الأعمال وضوابط الأمن اللازمة للتخفيف من المخاطر واختيار النموذج السحابي المناسب.

تطبيق ضوابط الأمن المحدّدة على النموذج السحابي بناءً على تقييم المخاطر.

مراقبة ومراجعة الضوابط المنفذة وأداء وفعالية مزوّد الخدمة السحابية بما يتوافق مع السياسة الوطنية للأمن السحابي.

التعاون لتحديد الدور الذي تؤديه الكفاءة في زيادة عدد المستخدمين.

1.4 مبادئ الأمن السحابي

وُضعت مبادئ الأمن السحابي الخمسة التالية لتزويد صنّاع القرار بالعناصر الأساسية اللازمة لدفع الاعتماد الآمن للخدمات السحابية وعملياتها في دولة الإمارات العربية المتحدة. وتساعد هذه المبادئ مستخدمي ومزوّدي الخدمات السحابية في اتخاذ قرارات تتعلق بالسياسة والتشغيل والمشتريات بما يتماشى مع السياسات المفصّلة في هذا المستند.

النهج المبني على المخاطر

تُؤخذ المخاطر المحتملة على الأمن والمرونة في عين الاعتبار عند تنفيذ عمليه التقييم لاعتماد السحابة وتوسيع استخدامها.

الأمن السحابي المبني على البيانات

تتماشى بيانات الأمن السحابي مع حساسية البيانات وأثرها على الأعمال وتوقعات الخصوصية.

إرشادات أفضل الممارسات

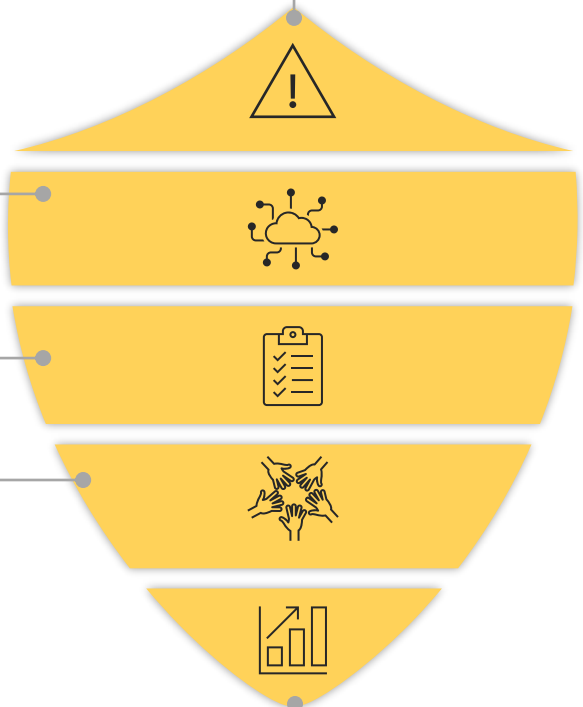
تهدف أطر العمل العالمية لأفضل الممارسات لتوفير ضمانات أمنية ودفع كفاءات الامتثال.

منظومة قائمة على التعاون والشفافية

تشجيع مستخدمي الخدمات السحابية ومزوّدي الخدمات السحابية والمنظمين على مشاركة المعلومات والممارسات الجيدة والإبلاغ عن الحوادث والمعلومات الاستخبارية في المنظومة السحابية.

التحسين المستمر

تحسين ممارسات أمن السحابة باستمرار لضمان ملاءمتها وكفاءتها وفاعليتها.



1.5 الموافقة على الاستثناءات

يجوز منح استثناء من السياسة من قبل مجلس الأمن السيبراني في ظل ظروف خاصة.

سيتم مراجعة الاستثناءات بناء على كل حالة ولا يتم تقديم أي ضمانات بالموافقة على الطلب.

القسم 2

مستخدمو الخدمات السحابية

يوضّح الجزء التالي الأقسام الأساسية والفرعية من السياسة والتي تنطبق على مستخدمي الخدمات السحابية في دولة الإمارات العربية المتحدة. وتوفّر الأقسام الفرعية للسياسة مزيداً من التفاصيل بشأن أهداف وبيانات السياسة.

2.1 الحوكمة السحابية

2.1.1 إطار الحوكمة

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

تأسيس القيادة والحوكمة لدعم تنفيذ متطلبات أمن السحابة.

بيانات السياسة

2.1.1.1 يجب على القيادة العليا للجهة المستخدمة للحوسبة السحابية إنشاء برنامج أمن سحابي يشمل إشراف وتوجيه واضحين، بالإضافة إلى تخصيص الموارد (الميزانية والأفراد والتكنولوجيا) لتنفيذ البرنامج بنجاح.

2.1.1.2 يجب على مستخدمي الخدمات السحابية توثيق السياسات التي تحكم الجوانب المهمة لأمن السحابة وإنشاء عملية لتحديد وضمان الامتثال للمتطلبات القانونية والتنظيمية المعمول بها في الخدمة السحابية.

2.1.1.3 عند شراء الخدمات السحابية، يجب على مستخدمي الخدمات السحابية التأكد من أن مزوّد الخدمات السحابية يمتلك ويطبق إطار حوكمة مناسب.

2.1 الحوكمة السحابية

2.1.2 إدارة المخاطر

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

تحديد ومعالجة مخاطر الأمان والخصوصية السحابية على نحوٍ استباقي في الوقت المناسب.

بيانات السياسة

2.1.2.1 يجب إنشاء وتنفيذ برنامج متميّز ومستمر لإدارة المخاطر ليشمل البيئة السحابية.

2.1.2.2 يجب إجراء تقييمات مخاطر الأمان والخصوصية لتحليل الأثر على البيانات أو الأصول المستضافة في البيئة السحابية.

2.1.2.3 يجب أن يتواصل مستخدمو الخدمات السحابية مع مزوّد الخدمة لمعرفة مدى امتثال المورّدين لمتطلبات أمن السحابة.

2.1 الحوكمة السحابية

2.1.3 أمن الأفراد

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

التأكد من فهم الأفراد الذين يستخدمون البيئة السحابية لمسؤولياتهم وضمان تلقيهم تدريبات أمنية منتظمة.

بيانات السياسة

2.1.3.1 يتعيّن على مستخدمي الخدمات السحابية اتباع متطلبات الأمن المنصوص عليها في السياسة الوطنية للأمن السيبراني، على أن ينطبق ذلك على جميع الأفراد المعنيين (الموظفين، والمورّدين، والمقاولين) الذين يستخدمون الخدمات السحابية

2.1.3.2 يجب على مستخدمي الخدمات السحابية التأكد من أن البنود التعاقدية مع مزوّدي الخدمات السحابية، تشمل: (1) التحقّق من خلفية موظفي المزوّد، (2) أدوار محدّدة بوضوح، ومصفوفة مسؤوليات تبيّن فصل الواجبات داخل نموذج المسؤولية المشتركة، (3) برامج منتظمة لرفع مستوى وعي المستخدم وبرامج تدريبية، (4) إجراءات تأديبية، (5) إجراءات نهاية خدمة منظمة، بما يشمل إنهاء العقد.

2.1 الحوكمة السحابية

2.1.4 أمن الطرف الخارجي وسلسلة التوريد

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

تقليل احتمالية تعرض سلسلة التوريد للخطر.

بيانات السياسة

2.1.4.1 يجب أن يعرف مستخدمو الخدمات السحابية المعلومات التي يتم مشاركتها أو الوصول إليها من موردي مزوّد الخدمة وسلسلة التوريد الخاصة بهم.

2.1.4.2 يجب على مستخدمي الخدمات السحابية تحديد المخاطر الأمنية لاستخدام موارد سلسلة التوريد.

2.1.4.3 يجب أن يتواصل مستخدمو الخدمات السحابية مع مزوّد الخدمة لمعرفة مدى امتثال المورّدين لمتطلبات أمن السحابة.

