وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

سياسة تأمين الحوسبة السحابية

الإصدار: 1.0

المؤلف: قسم إدارة مخاطر الأمن السيبراني

تصنيف الوثيقة: عام

تاريخ النشر: اغسطس 2018

تاريخ الوثيقة:

التاريخ	وصف الاصدار	الاصدار
مارس 2018	نشر النسخة الاولى 1.0	1.0
ابريل 2016	تغيير العلامات المؤسسية	1.1
يونيو 2017	تمييز الاسئلة الإجبارية	1.2
أغسطس 2018	تعديل النسق و تغيير شعار الوزارة	1.3

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

قائمة المحتويات

1- التكليف القانوني

ينص القرار الأميري رقم (8) لسنة 2016 بشأن تحديد تفويض وزارة المواصلات والاتصالات (المشار إليها فيما بعد باسم "الوزارة"") على أن تتمتع وزارة المواصلات والاتصالات بسُلطة الإشراف على قطاعات تكنولوجيا المعلومات والاتصالات داخل دولة قطر وتنظيمها وتطويرها بطريقة متوافقة مع متطلبات أهداف التنمية الوطنية، وذلك بهدف إيجاد بيئة مناسبة للمنافسة العادلة ودعم تطوير وتحفيز الاستثمار في تلك القطاعات؛ ومن أجل تأمين وزيادة كفاءة المعلومات والهياكل الأساسية التكنولوجية وتنفيذ برامج الحكومة الإلكترونية والإشراف عليها، بالإضافة إلى تحسين الوعي المجتمعي بأهمية تكنولوجيا المعلومات والاتصالات لتحسين حياة الفرد والمجتمع المحلي وبناء مجتمع قائم على المعرفة والاقتصاد الرقمي.

وتنص المادة (22) من القرار الأميري رقم (8) لسنة 2016 على دور الوزارة في حماية الهيكل الأساسي للمعلومات الوطنية الهامة عن طريق اقتراح وإصدار السياسات والمعايير وضمان الامتثال.

وقد أُعدت المبادئ التوجيهية الماثلة بمراعاة القوانين المعمول بها حاليًا في دولة قطر. وفي حالة نشوء أي اختلاف بين هذه الوثيقة وقوانين دولة قطر، تعطى الأسبقية لقوانين دولة قطر. ولذلك الغرض يُحذف ذلك البند من هذه الوثيقة، على أن تظل بقية الوثيقة سارية المفعول بدون التأثير على باقي الأحكام. وفي تلك الحالة ستكون التعديلات ضرورية لضمان الامتثال للقوانين ذات الصلة المعمول بها داخل دولة قطر.

2- مقدمة

تتيح الحوسبة السحابية الكثير من الفوائد الممكنة للجمهور وللجهات الحكومية، ومن بين تلك الفوائد القابلية للتوسع ،والمرونة، والأداء العالي، والجهد الإداري الأقل، بالإضافة إلى التكلفة الاقتصادية وسرعة الانتقال والوقت الأسرع للوصول إلى السوق وكذلك فرص الابتكار الجديدة.

وتسعى هذه الوثيقة إلى تحقيق تفهم وإدارة والسيطرة على المخاطر التي تؤثر بشكل رئيسي على السرية والأمن والمرونة المتعلقة باستخدام هذه الإمكانية.

وعادةً ما تفرض إدارة الأمن والمرونة في بيئات تكنولوجيا المعلومات التقليدية تحديات بالنسبة للجهات الحكومية، وتطرح الحوسبة السحابية بعض التحديات الإضافية.

على سبيل المثال:

- غياب التعريفات الواضحة المتعلقة بالسحاب والخدمات والتصميمات المختلفة المرتبطة به.
- غياب الاعتماد والتوثيق والمعايير المتعلقة بأمن السحاب، والمواءمة غير المكتملة مع معايير الأمن المستخدمة في الوقت الحالي.
- غياب لغة ومنهجية شراء واضحة لاختيار خدمة السحاب الأكثر ملاءمة.
- غياب فهم واضح لآثار ونتائج الحوسبة السحابية فيما يتعلق بنقل البيانات بين الدول.
- ضمان الالتزام بالقوانين واللوائح الوطنية.

الأكثر أهمية هو كيف يمكننا استيعاب التحول في التوازن بين المسؤولية والمساءلة بالنسبة للوظائف الرئيسية مثل الحوكمة والرقابة على البيانات وعمليات تكنولوجيا المعلومات، وفي بعض الأحيان جودة وتوفر الاتصال بشبكة الانترنت الذي يعد عنصراً أساسياً للخدمة.

إن الغرض من هذه السياسة هو تقديم نظرة عامة على الحوسبة السحابية وما تنطوي عليه من تحديات تتعلق بالأمن والخصوصية . وتناقش هذه الوثيقة التهديدات والمخاطر التكنولوجية ووسائل الحماية لبيئات السحاب ،كما تسعى لتوفير الرؤية والأفكار اللازمة لمساعدة صناع القرار فيما يتعلق بتكنولوجيا المعلومات والاتصالات في اتخاذ قرارات مدروسة عن طريق توفير أدوات مثل الاستبيانات التفصيلي التي يمكن استخدامها لتقييم عروض مزود خدمة السحاب .