2.1 الحوكمة السحابية

2.1.5 الضمانات والاختبارات المستقلة

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

ضمان التنفيذ الفعّال لضوابط أمن السحابة من خلال إجراء الاختبارات المستقلة وتقليل الاعتماد على الضمانات والتأكيدات التي يقدّمها المزوّد.

بيانات السياسة

2.1.5.1 يجب على مستخدمي الخدمات السحابية إشراك طرف خارجي يتمتع بالمهارات الكافية لإجراء اختبار مستقل لعملية تطبيق الرقابة الأمنية.

2.1.5.2 يجب على مستخدمي الخدمات السحابية إجراء اختبارات ضمان مستقلة لتصميم الخدمة ولمكوناتها.

2.2 الاتفاقيات التعاقدية

2.2.1 اتفاقيات عدم الإفصاح

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

حماية سرية البيانات المتعلقة بمستخدم الخدمات السحابية في البيئة السحابية.

بيانات السياسة

2.2.1.1 يجب على مستهلكي خدمات الحوسبة السحابية بذل العناية القانونية الواجبة ومراجعة جميع الالتزامات التعاقدية بالتفصيل قبل المشاركة في أي خدمات سحابية أو مع مزودي خدمات الحوسبة السحابية أو كليهما للتأكد من أن استخدام أي خدمات سحابية أو مزودي خدمات الحوسبة السحابية أو كليهما سيكون متناسب ا مع ملف تعريف مخاطر المؤسسة.

2.2.1.2 يجب أن تشتمل الاتفاقيات التعاقدية على اتفاقية عدم إفصاح رسمية، على أن يوقعها الطرفان قبل شراء أو استخدام الخدمات السحابية

2.2 الاتفاقيات التعاقدية

2.2.2 اتفاقيات مستوى الخدمة

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

حماية حقوق مستخدم الخدمات السحابية ومزوّد الخدمة على نحو استباقي.

بيانات السياسة

2.2.2.1 يجب أن تشتمل الاتفاقيات التعاقدية على اتفاقية مستوى خدمة رسمية توضح بالتفصيل مدى توفّر الخدمات المقدمة وملكية البيانات وتقسيم المسؤولية وغيرها على أن يتم توقيعها من قبل الطرفين قبل شراء أو استخدام الخدمات السحابية.

2.3 إدارة أمن البيانات ودورة حياتها

2.3.1 حوكمة البيانات

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

ضمان تصنيف البيانات وحمايتها من الاستخدام والوصول غير المصرح به والضياع والتدمير والتزوير.

بيانات السياسة

2.3.1.1 يجب وضع السياسات والإجراءات وتنفيذها فيما يتعلق بتصنيف البيانات وتحديدها ومعالجتها خلال كامل دورة حياتها وذلك لتأمين البيانات الموجودة (على نحو دائم أو مؤقت) داخل تطبيقات الخدمة الموزعة جغرافياً (المادية والافتراضية) والبنية التحتية والشبكة ومكونات الأنظمة ويتم مشاركتها مع أطراف خارجية أخرى للتأكد من الامتثال لاتفاقية سلسلة التوريد التنظيمية أو القانونية.

2.3.1.2 يجب تصنيف البيانات والأشياء التي تحتوي على بيانات من قبل مالك البيانات بناءً على نوع البيانات وقيمتها وحساسيتها وأهميتها.

2.3 إدارة أمن البيانات ودورة حياتها

2.3.2 التشفير وعلوم التشفير

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

حماية البيانات أثناء تخزينها ونقلها ومعالجتها داخل البيئة السحابية.

بيانات السياسة

2.3.2.1 يجب وضع السياسات والإجراءات وتنفيذها فيما يتعلق باستخدام بروتوكولات التشفير لحماية البيانات الحساسة المخزنة (مثل: خوادم الملفات، وقواعد البيانات، وأجهزة المستخدم النهائي)، والبيانات المستخدمة (الذاكرة)، والبيانات قيد الإرسال (مثل: واجهات النظام والإرسال عبر الشبكات العامة والرسائل الإلكترونية) وفقاً لقوانين الامتثال القانونية والتشريعية والتنظيمية المعمول بها.

2.3.2.2 يجب أن يحتفظ مستخدم الخدمات السحابية، أو مزوّد إدارة مفاتيح موثوق بالمفاتيح. ويجب أن يتم الفصل بين مهام إدارة المفاتيح واستخدامها

2.4 موقع البيانات وسيادتها

2.4.1 معرفة موقع البيانات

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

التأكد من أن مستخدم الخدمات السحابية على علم بمواقع تخزين البيانات ومعالجتها وإدارتها.

بيانات السياسة

2.4.1.1 يجب أن يكون موقع البيانات معروفاً في جميع المراحل ويتم التعامل معه وفقاً للقوانين واللوائح فيما يتعلق بموقع البيانات وسيادتها، أي المعايير والأطر المعمول بها والمنشورة داخل دولة الإمارات العربية المتحدة.

2.4.1.2 أثناء اختيار مزوّد الخدمات السحابية، يجب على مستخدمي الخدمات السحابية التأكد من أنه يعمل ضمن نطاقات قانونية مقبولة.

2.4.1.3 يجب على مستخدمي الخدمات السحابية التحقّق من قبولهم لأي اتفاقيات مع مزوّد الخدمة والتي تتعلق باستخدامه بياناتهم والتأكد أيضاً من أنها لا تتعارض مع التشريعات المحلية ذات الصلة.

2.4.1.4 يجب على مستخدمي الخدمات السحابية ان يحددو, اعتمادًا على تصنيف البيانات التي سيتم استضافتها متطلبات توطين البيانات ومتطلبات الأمان ذات الصلة المطلوب تنفيذها.

2.5 توافقية التشغيل وقابلية النقل

2.5.1 توافقية التشغيل

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

التأكد من أن مستخدم الخدمات السحابية يُمكنه اختيار العديد من مزوّدي الخدمات السحابية المتنوعين الذين يستطيعون التعاون والتفاعل مع بعضهم بعضاً.

بيانات السياسة

2.5.1.1 يجب وضع السياسات والإجراءات والأحكام والشروط المتفق عليها على نحو متبادل لتلبية متطلبات مستهلك السحابة لتطبيق خدمة إلى خدمة وإمكانية التشغيل البيني لمعالجة المعلومات وإمكانية النقل لتطوير التطبيقات وتبادل المعلومات والاستخدام واستمرار النزاهة.

2.5.1.2 يجب على مستخدمي الخدمات السحابية التأكد من أن معايير القطاع وواجهات برمجة التطبيقات المتاحة يتم استخدامها باستمرار وتطبيقها عبر بياناتهم وخدمات السحابة لدعم قابلية التشغيل البيني.

2.5.1.3 يجب مستخدمي الخدمات السحابية توثيق السياسات والإجراءات المناسبة التي تحدد متطلبات إمكانية التشغيل وإبلاغها بوضوح لجميع الأطراف.

2.5 توافقية التشغيل وقابلية النقل

2.5.2 قابلية النقل

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

حماية مستخدمي الخدمات السحابية من الحاجة إلى التعامل مع نفس المزوّد وضمان سهولة النقل والتغيير بين مختلف مزوّدي الخدمات السحابية.

بيانات السياسة

2.5.2.1 يجب أن تتضمن الاتفاقيات التعاقدية أحكاماً تحدّد قدرة المستخدم على الوصول إلى جميع البيانات المهيكلة وغير المهيكلة بإحدى الصيغ القياسية المستخدمة في المجال عند إنهاء العقد.

2.5.2.2 يجب على مستخدمي الخدمات السحابية التأكد عند شراء الخدمات السحابية من إثبات مزوّدي الخدمات السحابية بقابلية النقل.

2.5.2.3 يجب على مستخدمي الخدمات السحابية توثيق السياسات والإجراءات المناسبة التي تحدد متطلبات قابلية النقل وإبلاغها بوضوح لجميع الأطراف.

2.6 البنية السحابية والبنية التحتية والمحاكاة الافتراضية للسحابة

2.6.1 التحكم في التغيير والإعدادات

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

ضمان تحديد التغييرات التي تم إجراؤها على البنية التحتية السحابية وإدارتها، وكشف أي تغييرات غير مصرح بها.

بيانات السياسة

2.6.1.1 يجب على مستخدمي الخدمات السحابية التأكد عند شراء الخدمات السحابية من أن مزوّد الخدمة يمتلك ضوابط كافية لإدارة التغيير بما يمكّن من تتبع إعدادات مكونات الخدمة وموقعها وحالتها طوال فترة استخدام الخدمة.

2.6.1.2 يجب أن يتمكن المستخدمون من الوصول إلى نتائج أي تغيير أو نقل تتعرض له الصورة والتحقّق لاحقاً من سلامة الصورة من خلال الأساليب الإلكترونية (مثل: البوابات أو التنبيهات).

2.6 البنية السحابية والبنية التحتية والمحاكاة الافتراضية للسحابة

2.6.2 أمن مراكز البيانات

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

ضمان توفير الحماية المادية ضد الوصول غير المصرح به أو التلاعب أو السرقة أو تغيير إعدادات الأنظمة.

بيانات السياسة

2.6.2.1 عند شراء الخدمات السحابية، يجب على مستخدمي الخدمات السحابية التأكد من أن مزوّد الخدمات السحابية يمتلك ضوابط أمان كافية في مركز البيانات.

2.6 البنية السحابية والبنية التحتية والمحاكاة الافتراضية للسحابة

2.6.3 إدارة الأصول والأجهزة الطرفية

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

تعزيز الأمن الإلكتروني لمستخدم الخدمات السحابية من خلال معرفة الأصول والأجهزة الطرفية السحابية والمخاطر المرتبطة بها.

بيانات السياسة

2.6.3.1 يجب تطوير السياسات وتنفيذها لضمان فهرسة جميع أصول السحابة والأجهزة الطرفية وتعقبها وإدارتها على نحو آمن بناءً على مخاطر الأعمال المؤسسية.

2.6 البنية السحابية والبنية التحتية والمحاكاة الافتراضية للسحابة

2.6.4 أمن التطبيقات

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

حماية سرية وسلامة وتوفّر البيانات داخل تطبيقات وبيئة مزوّد الخدمات السحابية.

بيانات السياسة

2.6.4.1 يجب تطوير السياسات والإجراءات وتنفيذها بحيث يكون الأمن محوراً رئيسياً في دورة تطوير التطبيق؛ والتصميم والتطوير والتقييم.

2.6.4.2 يجب على مستخدمي الخدمات السحابية التأكد عند شراء الخدمات السحابية من أن مزوّد الخدمة يمتلك ضوابط أمن التغيير المناسبة.

2.6 البنية السحابية والبنية التحتية والمحاكاة الافتراضية للسحابة

2.6.5 تقوية الجهاز

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

تفعيل المنافذ والبروتوكولات والخدمات الضرورية فقط واللازمة لتلبية احتياجات العمل.

بيانات السياسة

2.6.5.1 يجب أن يتأكد المستخدمون من تطوير وتطبيق إرشادات تقوية مناسبة لجميع الأنظمة السحابية (المادية والافتراضية)، بما يشمل على سبيل المثال لا الحصر أنظمة التشغيل، والأجهزة الافتراضية، ومراقب الأجهزة الافتراضية Hypervisor، وأجهزة الشبكات والأمن.

2.7 إدارة الهوية وصلاحية الوصول

2.7.1 هويات مستخدمي الخدمات السحابية

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

إدارة هويات المستخدمين في السحابة على نحو آمن.

بيانات السياسة

2.7.1.1 يجب أن تقتصر بيئة مصادقة المستخدم وصلاحية إدارة الهويات/المعرفات على الموظفين المعتمدين التابعين للجهة المستخدمة للخدمة.

2.7.1.2 يجب على مستخدمي الخدمات السحابية تنفيذ عمليات مركزية لإنشاء حساب متميز (حسابات الجذر) والتحكم الصارم في الأنشطة التي يُمكن إجراؤها من خلال الحساب والحد منها. ويجب الأخذ في الاعتبار تطبيق المصادقة متعددة العوامل لجميع الحسابات داخل السحابة.

2.7.1.3 يجب أخذ في عين الإعتبار المصادقة متعددة العوامل لجميع الحسابات داخل السحابة.

2.7 إدارة الهوية وصلاحية الوصول

2.7.2 المصادقة والتصريح السحابي

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

منع الوصول غير المصرح به ومنع أي تعديل على الموارد والتطبيقات والبيانات المؤسسية في أثناء استخدام الخدمات السحابية.

بيانات السياسة

2.7.2.1 يجب على مستخدمي الخدمات السحابية وضع عمليات وإجراءات لمصادقة الوصول إلى الأنظمة والتطبيقات وأصول البيانات من خلال دمج المصادقة على السحابة مع خدمة الدليل الداخلية.

2.7.2.2 يجب تطبيق ضوابط التحكم بالوصول القائمة على الدور داخل واجهات الإدارة.

2.7.2.3 يجب على مستخدمي الخدمات السحابية تنفيذ العمليات والإجراءات للتحقّق من إمكانية الوصول المصرح به إلى البيانات ووظائف النظام.

2.7.2.4 يجب تطبيق خدمة المصادقة متعددة العوامل على الحسابات ذات الصلاحيات المرتفعة داخل السحابة.

2.7 إدارة الهوية وصلاحية الوصول

2.7.3 حوكمة الوصول

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

إزالة المخاطر المترتبة على العمليات المستخدمة لطلب الوصول والموافقة عليه ومنحه وإدارته ومراجعته.

بيانات السياسة

2.7.3.1 يجب على مستخدمي الخدمات السحابية تحديد وتنفيذ الطلبات والموافقات الرسمية كجزء من عملية توفير الوصول للمستخدم.

2.7.3.2 يجب على مستخدمي الخدمات السحابية التأكد من إلغاء أو تعديل الوصول في الوقت المناسب في حال تغير حالة الموظف الوظيفية أو حدوث تغييرات على هوية النظام.

2.7.3.3 يجب على مستخدمي الخدمات السحابية مراجعة حقوق الوصول والاستحقاقات دوريًا وإعادة التصديق عليها.

2.8 إدارة الحوادث الأمنية والاكتشاف الإلكتروني والأدلة الجنائية السحابية

2.8.1 عملية إدارة الحوادث

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

تقليل أثر المشكلات البيئية والأمنية والمشكلات المتعلقة بالموثوقية على الخدمة السحابية.

بيانات السياسة

2.8.1.1 يجب على مستخدمي الخدمات السحابية، بالموائمة مع مزوّدي الخدمات السحابية، وضع عمليات محدّدة لإدارة حوادث الخدمات السحابية، والتي يجب اختبارها وتطبيقها بانتظام استجابةً للحوادث الأمنية.

2.8.1.2 يجب أن تشتمل إدارة الحوادث على عمليات محدّدة مسبقاً لتمكن الاستجابة للأنواع الشائعة من الحوادث والهجمات على البيئة السحابية.

2.8 إدارة الحوادث الأمنية والاكتشاف الإلكتروني والأدلة الجنائية السحابية

2.8.2 الإبلاغ عن الحوادث

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

ضمان الإبلاغ عن الحوادث الأمنية ضمن إطار زمني مناسب وباستخدام صيغ مقبولة.

بيانات السياسة

2.8.2.1 يجب على مستخدمي الخدمات السحابية تنفيذ عملية محدّدة واتباع مسار معين للإبلاغ عن الحوادث الأمنية.

2.8.2.2 يُعد مستخدمو الخدمات السحابية مسؤولين عن إعلام وإخطار الجهات الخارجية ذات الصلة في غضون إطار زمني مقبول.

2.8.2.3 يجب حفظ وتحديث نقاط الاتصال مع السلطات التنظيمية المسؤولة، وسلطات إنفاذ القانون الوطنية والمحلية، وغيرها من السلطات القضائية القانونية.