3- التعاريف

- **الجهات**: الوزارات والمجالس العليا وغيرها من الجهات الحكومية ومنظمات القطاع العام في قطر.
- **الافتراضية المتقدمة**: تتم عندما يكون لدى البنية التحتية الافتراضية لتكنولوجيا المعلومات والاتصالات قدرات إدارة مميكنة.
- **التطبيق كخدمة (Aaas)**: انظر البرنامج كخدمة(SaaS).
- **السحاب**: مصطلح يستخدم للشبكات العالمية، وقد استخدم في الأصل للإشارة إلى الشبكة الهاتفية ولكن يشيع استخدامه الآن في الإشارة لشبكة الانترنت.
- **وسيط السحاب**: جهة تقوم بإنشاء وإدارة العلاقات مع عدة مزودي خدمة السحاب. وتعمل كحلقة ربط بين مزودي خدمة السحاب وعملاء خدمة السحاب. ولا يمتلك وسيط السحاب مصادر سحاب خاصة به.
- **Cloud bursting**: أسلوب يستخدمه السحاب الهجين (انظر السحاب الهجين) لتوفير موارد إضافية للسحاب الخاص عند الحاجة. فإذا زاد عبء العمل عن سعة السحاب الخاص، يخصص السحاب الهجين موارد إضافية بشكل تلقائي من خلال هذا الأسلوب.
- **خدمات الحوسبة السحابية**: انظر البند رقم 4-4.
- **نظام تشغيل السحاب**: نظام تشغيل مصمم خصيصاً للعمل ضمن بنية تحتية سحابية ويقدم للمستخدم على الشبكة.
- **التصميم السحابي**: تصميم لتكنولوجيا المعلومات يتوائم تماماً مع مكونات قائمة على السحاب.
- **القابلية للنقل عبر السحاب**: القدرة على نقل التطبيقات والبيانات من أحد مزودي خدمات السحاب إلى مزود آخر لخدمات السحاب (فيما يتعلق بالاعتماد على مورد واحد).
- **مزود خدمة السحاب**: جهة (عامة أو خاصة) تقدم منصات أو بنى تحتية أو تطبيقات أو أمن أو خدمات حفظ قائمة على السحاب لجهة/ منظمة أخرى. وعادةً ما تقدم هذه الخدمة لقاء رسوم.
- **خدمات السحاب**: انظر البند رقم 4-4.
- **تصميم خدمة السحاب**: تصميم تعمل فيه التطبيقات كخدمات على شبكة الإنترنت.
- **التخزين على السحاب**: خدمة تتيح للعملاء حفظ البيانات بنقلها على شبكة الإنترنت/ شبكة اتصال واسعة (WAN) لنظام حفظ آخر يديره طرف ثالث.
- **استخدام موارد السحاب**: استخدام خدمة السحاب بدلاً من خدمة تكنولوجيا المعلومات التقليدية مثل تعهيد حفظ البيانات إلى جهات خارجية.
- **ربط شبكات السحاب**: ربط عدة بيئات حوسبة سحابية.
- **برنامج السحاب**: برنامج يتيح إنشاء أو استخدام أو تشغيل أو إدارة التطبيقات في السحاب.
- **سحاب المجتمع**: انظر البند رقم 4-6.

- **الخدمة الذاتية للعميل:** خاصية تتيح لعملاء السحاب استخدام وإدارة وإنهاء الخدمات لأنفسهم دون اللجوء لمزود الخدمة.
- **ملصقات التصنيف:**
  - **غير مصنفة أو عامة أو بدون ملصق:** معلومات عامة.
  - **داخلية:** للاستخدام الداخلي للجهة الحكومية؛ أي مادة يتسبب الإفصاح عنها في ضرر بسيط إلى متوسط للطرف المتأثر.
  - **اطلاع محدود:** قَصر الاطلاع على مستخدمين أو أدوار أو مجموعات مستخدمين محددة؛ أي مواد يتسبب الإفصاح عنها في ضرر جدي للطرف المتأثر.
  - **محظورة:** معلومات سرية مع قصر الاطلاع على مجموعة صغيرة جداً من الأشخاص؛ أي مواد يتسبب الإفصاح عنها في ضرر بالغ للطرف المتأثر.
- **التجميع:** عملية تجميع البيانات أو الهويات عبر عدة منصات، ويمكن أن يدار التجميع من قبل مزود خدمة سحاب أو وسيط خدمة سحاب.
- **الحوكمة:** الضوابط والممارسات والعمليات التي تتأكد من الالتزام والتقيد بالسياسات.
- **حوسبة الشبكات:** تخصيص موارد عدة أجهزة حاسب آلي في شبكة واحدة لمواجهة مشكلة واحدة في نفس الوقت.
- **مجلس التعاون الخليجي:** مجلس التعاون لدول الخليج العربية وهو اتحاد سياسي واقتصادي للدول العربية والتي لها حدود على الخليج العربي وتقع في شبه الجزيرة العربية أو بالقرب منها؛ وهي، تحديداً، البحرين والكويت وعمان وقطر والمملكة العربية السعودية والإمارات العربية المتحدة.
- **الأجهزة أو البنية التحتية كخدمة (Iaas):** انظر البند بعنوان: الأجهزة أو البنية التحتية كخدمة.
- **تطبيق مستضاف:** تطبيق يعتمد على شبكة الإنترنت ويعمل عن بعد.
- **السحاب الداخلي:** نوع من السحاب الخاص تقدم خدماته من إدارة لتكنولوجيا المعلومات للعاملين في الجهة التي تضم تلك الإدارة.
- **تجميع الموارد المستقلة عن الموقع: هو** نوع من تجميع الموارد يتيح لمزود خدمة السحاب تعيين الموارد (المادية والافتراضية) للعميل، ولا تعتمد تلك الموارد على الموقع.
- **البرنامج الوسطي:** برنامج يقع بين التطبيقات وأنظمة التشغيل، وعادة ما يتكون من خدمات تتيح وتدعم التشغيل في تصميم موزع، ومثال ذلك البيانات على إحدى قواعد البيانات التي يمكن الوصول إليها من خلال قاعدة بيانات أخرى على منصة مختلفة.
- **وزارة المواصلات والاتصالات:** وزارة المواصلات والاتصالات في دولة قطر.