2.8 إدارة الحوادث الأمنية والاكتشاف الإلكتروني والأدلة الجنائية السحابية

2.8.3 الاستجابة للحوادث

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

احتواء وتقليل الآثار الناتجة عن الحوادث الأمنية.

بيانات السياسة

2.8.3.1 يجب على مستخدمي الخدمات السحابية وضع إجراءات واضحة لتفعيل إدارة الحوادث الأمنية، وإنشاء خطة استجابة للحوادث بما يتماشى مع خطة الاستجابة لحوادث الأمن السيبراني كما يجب عليهم تحديد بروتوكول ذي صلة لإعلام الإدارة بتطورات الحادث ومدى (نسبة) احتوائه والتواصل مع الجهات المعنية على النحو المناسب.

2.8.3.2 يجب على مستخدمي الخدمات السحابية تقييم القدرات التي يوفّرها مزوّدو الخدمات السحابية على نحو كافٍ والنظر في الحصول على مزوّدي الخدمات الخارجيين أو تقديم الخدمة داخليًا حيث قد لا تتوفّر إمكانات مزوّدو الخدمات السحابية.

2.8 إدارة الحوادث الأمنية والاكتشاف الإلكتروني والأدلة الجنائية السحابية

2.8.4 الاكتشاف الإلكتروني والأدلة الجنائية السحابية

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

دعم عمليات التحري في الحوادث وتلبية طلبات الاكتشاف الإلكتروني للإجراءات القانونية.

بيانات السياسة

2.8.4.1 يجب على مستخدمي الخدمات السحابية تحديد الموظفين المناسبين للإشراف على إعداد وإدارة قدرات الاكتشاف الإلكتروني والأدلة الجنائية السحابية بمقاييس واضحة.

2.8.4.2 يجب على مستخدمي الخدمات السحابية وضع بروتوكولات للتعامل مع الأدلة الجنائية الإلكترونية بحيث تتوافق مع إجراءات إنفاذ القانون فيما يتعلق بالتعامل مع الأدلة الرقمية والتأكد من امتثال مزوّدي الخدمات السحابية لهذه البروتوكولات.

2.9 المرونة السحابية

2.9.1 الاحتفاظ الآمن بالنسخ الاحتياطية

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

ضمان توفّر المعلومات على قدرٍ كبير لتقليل أثر الحوادث.

بيانات السياسة

2.9.1.1 يجب على مستخدمي الخدمات السحابية تحديد متطلبات النسخ الاحتياطي المنتظم للمعلومات داخل البيئات السحابية والجدول الزمني لاختبار استعادة النسخ الاحتياطية.

2.9.1.2 يجب على مستخدمي الخدمات السحابية تطبيق متطلبات التشفير للنسخ الاحتياطية والتأكد من نجاح جهود استعادة هذه البيانات.

2.9 المرونة السحابية

2.9.2 استمرارية الأعمال والتعافي من الكوارث

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

ضمان توفّر الموارد والمعلومات على قدرٍ كبير كجزء من المجهودات المتواصلة، بالإضافة إلى العمل على تقليل أثر انقطاع الخدمات والحوادث.

بيانات السياسة

2.9.2.1 يجب اختبار والإبلاغ عن متطلبات استمرارية التشغيل، بما يشمل وقت التشغيل، وأولويات الاسترداد، كونها جزءًا من عقود الخدمة السحابية.

2.9.2.2 يجب على مستخدمي الخدمات السحابية مراجعة خطط استمرارية الأعمال واستعادة القدرة على العمل بعد الكوارث لدى مزوّدي الخدمات السحابية والتأكد من توافقها مع متطلبات استمرارية الأعمال لمستخدم الخدمات السحابية.

2.9.2.3 يجب أن تحدد خطط الاسترداد على الأقل الفترة القصوى المسموح بها للاضطراب (MTPD)، وهدف وقت الاسترداد (RTO)، وهدف نقطة الاسترداد (RPO)، وأدوار ومسؤوليات جميع الأطراف ذات الصلة.

القسم 3

مزوّدو الخدمات السحابية

يوضّح الجزء التالي الأقسام الأساسية والفرعية من السياسة والتي تنطبق على موزعي الخدمات السحابية في دولة الإمارات العربية المتحدة. وتوفّر الأقسام الفرعية للسياسة مزيداً من التفاصيل بشأن أهداف وبيانات السياسة.

3.1 الحوكمة السحابية

3.1.1 إطار الحوكمة

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

تنسيق وتوجيه نهج شامل لإدارة الخدمات والمعلومات المخزنة فيها.

بيانات السياسة

3.1.1.1 يجب إنشاء إطار حوكمة للأمن لضمان استمرارية فعالية الإجراءات والموظفين والضوابط المادية والتقنية طوال فترة الخدمة، واستجابتها للتغيرات في الخدمة والتهديد وتطور التكنولوجيا.

3.1 الحوكمة السحابية

3.1.2 إدارة المخاطر

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

التأكد من أن اعتبارات الأمن والخصوصية جزء من عملية المخاطر التشغيلية وآليات الإبلاغ الخاصة بمزوّد الخدمة.

بيانات السياسة

3.1.2.1 يجب مراقبة مخاطر الأمن والخصوصية التي تؤثر في الخدمات والإبلاغ عنها باستمرار بناءً على عملية إدارة المخاطر الموثقة رسمياً.

3.1 الحوكمة السحابية

3.1.3 أمن الأفراد

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

تقليل احتمالية تعرض بيانات المستخدم إلى الانكشاف العرضي أو الخبيث من جانب موظفي مزوّد الخدمة، والتأكد من تنفيذ الفحوصات الشاملة المدعومة بتقديم التدريبات المناسبة.

بيانات السياسة

3.1.3.1 يجب أن يخضع الموظفون الذين يملكون صلاحيات الوصول إلى بيانات وأنظمة المستخدم إلى التدقيق الأمني وإجراء التحقّق من خلفية الموظف.

3.1.3.2 يجب توفير التعليم والتدريب الأمني المستمر للموظفين بناءً على دورهم المميز في البيئة السحابية وبما يتوافق مع متطلبات المستخدمين (حسب الاقتضاء).

3.1.3.3 يجب اتباع عملية تأديبية ومنظمة إجراءات رسمية في حال انتهاء خدمة أحد الموظفين وفقاً للالتزامات التعاقدية مع مستخدمي الخدمات السحابية.

3.1 الحوكمة السحابية

3.1.4 أمن الطرف الخارجي وسلسلة التوريد

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

تقليل احتمالية تعرض سلسلة التوريد للاختراق والتأكد من أنها تدعم جميع متطلبات السياسة السحابية على نحو مُرض للمضي قدماً في تنفيذها من جانب مزوّد الخدمة.

بيانات السياسة

3.1.4.1 يجب على مزوّد الخدمات السحابية إدارة المخاطر الأمنية الناتجة عن المورّدين الخارجيين وشركاء تقديم الخدمة.

3.1.4.2 يجب أن يفرض مزوّد الخدمات السحابية متطلبات أمن السحابة على المورّدين بما يتماشى مع هذه السياسة ومتطلبات المستخدم (حسب الاقتضاء).

3.1.4.3 يجب على مزوّد الخدمات السحابية تنفيذ عمليات إدارة توافق متطلبات الأمن للمورد وإجراء عمليات تدقيق منتظمة وتقديم تقارير للمستخدمين على أساس الحاجة إلى المعرفة.

3.1 الحوكمة السحابية

3.1.5 الضمانات والاختبارات المستقلة

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

التأكد من تطبيق جميع متطلبات الأمن السحابية، وتحقيق الأهداف في الممارسة العملية.

بيانات السياسة

3.1.5.1 يجب أن يحمل مزوّد الخدمات السحابية شهادات امتثال للمعايير المعترف بها لنطاق الخدمات والمنتجات السحابية التي يتم توفيرها للمستخدمين.

3.1.5.2 يجب أن يوفر مزوّد الخدمات السحابية المرونة اللازمة لتمكين المستخدمين لاختبار ضمان مستقل لتصميم الخدمات والمكونات.

3.2 الاتفاقيات التعاقدية

3.2.1 اتفاقيات عدم الإفصاح

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

حماية سرية البيانات المتعلقة بمستخدم الخدمات السحابية في البيئة السحابية.

بيانات السياسة

3.2.1.1 يجب أن تشتمل الاتفاقيات التعاقدية على اتفاقية عدم إفصاح رسمية، على أن يتم توقيعها من قبل الطرفين قبل شراء أو استخدام الخدمات السحابية

3.2.1.2 يجب أن تشتمل الاتفاقيات التعاقدية على اتفاقية عدم إفصاح رسمية، على أن يتم توقيعها من قبل الطرفين قبل شراء أو استخدام الخدمات السحابية

3.2 الاتفاقيات التعاقدية

3.2.2 اتفاقيات مستوى الخدمة

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

حماية حقوق مستخدم الخدمات السحابية ومزوّد الخدمة على نحو استباقي.

بيانات السياسة

3.2.2.1 يجب أن تشتمل الاتفاقيات التعاقدية على اتفاقية مستوى خدمة رسمية توضح بالتفصيل مدى توفّر الخدمات المقدمة وملكية البيانات وتقسيم المسؤولية وغيرها على أن يتم توقيعها من قبل الطرفين قبل شراء أو استخدام خدمات الخدمات السحابية.

3.2.2.2 يجب أن تشتمل اتفاقيات مستوى الخدمة بين مزوّد خدمة الخدمات السحابية ومورد الطرف الخارجي على المخاطر المرتبطة بموردي الطرف الخارجي وشركاء تقديم الخدمة.

3.3 إدارة أمن البيانات ودورة حياتها

3.3.1 حوكمة البيانات

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

التأكد من الحفاظ على أمن البيانات في البيئات السحابية، بحيث يقتصر الوصول على الموظفين المصرح لهم فقط.

بيانات السياسة

3.3.1.1 يجب وضع سياسات وإجراءات لتصنيف البيانات وحمايتها ومعالجتها خلال دورة حياتها، بما يتماشى مع جميع القوانين، واللوائح، والمعايير، ومستويات المخاطر المعمول بها.

3.3 إدارة أمن البيانات ودورة حياتها

3.3.2 التشفير وعلوم التشفير

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

حماية البيانات من خلال تطبيق عمليات التشفير المتوافقة مع معايير القطاع وأفضل ممارسات إدارة المفاتيح.

بيانات السياسة

3.3.2.1 يجب وضع سياسات للتشفير وإدارة المفاتيح وتنفيذها لضمان التشفير الآمن للبيانات أثناء تخزينها ونقلها.

3.4 موقع البيانات وسيادتها

3.4.1 الشفافية في الإبلاغ عن مواقع البيانات

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

ضمان شفافية مزوّد الخدمة مع المستخدمين فيما يتعلق بمواقع معالجة البيانات ونقلها وتخزينها.

بيانات السياسة

3.4.1.1 يجب إبلاغ المستخدم بمواقع معالجة البيانات وتخزينها ونقلها، بالإضافة إلى مواقع حفظ نُسخِها الاحتياطية، كما يجب الامتثال للالتزامات التعاقدية والقوانين واللوائح المعمول بها فيما يتعلق بموقع البيانات وسيادتها في جميع هذه المراحل.

3.5 توافقية التشغيل وقابلية النقل

3.5.1 توافقية التشغيل

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

ضمان قيام مزوّدي الخدمات السحابية بالارتقاء بمستوى توافقية التشغيل إلى أقصى حد ممكن، بما يمنح المستخدم حرية شراء خدمات سحابية مختلفة من مزوّدي خدمات مختلفين في نفس الوقت.

بيانات السياسة

3.5.1.1 يجب الحفاظ على توافقية التشغيل بين توافقية التشغيل بين المستخدمين وبيئات مزوّدي الخدمة والمزوّدين المختلفين لضمان حرية المستخدم في اختيار المزوّد المفضل لديه للخدمات ذات الصلة.

3.5.1.2 يجب أن يستخدم مزوّد الخدمات السحابية واجهات برمجة التطبيقات المفتوحة والمنشورة لضمان دعم توافقية التشغيل بين المكونات وتسهيل عملية ترحيل التطبيقات.

3.5.1.3 يجب أن يستخدم المزوّد نظاماً افتراضياً معروفاً في القطاع، بالإضافة إلى صيغ افتراضية قياسية لضمان توافقية التشغيل.

3.5.1.4 يجب أن يتبع مزوّد الخدمات السحابية أي سياسات وإجراءات يحددها المستهلكون بما يتماشى مع متطلبات توافقية التشغيل للمستهلك.

3.5 توافقية التشغيل وقابلية النقل

3.5.2 قابلية النقل

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

حماية مستخدمي الخدمات السحابية من الحاجة إلى التعامل مع نفس المزوّد وضمان سهولة النقل والتغيير بين مزوّدي الخدمات السحابية.

بيانات السياسة

3.5.2.1 يجب على مزوّدي الخدمات السحابية توفير وثيقة للمستخدمين توضح بالتفصيل معايير توافقية التشغيل وقابلية النقل المستخدمة.

3.5.2.2 يجب على مزوّدي الخدمات السحابية استخدام بروتوكولات شبكة آمنة وموحدة لاستيراد البيانات وتصديرها وإدارة الخدمة.

3.5.2.3 يجب أن يتبع مزوّدي الخدمات السحابية أي سياسات وإجراءات يحددها المستهلكون بما يتماشى مع متطلبات قابلية المستهلك للنقل

3.6 البنية السحابية والبنية التحتية والمحاكاة الافتراضية للسحابة

3.6.1 التحكم في التغيير والإعدادات

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

ضمان عدم تسبب التغييرات في البنية التحتية الخاصة بالسحابة بانقطاع طويل وتعطيل للخدمات السحابية.

بيانات السياسة

3.6.1.1 يجب التخطيط على نحو استباقي للتغييرات التي ستطرأ على البنية التحتية السحابية للمزوّد وتنظيمها بكفاءة، وبما يضمن الامتثال لمتطلبات وقت التشغيل المعمول بها.

3.6.1.2 يجب أن يضمن مزوّد الخدمات السحابية سلامة جميع صور الأجهزة الافتراضية في جميع الأوقات. ويجب تسجيل أي تغييرات يتم إجراؤها على صور الأجهزة الافتراضية، والإبلاغ عنها بغض النظر عن حالة تشغيلها (على سبيل المثال: معلق، أو متوقف، أو قيد التشغيل).

3.6 البنية السحابية والبنية التحتية والمحاكاة الافتراضية للسحابة

3.6.2 أمن مراكز البيانات

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

حماية أصول ومرافق مزوّد الخدمة من مخاطر الأمن المادي والعوامل البيئية.

بيانات السياسة

3.6.2.1 يجب أن يحافظ مزوّد الخدمة على الأمن المادي لمرافقه وأصوله من خلال تحديد صلاحيات الدخول لتقتصر على الموظفين المصرح لهم فقط، ومراقبة دخول الزوار وأنظمة مراقبة مركز البيانات، كما يجب أن يحمي منشآته على نحو استباقي من العوامل البيئية.

3.6 البنية السحابية والبنية التحتية والمحاكاة الافتراضية للسحابة

3.6.3 إدارة الأصول والأجهزة الطرفية

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

تعزيز موقف الأمن السيبراني لمزوّد الخدمة من خلال فهم أصوله والأجهزة الطرفية والمخاطر المرتبطة به.

بيانات السياسة

3.6.3.1 يجب تطوير السياسات وتنفيذها لضمان فهرسة جميع الأصول والأجهزة الطرفية وتعقبها وإدارتها على نحو آمن بناءً على مخاطر الأعمال المؤسسية.

3.6 البنية السحابية والبنية التحتية والمحاكاة الافتراضية للسحابة

3.6.4 أمن التطبيقات

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

حماية سرية وسلامة وتوفّر البيانات داخل تطبيقات وبيئة مزوّد الخدمات السحابية.