- **سياسة تأمين المعلومات الوطنية:** سياسة تأمين المعلومات الوطنية هي مجموعة كاملة من ضوابط الأمن الصادرة من مركز كيوسرت، قطاع الأمن التابع لوزارة المواصلات و الاتصالات.
- **المنصة كخدمة (PaaS):** انظر البند رقم 4-6.
- **الفريق القطري للاستجابة لطوارئ الحاسبات (كيوسرت):**(إحدى مبادرات وزارة المواصلات والإتصالات التي تعنى بقضايا الأمن السيبراني).
- **مصفوفة المسؤولية والمساءلة والتشاور والإعلام (RACI):** نموذج شائع يستخدم لتحديد أدوار ومسؤوليات أعضاء المبادرات ذات الوظائف المتداخلة. وتتيح المصفوفة للأعضاء سهولة تحديد المجموعات المسؤولة والتي ستساءل عن الأنشطة وتلك التي يجب التشاور معها أو إعلامها.
- **البرنامج كخدمة (SaaS):** انظر البند رقم 4-6.
- **اتفاقية مستوى الخدمة:** اتفاق تعاقدي بين مزود خدمة وعميل (إحدى الجهات الحكومية) يحدد متطلبات العميل ،وينص على مسؤوليات وضمانات مزود الخدمة عن مستوى الخدمة فيما يتعلق بالتوفر والأداء والدعم.
- **الاعتماد على مورد واحد:** الاعتماد على مورد معين (مزود خدمة سحاب) وصعوبة التحول من مزود خدمة سحاب إلى آخر.
- **آلة افتراضية:** ملف (يعرف عادةً باسم "الصورة") يظهر للمستخدم عند استخدامه كآلة حقيقية. ويمكن تشغيل أو وقف الآلة الافتراضية حسب الحاجة، كما يمكن حفظ التغييرات التي تتم على الآلة الافتراضية أثناء عملها على قرص لجعلها مستمرة (مصدر التعريف: NIST).
- **التحول إلى الافتراضية:** محاكاة البرنامج أو الجهاز بحيث يمكن أن يعمل عليه برنامج آخر.
- **السحاب الافتراضي الخاص:** سحاب خاص يوجد ضمن سحاب مشترك أو عام.

4- ما هي الحوسبة السحابية

الحوسبة السحابية: هي نموذج لتوريد وتوفير تكنولوجيا المعلومات والاتصالات لإتاحة اتصال الشبكة بمجموعة مشتركة من مصادر الحوسبة القابلة للتهيئة على نحو ملائم عند الطلب (مثل الشبكات والخوادم والتخزين والتطبيقات والخدمات) التي يمكن توفيرها وطرحها بأقل جهد إدارة أو تعامل مع مزود الخدمة.

وتتألف الحوسبة السحابية من خمس خصائص رئيسية وثلاثة نماذج خدمة وأربعة نماذج استخدام.

البنية التحتية السحابية: هي مجموع الأجهزة والبرامج التي تتيح تفعيل الخصائص الرئيسية الخمس للحوسبة السحابية .ويمكن أن ينظر إلى البنية التحتية السحابية على أنها تحتوي على طبقة مادية وطبقة تجريدية. وتتألف الطبقة المادية من الأجهزة الضرورية لدعم خدمات السحاب التي يتم توفيرها، وتتألف الطبقة التجريدية من البرامج المستخدمة على الطبقة المادية.

4-1خصائص الحوسبة السحابية:

- الخدمة الذاتية عند الطلب: يمكن للعميل تجهيز عدة قدرات حوسبة حسب الحاجة. ويمكن أن يتم ذلك على شبكة الانترنت بشكل كامل.
- الاتصال العام بالشبكة: تتوفر الخدمات على الشبكة، ويكون الاتصال مدعوماً من خلال عدة منصات (مثل الهواتف النقالة والحواسب اللوحية والمحمولة ومحطات العمل).
- تجميع الموارد: يتم تجميع مصادر الحوسبة التابعة لمزود خدمة السحاب لخدمة عدة مستهلكين في نفس الوقت ،ويمكن للمستهلكين أن يكونوا في أي مكان في العالم. وتشمل أمثلة المصادر التخزين والمعالجة والذاكرة والنطاق العريض للشبكة.
- القابلية للتوسع: يمكن أن يتم تجهيز وطرح مصادر السحاب بسهولة. وبالنسبة للمستهلك، قد تبدو المصادر المتاحة للتجهيز غير محدودة، ويمكن تخصيصها بأي مقدار وفي أي وقت.
- الخدمة المدروسة: تتحكم أنظمة السحاب في استخدام المصادر وتحقيق الأداء الأمثل لها بشكل تلقائي. ويمكن مراقبة استخدام المصادر والتحكم فيه والإبلاغ عنه؛ مما يوفر الشفافية لكل من المزود والمستهلك.

4-2 نماذج خدمة الحوسبة السحابية

- البرنامج كخدمة: يتيح هذا النموذج للجهة احكومية إمكانية استخدام تطبيقات مزود خدمة السحاب التي تعمل على بنية تحتية سحابية. ويمكن الوصول إلى تطبيقات البرنامج على شبكة الانترنت عبر واجهة انترنت أو عبر تطبيق جهاز كمبيوتر مكتبي. ولا يكون للمستهلك أي تحكم في ضبط الأجهزة الأساسية .
- المنصة كخدمة: يتيح هذا النموذج للجهة الحكومية إمكانية استخدام أو تثبيت تطبيق قامت الجهة بإنشائه أو شرائه على البنية التحتية السحابية بشرط أن يكون قد تم إنشاء التطبيق باستخدام لغات برمجة ومكتبات وخدمات وأدوات يدعمها مزود خدمة السحاب. ولا يكون للمستهلك تحكم في ضبط الأجهزة الأساسية أو التخزين أو الشبكة أو نظام التشغيل أو مستويات الإدارة.
- البنية التحتية كخدمة: يتيح هذا النموذج للجهة الحكومية إمكانية استخدام موارد المعالجة والتخزين والشبكات وغير ذلك من موارد الحوسبة بحيث يتمكن المستهلك من تثبيت وتشغيل أي برنامج بما في ذلك أنظمة تشغيل وتطبيقات. ولا تدير الجهة الحكومية البنية التحتية السحابية الأساسية أو تتحكم فيها، ولكنها تتحكم في أنظمة التشغيل والتخزين والتطبيقات المستخدمة.

4-3 نماذج الاستخدام:

- السحاب الخاص: تخصص البنية التحتية السحابية للاستخدام الحصري من قبل منظمة واحدة/ جهة حكومية واحدة تتألف من عدة مستهلكين (كالإدارات المختلفة). ويمكن امتلاكها وإدارتها وتشغيلها من قبل المنظمة أو طرف ثالث، أو بالاشتراك بين المنظمة وطرف ثالث، كما يمكن أن توجد في المقر أو خارجه، أو داخل البلاد أو خارجها.

- سحاب الجماعة: تخصص البنية التحتية السحابية للاستخدام الحصري من قبل جماعة معينة/ قطاع معين من المستهلكين من منظمات تشترك في طبيعة العمل والالتزامات (كأن يكون لها نفس الرسالة، ونفس متطلبات أمن تكنولوجيا المعلومات والاتصالات، ونفس الاعتبارات القانونية والاعتبارات المتعلقة بالتزام القطاع). ويمكن امتلاك هذه البنية التحتية السحابية وإدارتها وتشغيلها من قبل واحدة أو أكثر من المنظمات التي تضمها تلك الجماعة ،أو من قبل طرف ثالث، أو بالاشتراك بين المنظمات وطرف ثالث، كما يمكن أن توجد في المقر أو خارجه، أو داخل البلاد أو خارجها (مثل شبكة الحكومة القطرية).
- السحاب العام: تخصص البنية التحتية السحابية للاستخدام المفتوح من قبل أي منظمة. ويمكن تملكها وإدارتها وتشغيلها من قبل منظمات خاصة أو عامة، أو أي خليط بين تلك المنظمات. وتوجد هذه البنية التحتية في مقر مزود خدمة السحاب.
- السحاب الهجين: البنية التحتية لهذا السحاب عبارة عن خليط من بنيتين تحتيتين مختلفتين أو أكثر (بنية تحتية خاصة، أو بنية تحتية خاصة بجماعة، أو بنية تحتية عامة) تظل كيانات منفصلة، ولكنها مرتبطة ببعضها البعض بتكنولوجيا موحدة أو خاصة تتيح قابلية البيانات والتطبيقات للنقل (مثل موازنة الحمل بين أنواع السحاب) .

ويلخص الجدول التالي المفاهيم الرئيسية للبندين رقم 4-4 ورقم 4-6

	جهة إدارة* البنية التحتية	جهة ملكية البنية التحتية	موقع البنية التحتية	الأطراف التي يحق لها الوصول إلى البنية التحتية واستهلاكها
عامة	مزود خارجي	مزود خارجي	خارج الموقع	أي شخص
خاصة/ مخصصة لجماعة	الجهة أو مزود خارجي	الجهة أو مزود خارجي	في الموقع أو خارجه	الموثوقون**
هجين	الجهة و مزود خارجي	الجهة و مزود خارجي	في الموقع وخارجه	الموثوقون وغيرهم

* تشمل الإدارة: الحوكمة والعمليات والأمن والالتزام... الخ

** المستهلكون الموثوقون: هم الذين يعتبرون جزءً من الجهة من ناحية قانونية.

4-4لماذا هناك حاجة لسياسة قطرية لأمن الحوسبة السحابية؟

على مدى السنوات، أصبحت منظمات تكنولوجيا المعلومات والاتصالات والمهنيين في مجال تكنولوجيا المعلومات والاتصالات في قطر على دراية جيدة بالمخاطر وممارسات الحوكمة والمتطلبات القانونية المصاحبة لبيئات تكنولوجيا المعلومات التقليدية القائمة على أجهزة الكمبيوتر المكتبية. إلا أنه نظراً للتصميم الفريد وطبيعة الموقع الخارجي العابر للحدود لخدمات السحاب، يتعين معالجة متطلبات خصوصية وأمن المعلومات الشخصية (مشروع قانون خصوصية وحماية معلومات قطر) وكذلك متطلبات أمن البيانات الحكومية (سياسات تأمين المعلومات الوطنية) وعملياتها واتصالاتها من منظور مختلف.

5- المخاطر المحتملة للحوسبة السحابية

تبعاً لنموذج السحاب الذي يقع عليه الاختيار، يكون من الضروري تفهم المخاطر التالية والحد منها.