بيانات السياسة

3.6.4.1 يجب تصميم وتطوير ونشر واختبار التطبيقات وواجهات البرمجة وفقاً لمعايير القطاع الرائدة، بالإضافة إلى الالتزام بمتطلبات الامتثال القانونية أو التشريعية أو التنظيمية المعمول بها.

3.6 البنية السحابية والبنية التحتية والمحاكاة الافتراضية للسحابة

3.6.5 تقوية الجهاز

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

تفعيل المنافذ والبروتوكولات والخدمات الضرورية فقط واللازمة لتلبية احتياجات العمل.

بيانات السياسة

3.6.5.1 يجب أن يضمن مزوّد الخدمة تطوير وتطبيق إرشادات قوية مناسبة للأنظمة السحابية (المادية والافتراضية) كما هو مناسب، بما يشمل على سبيل المثال لا الحصر: أنظمة التشغيل، والأجهزة الافتراضية، ومراقب الأجهزة الافتراضية Hypervisor، وأجهزة الشبكات والأمن.

3.7 إدارة الهوية وصلاحية الوصول

3.7.1 إدارة الهوية السحابية وصلاحية الوصول

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

تلبية توقعات مستخدمي الخدمات السحابية لمنع الوصول غير المصرح به إلى البيانات.

بيانات السياسة

3.7.1.1 يجب أن تفي عمليات المصادقة والتحكم في الوصول والمساءلة والتسجيل (الصيغة والاحتفاظ والوصول) بالمواصفات المطلوبة من مستخدم الخدمات السحابية والتي تكون متوافقة مع المتطلبات التنظيمية والقانونية.

3.8 إدارة الحوادث الأمنية والاكتشاف الإلكتروني والأدلة الجنائية السحابية

3.8.1 عملية إدارة الحوادث

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

تقليل أثر المشكلات البيئية والأمنية ومشكلات الموثوقية على الخدمة السحابية.

بيانات السياسة

3.8.1.1 يجب أن يتبع مزوّد الخدمات السحابية عمليات محدّدة لإدارة حوادث الخدمات السحابية، والتي يجب اختبارها وتطبيقها بانتظام استجابةً للحوادث الأمنية.

3.8 إدارة الحوادث الأمنية والاكتشاف الإلكتروني والأدلة الجنائية السحابية

3.8.2 الإبلاغ عن الحوادث

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

ضمان الإبلاغ عن الحوادث الأمنية ضمن إطار زمني مناسب وباستخدام صيغ مقبولة.

بيانات السياسة

3.8.2.1 يجب إعلام مستخدمي الخدمات السحابية والسلطات في الإمارات العربية المتحدة المتأثرة بالحوادث الأمنية بما يتوافق مع الأطر الزمنية المعمول بها.

3.8.2.2 يجب تنفيذ مسح منتظم للتهديدات والثغرات الأمنية لتحديد أولويات المعالجة والاستجابة بهدف التوصل إلى توقعات ذات جودة عالية. ويجب إعلام مجتمع الحوسبة الحسابية بخصوص التهديدات الناشئة، حسب الحاجة.

3.8.2.3 يجب على مزوّدو خدمات الحوسبة السحابية إبلاغ التهديدات الناشئة لمجتمع السحابة الأوسع، حسب الاقتضاء.

3.8 إدارة الحوادث الأمنية والاكتشاف الإلكتروني والأدلة الجنائية السحابية

3.8.3 الاستجابة للحوادث

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

احتواء وتقليل الآثار الناتجة عن الحوادث الأمنية.

بيانات السياسة

3.8.3.1 يجب بناء قدرات استجابة للحوادث لتمكين احتواء وتقليل آثار الحوادث الأمنية على نحو فعّال من خلال خطط رسمية للاستجابة للحوادث بما يتماشى مع خطة وإطار الاستجابة لحوادث الأمن السيبراني.

3.8 إدارة الحوادث الأمنية والاكتشاف الإلكتروني والأدلة الجنائية السحابية

3.8.4 الاكتشاف الإلكتروني والأدلة الجنائية السحابية

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

دعم عمليات التحري في الحوادث وتلبية طلبات الاكتشاف الإلكتروني للإجراءات القانونية.

بيانات السياسة

3.8.4.1 يجب تفعيل الأنظمة والأنشطة المناسبة لتمكين ضوابط التسجيل والمراقبة، وذلك بهدف إنشاء سجلات التدقيق والاحتفاظ بها والسماح بالمراجعات اللازمة والاحتفاظ بها.

3.8.4.2 يجب توفير قدرات الأدلة الجنائية ضمن وقت زمني مناسب للطلبات القانونية أو التنظيمية، بما يشمل الاستجابة لطلبات معلومات الاكتشاف الإلكتروني.

3.9 المرونة السحابية

3.9.1 أمن النسخ الاحتياطية واستمرارية الأعمال والتعافي من الكوارث

النسخة 1.0

دورة حياة الاعتماد

الفهم	التقييم	التطبيق	المراقبة	التعاون

قابلية تطبيق نموذج الخدمة

البنية التحتية كخدمة IaaS	المنصة كخدمة PaaS	البرمجيات كخدمة SaaS

أهدف السياسة

تلبية توقعات مستخدمي الخدمات السحابية لمتطلبات التوفّر والاستمرارية لخدمات السحابة.

بيانات السياسة

3.9.1.1 يجب أن يضمن مزوّد الخدمة جاهزيته لتلبية الأهداف التشغيلية والنسخ الاحتياطية والتعافي من الكوارث الخاصة بالمستخدمين.

3.9.1.2 يجب أن يضع مزوّد الخدمة خطة مفصّلة للتعافي من حالات الكوارث يجب اختبارها على فترات منتظمة.

القسم 4

التنفيذ

التنفيذ

يجب قراءة هذه السياسة وتفسيرها جنبًا إلى جنب مع إطار عمل مراقبة الامتثال لضوابط الأمن السحابي الواردة في الملحق 6.6، والذي ينص بالتفصيل على بيانات الضوابط اللازمة لدعم متطلبات السياسة.

سيتعاون مجلس الأمن السيبراني مع الجهات التنظيمية في القطاع والجهات الرائدة في الإمارات لضمان الامتثال لمتطلبات هذه السياسة.

يُتوقّع من مستخدمي الخدمة السحابية ومزوّدي خدمات الحوسبة السحابية إجراء تقييمات ذاتية للتحقّق من امتثالهم لمتطلبات هذه السياسة، وتقديم تقرير يتضمن النتائج التي توصّلوا إليها إلى الهيئات المختصة، وذلك مرةً كل عام أو عند الطلب.

لإحداث التغيير المنشود لإنجاح تعزيز الأمن السحابي، من الضروري التركيز على التثقيف والتوعية والتواصل. سيتعاون مجلس الأمن السيبراني مع مختلف المشاركين، ويشجّعهم على إعطاء الأولوية لتعزيز الأمن السحابي على المستويين الوطني والتنظيمي. كما سيعمل المجلس على تثقيف أصحاب المصلحة وتوعيتهم في حال تحديث العمليات والإجراءات أو إطلاق حلول جديدة لدعم كيفية تعاملهم مع المعلومات، سواء جمع المعلومات أو تحليلها أو نشرها أو واستخدامها على مستوى مختلف المؤسسات. وبالإضافة إلى ذلك، سيتعاون المجلس مع أصحاب المصلحة المشاركين للتعرّف على المؤسسات التي من شأنها المساهمة بمعلومات ذات قيمة لعملية ابتكار حلول إلكترونية جديدة للأمن السيبراني، وتعزيز ربط مختلف مصادر المعلومات ببعضها بغرض زيادة القدرات الشاملة للفضاء الإلكتروني في دولة الإمارات العربية المتحدة.

القسم 5

مراقبة الأداء

مراقبة الأداء

تحدّد السياسة الوطنية للأمن السحابي تدابير مراقبة وتقييم التقدّم المُحرز نحو الأهداف التالية:

- تعزيز الشفافية والإدارة الفعّالة للخدمات السحابية.
- تقديم إرشادات للتحسين و التدّخل لإجراء التصحيحات اللازمة عند الحاجة.
- قياس مدى جودة تطبيق مزوّدي خدمات الحوسبة السحابية والمستخدمين لمتطلبات الأمن السحابي.