الموضوع	التفسير
تصميم التطبيق	☐ تخصيص أقل، إذ قد يؤدي ذلك إلى زيادة التعقيدات عند التكامل مع الأنظمة المتوارثة القائمة. ☐ بعض التطبيقات التي تتطلب الوصول إلى البيانات آني (مثل بعض تطبيقات قواعد البيانات) قد تحتاج إلى المراجعة لاستيعاب فترة انتظار الشبكة لتجنب الأخطاء الناتجة عن المدخلات والمخرجات. ☐ بعض نماذج تراخيص البرامج قد تحتاج إلى المراجعة لاستيعاب الاستخدامات الفعالة للسحاب.
التصميم	☐ قبل اتخاذ قرار الانتقال إلى بيئة السحاب، يجب على الجهة الحكومية للدولة أن تقيم تأثير ذلك على عمليات النشاط لتجنب أي عوائق فنية.
استمرارية العمل	☐ التطبيقات/ الخدمات التي لم تكن تتطلب الوصول إلى الشبكة قبل ذلك للعمل كما ينبغي، سوف تتأثر بفقدان الاتصال بالإنترنت و/أو الشبكة الواسعة (WAN). ويجب مراجعة وتوثيق خطط استمرارية العمل والتعافي من الكوارث بشكل كامل لاستيعاب التصميم الجديد.
موقع البيانات	☐ نظرًا للطبيعة الديناميكية للسحاب، قد لا تكون الجهة الحكومية على علم تام بالموقع الفعلي للمعلومات الخاصة بها في نقطة محددة من الوقت.

التمويل	☐ نظراً لنموذج السداد الخاص ببعض خدمات السحاب، قد تحتاج عملية إعداد الموازنة التقديرية للمصروفات الرأسمالية لتكنولوجيا المعلومات والاتصالات إلى إعادة تخطيط بحيث تصنف كمصروفات تشغيلية بدلاً من مصروفات رأسمالية. ☐ بعض نماذج تراخيص البرامج قد تحتاج إلى المراجعة لاستيعاب الاستخدامات الفعالة للسحاب.
الجوانب القانونية والتنظيمية	☐ يجب أن يتوفر لدى الجهة الحكومية القدرة على/ضمان أن تجد معلوماتها و أن تصل إليها في أي وقت. ☐ يجب أن تكون الجهات التابعة للدولة على دراية بكافة التشريعات والمتطلبات التنظيمية القطرية، بما في ذلك على سبيل المثال لا الحصر سياسة تأمين المعلومات الوطنية، وقانون الاتصالات رقم 64 لسنة 4003 وقانون حماية وخصوصية البيانات.
اتفاقيات مستوى الخدمة	☐ تحتاج الجهات الحكومية إلى ضمان تحقيق مستويات الخدمة المتفق عليها. كما يجب أن تضمن تلك الجهات وجود اتفاقيات مكتوبة لمستوى الخدمة مع مزودي خدمات السحاب.
الخصوصية والسمعة	☐ يجب أن تكون الجهات الحكومية مدركة للمخاطر المرتبطة بأي كشف عن المعلومات الحكومية أو الشخصية يحدث من خلال وصول طرف ثالث إلى تلك المعلومات. ☐ يجب أن تكون الجهات الحكومية على علم بأنه في حالة حدوث خرق للبيانات فإن ذلك سيؤثر تأثيراً سلبياً على سمعة الجهة، وربما يمتد الضرر إلى الحكومة ككل.
رأس المال البشري	☐ الانتقال إلى التصميم السحابي يعني طلب أقل على مسؤولي دعم الأجهزة والأنظمة المخصصة لمنتجات بعينها، وطلب أعلى على مهندسي النظم ومديري البرامج ومسؤولي الأمن والخصوصية ومحللي البيانات ومصممي ومطوري التطبيقات .
الأمن	☐ يجب أن تكون الجهات الحكومية مدركة بأنها ستظل مسؤولة عن أمن المعلومات حتى عند الاعتماد على مزود خدمات سحابية.

	☐ يجب أن تدرس الجهات الحكومية قابلية البيانات للنقل في حالة إخفاق مزود خدمة السحاب. كما يجب أن يؤخذ الوضع المالي لمزود خدمة السحاب في الاعتبار لتقليل التغيرات الناتجة عن الإخفاق المالي لمزود خدمة السحاب. ☐ يجب أن تضمن الجهات الحكومية وجود عقود بينها وبين مزود خدمة السحاب تصف ضوابط الأمن.
المعايير	☐ يجب أن تجري الجهات الحكومية فحصاً شاملاً لشهادات التزام مزود خدمة السحاب، مع الانتباه الخاص إلى نطاق وصلاحية تلك الشهادات.

6- مسؤولية الجهة إزاء النماذج المختلفة للسحاب

اعتماداً على نموذج السحاب الذي يتم اختياره، يمكن لأي جهة تشترك في خدمة الأجهزة أو البنية التحتية كخدمة (IaaS) أن تحتفظ بالسيطرة الكاملة، وتتحمل بالتالي المسؤولية ،عن الأمن والصيانة المستمرين لكافة أنظمة التشغيل والتطبيقات وعمليات التهيئة الافتراضية (بما في ذلك المشرف الافتراضي وأجهزة الأمن الافتراضي) والبيانات. وفي هذه الحالة، يكون مزود خدمة السحاب مسؤولاً عن صيانة الشبكة الملموسة الأساسية وأجهزة الحوسبة.

ويوضح الشكل التالي كيف تتباين مسؤولية كل جهة تبعاً لنموذج السحاب.

مثال لكيفية اختلاف النطاق والمسؤولية تبعا لنوع خدمة السحاب:

مسؤولية مستهلك خدمات السحاب	
مسؤولية مزود خدمات السحاب	

نطاق المسؤولية	نوع خدمة السحاب		
	البنية التحتية كخدمة (IaaS)	المنصة كخدمة (PaaS)	البرنامج كخدمة (SaaS)
البيانات			
البرامج، تطبيقات المستخدم			

أنظمة التشغيل، قواعد البيانات			
البنية التحتية الافتراضية (برنامج إدارة الافتراضية hypervisor، التطبيقات الافتراضية، المديرين الافتراضيين VMs، الشبكات الافتراضية .. الخ)			
أجهزة الكمبيوتر والشبكات (المعالج، الذاكرة، التخزين ، الربط بالكابلات ... الخ)			
مركز البيانات (مرفق مادي)			

المصدر: إرشادات التحول إلى الافتراضية وفق معيار أمن بيانات بطاقات الدفع (PCI-DSS)، 4022

7- المحركات الرئيسية للاستخدام

تطرح الحوسبة السحابية العديد من المزايا والقدرات التي يمكن اعتبارها محفزات للاستخدام بالنسبة للجهات الحكومية.

المحفز	المزايا
القيمة مقابل المال	☐ تقليل التكرار وتخفيض التكلفة من خلال الدمج وتجميع الموارد والمشاركة فيها. ☐ السماح بالدفع "المتحكم فيه" المتاح من خلال نموذج "ادفع بقدر ما تستخدم". ☐ توفير الطاقة والحفاظ على البيئة. ☐ جهد إداري أقل يسمح للجهة الحكومية بالتركيز على الأهداف الرئيسية وتحسين العمليات.
المرونة	☐ التجهيز والاستخدام السريع للخدمة والتوسع حسب الطلب.
دعم التشغيل	☐ درجة حضور عالية ودعم مهني على مدار الساعة.
الأمن	☐ السحاب عبارة عن منصة أكثر وحدة وتناغماً تتيح ميكنة إدارة الأمن)مثل اختبار الثغرات، وعمليات التدقيق، وإدارة التحديثات(والتنفيذ المستمر لأفضل الممارسات. ☐ تصمم منصات السحاب وتدار لتوفير عنصر الحضور والتواجد.

	▯ استخدام أنظمة السحاب تبعاً لدرجات المشروعات يمكن أيضاً أن تعزز الأمن. فقد استثمر موردون كبار ناضجين ومن مستوى مشروعات السحاب في أنظمة وعمليات متقدمة وموارد بشرية قادرة على توفير مستوى عالمي من الأمن. ▯ إن حجم التشغيل يعزز الأمن ويقلل التكاليف للبناء والإدارة في السحاب مقارنةً بقيام الجهات بالتنفيذ على مستوى فردي. ▯ ونظراً لحجم ومستوى أعمالهم، يمكن لموردي خدمات السحاب الكبار والناضجين تعيين موظفين متخصصين، وهو ما يعتبر أمراً غير اقتصادي بالنسبة للجهات الفردية.
الذكاء	▯ نظراً للمستويات والموارد التي يتم تجميعها والمشاركة فيها في السحاب، والتي يوفرها مورد خدمات السحاب (سواءً كان شريكاً أو جهة)، يمكن إنتاج سيناريوهات جديدة ومبتكرة بجزء قليل جداً من التكلفة فيما لو تم التنفيذ بصورة فردية.

8- النطاق والتطبيق

تنطبق هذه الوثيقة على كافة الجهات الحكومية في الحكومة القطرية التي تستخدم أو تخطط لاستخدام خدمات الحوسبة السحابية. كما يمكن أيضاً اعتبار الوثيقة بمثابة دليل أمني لقطاع الاتصالات وتكنولوجيا المعلومات ككل في دولة قطر.

9- نصوص السياسة

يجوز للجهات التابعة للحكومة القطرية اختيار خدمات سحابية محلية أو بإحدى دول مجلس التعاون الخليجي **إذا** أثبتت التزاماً بالمتطلبات الأمنية المنصوص عليها في هذه الوثيقة. ولا يجوز للجهات التابعة للحكومة القطرية استخدام مزود خدمات سحاب خارج الولاية القانونية أو الحدود الجغرافية لدولة قطر ودول مجلس التعاون الخليجي ما لم تكن استحقاقات الخدمة مطابقة لقوانين خصوصية وحماية المعلومات، وسياسة تأمين المعلومات الوطنية (وخاصة سياسة تصنيف البيانات) وغير ذلك من القوانين والتشريعات الحاكمة والمعمول بها.

10- سياسة أمن السحاب

10-1 غرض السياسة

يتمثل الغرض من هذه السياسة في التأكد من أن تجهيز خدمة السحاب يتفق مع ويلبي متطلبات الأعمال والأمن والقوانين واللوائح ذات الصلة.

10-2 السياسة والضوابط الأساسية

10-2-1 وثيقة سياسة أمن الحوسبة السحابية	يتعين اعتماد وثيقة سياسة أمن الحوسبة السحابية لكل جهة من الإدارة العليا، ويتم نشرها وتوزيعها على جميع الموظفين والأطراف الخارجية ذات الصلة سواءً كجزء من سياسة أمن المعلومات للجهة أو كسياسة منفصلة. ويجب أن تحدد السياسة الأهداف والأغراض التي تحكم خدمة الحوسبة السحابية.
10-2-2 قيادة برنامج الأمن	يتم تحديد الإدارة العليا المسؤولة عن سياسة أمن الحوسبة السحابية بالاسم والمسمى الوظيفة ورقم هاتف العمل وعنوان العمل وتاريخ التكليف. كما يجب توثيق التغييرات التي تطرأ على الإدارة العليا في غضون ثلاثين (60) يوماً تقويمياً من تاريخ سريان التغيير.
10-2-3 مراجعة سياسة الأمن	يتعين مراجعة سياسة الأمن بشكل دوري على فترات مقررة، أو حدثت تغييرات مؤثرة، وذلك لضمان استمرار ملاءمتها وكفايتها وفاعليتها. على سبيل المثال: تعديلات التصميم، أو تعديلات نموذج الخدمة أو تحديثات الخدمة أو تغيير مزود خدمة السحاب.
10-2-4 إكمال وتقديم استبيان ضوابط أمن السحاب	تلتزم الجهة الحكومية بعدم توقيع أي اتفاق مع مزود خدمة السحاب قبل إكمال واجتياز كافة الضوابط الإلزامية في (**استبيان تقييم مزود خدمة السحاب**) (انظر الملحق أ).
10-2-5 تدقيق مزود خدمة السحاب	تلتزم الجهة الحكومية بالتأكد من اجتياز مزود خدمة السحاب لكافة المتطلبات الأمنية الضرورية وفقاً لتقييم يجريه مدقق مستقل.