القسم 6

الملاحق

6.1 الوثائق المرجعية

معايير وسياسات دولة الإمارات العربية المتحدة

يوضّح الجدول التالي معايير وسياسات دولة الإمارات العربية المتحدة التي تم الاستناد إليها في تعريف بيانات هذه السياسة.

الهيئة/الجهة	وثيقة
هيئة تنظيم الاتصالات والحكومة الرقمية	السياسة الوطنية لتنظيم قطاع الخدمات السحابية (مسودة)
هيئة تنظيم الاتصالات والحكومة الرقمية	قانون ضمان أمن المعلومات في دولة الإمارات العربية المتحدة.
هيئة تنظيم الاتصالات والحكومة الرقمية	سياسة الخدمات السحابية أولاً (مسودة)
مركز دبي للأمن الإلكتروني	المعيار الأمني لاعتماد مزوّدي الخدمات السحابية
مركز دبي للأمن الإلكتروني	نظام أمن المعلومات (النسخة الثانية)
حكومة الإمارات الذكية	إطار عمل البيانات الذكية في دولة الإمارات العربية المتحدة (النسخة الثانية)

6.1 الوثائق المرجعية

المعايير الدولية

يوضّح الجدول التالي المصادر الدولية المشار إليها في هذه الوثيقة.

الهيئة/الجهة	الوثيقة
المعهد الوطني للمعايير والتكنولوجيا	SP 800-145 - تعريف المعهد الوطني للمعايير والتكنولوجيا للحوسبة السحابية
المعهد الوطني للمعايير والتكنولوجيا	SP 500-322 - تقييم الخدمات السحابية على أساس NIST SP 800-145
ISO/IEC	17788 - نظرة عامة على الخدمات السحابية ومصطلحاتها
ISO/IEC	27001 - إدارة أمن المعلومات
ISO/IEC	27002 - أمن المعلومات والأمن السيبراني وحماية الخصوصية - ضوابط أمن المعلومات
ISO/IEC	27017 - دليل استخدام ضوابط أمن المعلومات استناداً إلى ISO/IEC 27002 للخدمات السحابية
ISO/IEC	27018 - دليل حماية معلومات التعريف الشخصية (PII) في وحدات التخزين السحابي العامة والتي تعمل كمعالجات لهذه المعلومات
ISO/IEC	19086 - إطار عمل اتفاقيات مستوى خدمة الخدمات السحابية
ISO/IEC	19941 - توافقية التشغيل وقابلية النقل للحوسبة السحابية
تحالف أمن الخدمات السحابية (CSA)	هيكلية الضوابط السحابية

6.2 قائمة الاختصارات

الهيئة/الجهة	الوثيقة
التطبيقات كخدمة	راجع البرمجيات كخدمة (SaaS)
مزوّدو الخدمات السحابية	مزوّد الخدمات السحابية: جهة (خاصة أو عامة) توفّر منصات أو بنية تحتية أو تطبيقات أو خدمات أمنية أو خدمات تخزين قائمة على السحابة إلى جهة/مؤسسة أخرى مقابل رسوم مالية محدّدة.
بنية الخدمة السحابية	بنية الخدمة السحابية هي البنية التي تمكّن التطبيقات من العمل كخدمة على الإنترنت.
مجلس التعاون الخليجي	مجلس التعاون الخليجي هو اتحاد سياسي واقتصادي للدول العربية المطلة على الخليج العربي والتي تقع في شبه الجزيرة العربية أو بالقرب منها، وتشمل البحرين والكويت وعُمان وقطر والمملكة العربية السعودية والإمارات العربية المتحدة.
البنية التحتية كخدمة IaaS	البنية التحتية كخدمة: نموذج خدمة يتم فيه استضافة البنية التحتية الخلفية لتكنولوجيا المعلومات اللازمة لتشغيل التطبيقات على السحابة على أساس اشتراك محدّد.
المنصة كخدمة PaaS	المنصة كخدمة: نموذج خدمة يتم فيه توفير نظام يتم استضافته على السحابة بهدف تطوير التطبيقات وتشغيلها . وإدارتها.
البرمجيات كخدمة SaaS	البرمجيات كخدمة: نموذج خدمة يتم فيه ترخيص البرامج المستضافة على السحابة وتوفيرها على أساس اشتراك محدّد.
مصفوفة الأدوار والمسؤوليات	مصفوفة الأدوار والمسؤوليات هي نموذج مشترك يستخدم لتحديد الأدوار والمسؤوليات لأعضاء المبادرات المشتركة بين الأقسام، حيث تتيح المصفوفة للأعضاء معرفة المجموعات المسؤولة عن الأنشطة بسهولة كما تحدّد الأفراد الذي يجب استشارتهم أو إبلاغهم.
اتفاقية مستوى الخدمة	اتفاقية تعاقدية بين مزوّد الخدمة والمستخدم (جهة حكومية) توضح متطلبات المستخدم، ويحدّد فيها مزوّد الخدمة مستوى مسؤوليات الخدمة والضمانات فيما يتعلق بالتوفّر والأداء ومستويات الدعم.
الجهاز الظاهري	نوع من الملفات (يسمى صورة) يظهر للمستخدم كبرنامج فعلي عند تشغيله. يُمكن تشغيل أو إيقاف برنامج التشغيل . الافتراضي حسب الحاجة، كما يُمكن تخزين التغييرات التي تم تنفيذها على برنامج التشغيل الافتراضي أثناء تشغيله على القرص بهدف تثبيتها.(مصدر التعريف: المعهد الوطني للمعايير والتكنولوجيا)
السحابة الافتراضية الخاصة	سحابة خاصة موجودة داخل سحابة مشتركة أو عامة.

6.3 التعاريف

الهيئة/الجهة	الوثيقة
التصنيفات	البيانات المفتوحة: • البيانات التي يتم مشاركتها ونشرها على الإنترنت بأقل حد من القيود. البيانات غير العلنية: • سري للغاية • حسّاس • سري
البيئة الاتحادية	عملية دمج البيانات أو الهويات عبر منصات متعددة، يُمكن إدارة البيئة الاتحادية بواسطة مزوّد الخدمة السحابية أو بواسطة وسيط خدمات سحابية.
الحوكمة	الضوابط والممارسات والعمليات التي تضمن تنفيذ السياسات.
التطبيقات المستضافة	تطبيق يتم تشغيله عن بُعد يتميز بأنه مبني على الإنترنت أو الويب.
السحابة الداخلية	نوع من أنواع السحابة الخاصة التي يتم توفير خدماتها من قبل قسم تكنولوجيا المعلومات للمستخدمين ضمن المؤسسة.
التقيد بمورد محدّد	الاعتماد على مورد معين (مزوّد خدمة سحابية) وصعوبة الانتقال من مزوّد خدمة سحابية إلى آخر.
المحاكاة الافتراضية	محاكاة البرنامج أو الجهاز والتي يُمكن استخدامها لتشغيل البرامج الأخرى.

6.4 الأدوار و المسؤوليات

يحدّد الجدول أدناه الجهات المعنية الرئيسية وأدوارها ومسؤولياتها فيما يتعلق بهذه السياسة.