11- سرعة الأداء

11-1 غرض السياسة

تعد سرعة الأداء أحد أُسس وأبرز خصائص الحوسبة السحابية؛ ويقصد بذلك التحسينات والتحديثات والتعديلات السريعة التي يمكن تطبيقها على منتجات وخدمات السحاب. إن هذا الوقت الأقل والأقصر في الأداءايعني وقتاً أقل لإكمال تقييم للمخاطر على نحو صحيح ولتقدير الآثار والنتائج الأمنية .

11-2 السياسة والضوابط الأساسية

11-2-1 التحديثات والإصدارات	تخضع دوائر التحديث والإصدار الملائمة التي تؤثر على الخصائص الأمنية مع مزود خدمة السحاب لموافقة الجهة الحكومية وفق ما تحدده فرق العمل التابعة للجهة الحكومية (مثل الجوانب الأمنية واستمرارية العمل والجوانب القانونية والحوكمة .... الخ.)
11-2-2 الممارسات السريعة لإدارة مخاطر مزود خدمة السحاب	ستقوم الجهة الحكومية بطلب وتقييم معلومات تفصيلية عن كيفية ضمان وتطبيق مزود خدمة السحاب لإدارة المخاطر على نحو يتسم بالذكاء والسرعة والشمولية وذلك قبل التعاقد معه.
11-2-3 تحقيق الأداء الأمثل لإدارة المخاطر	تقوم الجهة الحكومية بتحقيق الأداء الأمثل في عملياتها وأدواتها الخاصة بإدارة المخاطر وذلك لاستيعاب الاستخدامات المتكررة والسريعة للسحاب.
11-2-4 منهجية فحص الضوابط لدى مزود خدمة السحاب	ستقوم الجهة الحكومية بطلب والتحقق من ثم المصادقة على منهجية مراقبة المخاطر الخاصة بمزود خدمة السحاب، أو التأكد من مطابقة سياسة أمن المعلومات لأفضل الممارسات العالمية.

12- التحول إلى الافتراضية

12-1 غرض السياسة

في الحوسبة السحابية، أغلبية ضوابط الفصل المنطقي ليست مادية)مثل الخوادم المنفصلة). بدلاً من ذلك ، يتم تنفيذ الفصل من خلال ضوابط نظام وتطبيقات ممنطقية مصممة للمساعدة في ضمان تجزئة وسلامة البيانات عبر المنصة .إن أحد الآليات الشائعة لتحقيق هذا الفصل في البيانات والخدمات هو "التحول إلى الافتراضية".

12-2 السياسة و الضوابط الأساسية

12-2-1 إرشادات وسياسات التقوية لدى مزود خدمة السحاب	يتعين على الجهة الحكومية تقييم إرشادات وسياسات تقوية التحول للافتراضية لدى مزود خدمة السحاب، وتقييم الفجوة لدى الطرف الثالث وفقاً للمعايير القياسية لأمن التحول إلى الرقمية مثل: المنشور الخاص رقم 800-125 NIST SP800-125 الصادر عن المعهد الوطني للمعايير القياسية والتكنولوجيا. ويشمل ذلك على سبيل المثال لا الحصر: • إيقاف أو حذف كافة الواجهات والمنافذ والأجهزة والخدمات غير الضرورية. • ضبط كافة واجهات الشبكة الافتراضية ومناطق التخزين بأمان. • وضع حدود على استخدام موارد الآلة الافتراضية (VM). • ضمان تقوية كافة أنظمة التشغيل والتطبيقات التي تعمل داخل الآلة الافتراضية. • التحقق من تكامل عمليات إدارة مفاتيح التشفير. • تقوية الأجهزة والحاويات الافتراضية للآلات الافتراضية الفردية.
12-2-2 أمن اللقطات الفوتوغرافية السريعة – (Snapshots)	يتعين على الجهة الحكومية ضمان وجود ضوابط لدى مزود خدمة السحاب لضمان التقاط اللقطات الفوتوغرافية السريعة المصرح بها فقط، وأن مستوى تصنيف وموقع تخزين تلك اللقطات متكافيء من ناحية القوة مع بيئة تحويل الإنتاج إلى الافتراضية (توجد مراجع إضافية عن تصنيف البيانات في سياسات تأمين المعلومات الوطنية).
12-2-3 أمن إدارة الافتراضية hypervisor Security	يتعين على الجهة الحكومية ضمان تطبيق الضوابط التالية: • إمكانية وصول الجهة الحكومية لسجلات الوصول الإدارية الخاصة بمسؤول أمن إ دارة الافتراضية hypervisor. • توفر الدخول الكامل لبرنامج إدارة الافتراضية hypervisor.
12-2-4 دعم صورة العميل	يتعين على الجهة الحكومية التاكد من مزود خدمة السحاب يدعم استخدام الآلات الافتراضية الموثوقة المقدمة من الجهة الحكومية، وأن تلك الآلات الافتراضية قد صُنعت في إطار من الالتزام بإرشادات التقوية المنصوص عليها في سياسة تأمين المعلومات الوطنية.