أصحاب المصلحة	الأدوار والمسؤوليات
مجلس الأمن السيبراني لدولة الإمارات العربية المتحدة	بصفته الجهة المسؤولة عن هذه الوثيقة، سيقوم مجلس الأمن السيبراني بما يلي: • إصدار السياسة الوطنية للأمن السحابي ومراجعة الوثيقة دوريًا للتأكد من ملاءمتها. • التنسيق مع الجهات المعنية لتوزيع هذه السياسة على القطاعات والجهات الحيوية. • الإشراف على تنفيذ الأحكام المنصوص عليها في السياسة والتأكد من الالتزام بها.
الجهات الحكومية وقطاعات البنية التحتية الحيوية في الدولة	• الامتثال للمتطلبات الموضحة في السياسة الوطنية للأمن السحابي. • تطبيق أحكام السياسة على الخدمات المعمول بها. • التحقّق من تطبيق إجراءات التقصي وإجراء تقييمات المخاطر الموضحة في هذه السياسة.
مزوّدو الخدمات السحابية	• يجب على مزوّدي الخدمات السحابية الامتثال لمتطلبات الأمن الموضحة في السياسة.
مستخدمو الخدمات السحابية من الجهات غير الحكومية/ التي لا تتبع إلى قطاعات البنية التحتية الحيوية	• قد يختار هؤلاء المستخدمون الالتزام بمتطلبات الأمن المذكورة في السياسة لغايات تحسين وضعهم الأمني.

6.5 الخلاصة

نبذة عن الخدمات السحابية

وفقاً لما حدّده المعهد الوطني للمعايير والتكنولوجيا، تُعد الخدمات السحابية نموذجاً يوظف مجموعة مشتركة من موارد الحوسبة القابلة للإعداد، مثل: الشبكات والخوادم والتخزين والتطبيقات والخدمات، لتوفير إمكانية الوصول إلى الشبكة من كل مكان، حيث يُمكن الحصول على هذه الخدمة واستخدامها بسرعة وبأقل جهد إداري أو تفاعل مع مزوّد الخدمة. يتكون نموذج الخدمات السحابية من خمس خصائص أساسية وثلاثة نماذج خدمة وأربعة نماذج نشر.

خصائص الخدمات السحابية

- **الخدمة الذاتية عند الحاجة:** يُمكن للمستخدم توفير إمكانات الحوسبة من جانب واحد حسب الحاجة تلقائياً ودون الحاجة إلى أي تفاعل بشري.
- **وصول واسع للشبكة:** تتوفّر القدرات عبر الشبكة ويُمكن الوصول إليها من خلال الأجهزة القياسية مثل: الهواتف المحمولة والأجهزة اللوحية وأجهزة الكمبيوتر المحمولة ومحطات العمل.
- **تجميع الموارد:** يقوم مزوّد الخدمة السحابية بتجميع موارد الحوسبة المتاحة لخدمة مستخدمين متعددين، حيث يقوم بتخصيص الموارد المادية والافتراضية المختلفة وإعادة تخصيصها ديناميكيًا وفقاً لطلب المستخدم. عادةً لا يمتلك المستخدم أي معلومات - أو يمتلك قدراً بسيطاً من المعلومات - فيما يتعلق بموقع تخزين البيانات.
- **المرونة السريعة:** يُمكن توفير القدرات بشكل مرن بناء على الطلب، وقد يحدث ذلك تلقائياً في بعض الحالات، مما يمكّن من توسيع النطاق بسرعة نحو الخارج والداخل بطريقة غير محدودة.
- **الخدمة المُقاسة:** مراقبة استخدام الموارد وضبطها، ورفع التقارير بها لتوفير الشفافية لمزوّدي الخدمة والمستخدمين. وتتحكم الأنظمة السحابية تلقائياً في استخدام الموارد وفي عملية تحسينها من خلال الاستفادة من قدرتها على القياس.

6.5 الخلاصة

نماذج الخدمة السحابية

- **البرمجيات كخدمة (SaaS):** يمتلك المستخدم صلاحية استخدام تطبيقات المزوّد التي تعمل على البنية التحتية السحابية. والتي يُمكن الوصول إليها عن بُعد من أجهزة مختلفة، مثل: الويب أو واجهة البرنامج. ويملك المستخدم صلاحية استخدام التطبيق فقط ولا يستطيع إدارة أو التحكم في البنية التحتية السحابية الأساسية المستخدمة.
- **المنصة كخدمة (PaaS):** يمتلك المستخدم صلاحية نشر تطبيقات من تطويره أو تطوير غيره على البنية التحتية السحابية، على أن يتم تطويرها باستخدام لغات البرمجة والمكتبات والخدمات والأدوات التي يدعمها المزوّد. ومع ذلك، لا يستطيع المستخدم إدارة البنية التحتية السحابية الأساسية المستخدمة أو التحكم فيها.
- **البنية التحتية كخدمة (IaaS):** يمتلك المستخدم صلاحية توفير موارد الحوسبة الأساسية، مثل: المعالجة والتخزين والشبكات، لنشر وتشغيل البرامج، بما يشمل أنظمة التشغيل والتطبيقات.

6.5 الخلاصة

نماذج نشر السحابة

- **السحابة الخاصة:** يتم توفير البنية التحتية السحابية لتستخدم حصراً من قبل مؤسسة واحدة تتكون من مستخدمين متعددين (على سبيل المثال: وحدات الأعمال). وقد تكون مملوكة ومدارة ومشغلة من قبل المؤسسة أو طرف خارجي أو مزيج منهما، وقد تكون موجودة داخل المباني التابعة للجهة المالكة أو خارجها.
- **السحابة المجتمعية:** يتم توفير البنية التحتية السحابية بحيث تستخدم حصراً من قبل مجتمع معين من المستخدمين الذين ينتمون إلى مؤسسات لها اهتمامات مشتركة (على سبيل المثال، المهمة ومتطلبات الأمن والسياسة واعتبارات الامتثال). وقد تكون مملوكة ومدارة ومشغلة من قبل مؤسسة واحدة أو عدة مؤسسات داخل المجتمع أو طرف خارجي أو مزيج منهما، وقد تكون موجودة داخل المباني التابعة للجهة المالكة أو خارجها.
- **السحابة العامة:** يتم توفير البنية التحتية السحابية للاستخدام المفتوح من قبل عامة الناس. وقد تكون مملوكة ومدارة ومشغلة من قبل المؤسسة أو طرف خارجي أو مزيج منهما، وقد تكون موجودة داخل المباني التابعة للجهة المالكة أو خارجها.
- **السحابة الهجينة:** تتكون البنية التحتية السحابية من اثنين أو أكثر من البنى التحتية السحابية المتميزة (خاصة أو مجتمعية أو عامة) التي تبقى مملوكة من قبل جهات محدّدة ولكنها ترتبط ببعضها بواسطة تقنية قياسية أو مملوكة تمكن نقل البيانات والتطبيقات.

6.5 الخلاصة

الابتكار السحابي

شهد قطاع الخدمات السحابية نمواً كبيراً في الآونة الأخيرة، ومن المتوقع أن يستمر بالنمو على نحو أكبر مع ازدياد عدد الجهات التي تستخدم الخدمات السحابية ضمن مؤسساتها، معتمدة على نموذج واحد على الأقل من نماذج الخدمة السحابية الثلاثة. وبطبيعة الحال، تدفع الزيادة الملحوظة في اعتماد الخدمات السحابية النمو التكنولوجي في المجال، لذا أصبحت حوسبة الحافة والشبكات المعرفة بالبرمجيات والتحوّل إلى Omnicloud توجهات رئيسية ناشئة في الخدمات السحابية. ومع ذلك، يصاحب أي تكنولوجيا جديدة ظهور تهديدات أمنية جديدة، لذا فإنه من المهم فهم هذه التكنولوجيا على نحو كامل. بما يمكّن من تقييم التهديدات الناتجة والتخفيف من حدتها .

- **حوسبة الحافة Cloud Edge** - بناء شبكة موزعة تتكون من مراكز بيانات "دقيقة" للإبقاء على متطلبات الحوسبة والتخزين والشبكة في "حافة" الشبكة، مما يقلل من زمن الوصول.
- **الشبكة المعرفة بالبرمجيات (SDN)** - نهج جديد للشبكات يسمح بالإعداد الديناميكي للشبكات أثناء التنقل من خلال البرمجة.
- **Omnicloud والسحابة المتعدّدة Multicloud** - إزالة الحواجز بين البنى التحتية السحابية المختلفة التي تؤدي إلى التقيد بموردين محددين وتمكين التعاون عبر جميع الأنظمة الأساسية.