12-2-5 قائمة الموردين التابعين لمورد خدمة السحاب	يلتزم مورد خدمة السحاب بتزويد الجهة الحكومية بقائمة كاملة لمورديه الذين سيكون لهم حق الوصول إلى بيانات الجهة الحكومية، وذلك في أي وقت خلال مدة سريان الاتفاقية. كما يجب أن يقوم مزود خدمة السحاب بإخطار الجهة بأي تغيير يطرأ على قائمة الموردين.

13- إدارة الهوية والسجلات

13-1 غرض السياسة

تمثل الإدارة المتواصلة والآمنة للهوية مكوناً أساسياً من مكونات الحوسبة السحابية من منظور الأعمال والقابلية للاستخدام والأمن.

في حين تمثل إدارة السجلات (من لديه حق الوصول إلى السجلات؟) قضية أخرى من قضايا الإدارة التي يتعين تناولها والاتفاق عليها مقدماً.

13-2 السياسة والضوابط الأساسية

13-2-1 الهوية المتحدة	يجب على الجهة الحكومية تبني معايير قياسية متحدة للهوية مثل اللغة الترميزية لتأكيد الأمن SAML أو الهوية المفتوحة OpenID واستخدام ذلك في توثيق المستخدمين لدى مزود خدمة السحاب.
13-2-2 توثيق الدليل النشط	يجب على الجهة الحكومية ألا تمنح مزود خدمة السحاب أي تصريح للاستخدام /الوصول المباشر لبيئة التوثيق الخاصة بالجهة مثل الدليل الرئيسي للجهة.
13-2-3 التوثيق متعدد العوامل	يتعين على الجهة الحكومية التأكد من دعم مزود خدمة السحاب لعدة آليات توثيق متعددة العوامل مثل الرموز tokens، وكلمات المرور التي تستخدم لمرة واحدة على الهواء OTA، والبيانات الشخصية.... الخ
13-2-4 إدارة الهوية لدى مزود خدمة السحاب	يتعين على الجهة الحكومية اختيار مزود خدمة السحاب الذي يتيح لها التحكم في إدارة هوياتها الخاصة (بما في ذلك إنشاء هويات الموظفين وإمكانية حذفها/ إنهائها.)

13-2-5 المتطلبات التنظيمية للهوية	على الجهة الحكومية التأكد من استيفاء عملية التوثيق ومراقبة الدخول والمساءلة وعملية الدخول (من ناحية الصيغة والحفظ والوصول) لدى مزود خدمة السحاب للمتطلبات التنظيمية والقانونية للجهة.
13-2-6 مراقبة السجلات	يتعين على الجهة الحكومية تدريب موظفي تكنولوجيا المعلومات لديها على الدخول على خدمات السجلات الخاصة بمزود خدمة السحاب واستخدامها.
03-4-7 مستوى الدخول والحفظ	يتعين على الجهات الحكومية التأكد من توفر إمكانية الدخول لكافة الأحداث الأمنية (تغطية الجلسات ومعلومات العمليات) لمدة لا تقل عن 00 يوماً.

14- أمن تطبيقات الإنترنت

14-1 غرض السياسة

يعد أمن التطبيقات عنصراً هاماً أهمية مطلقة في الحوسبة السحابية. فالسحاب بطبيعة الحال بيئة مفتوحة، كما أن مزودي خدمة السحاب يعرضون عدداً متزايداً من واجهات الإنترنت وواجهات برمجة التطبيقات APIs لشبكة الإنترنت– على نحو يفوق كثيراً الحلول التقليدية الأرضية المغلقة، مما يزيد كثيراً من احتمالات تعرض التطبيقات للهجوم.

14-2 السياسة والضوابط الأساسية

14-2-1 فريق الأمن لدى مزود خدمة السحاب	يجب على الجهة الحكومية أن تحتفظ بالمعلومات التالية: 1- موقع ووقت الوصول لفريق الأمن التابع لمزود خدمة السحاب .
14-2-2 أمن التطبيقات	يتعين على الجهة الحكومية التاكد من تطبيق مزود خدمات السحاب لما يلي: 1- الجدران النارية لطبقة التطبيق. 2- تنفيذ مراجعات رموز التأمين (إن أمكن) قبل تجهيز طرح أي تطبيق. 3- أفضل الممارسات للتطوير الآمن شبكة الإنترنت مثل إرشادات التطوير الآمن الصادرة عن مشروع تطبيق الأمن على الانترنت المفتوح (OWASP). 4- أفضل الممارسات لتقوية أمن أنظمة التشغيل والتطبيقات. 5- الاختبار الدوري للاختراق، وتحديد برنامج للمعالجة، وأنه يشمل إصلاح الثغرات على أساس الأولوية. ويجب تحديد أولويات الثغرات، ويجب إصلاحها ومعالجتها ضمن اتفاقيات مستوى الخدمة المتفق عليها بين الجهة الحكومية ومزود خدمة السحاب. 6- دورة حياة مناسبة لتطوير البرامج (SDLC) وأن الأمن يمثل جزءً متكاملاً في المراحل التالية على الأقل: • التخطيط وتجميع المتطلبات • التصميم ومرحلة التصميم الوظيفي • الترميز • الاختبار • الصيانة

15- التعافي من الكوارث

15-1 غرض السياسة

تحتاج ضوابط حماية البيانات إلى الصيانة لضمان مستوى مرتفع من توفر البيانات وقدرتها على البقاء والتعافي (Resilience) .

15-2 السياسة والضوابط الأساسية

15-2-1 إدارة التغيير والاستجابة للحوادث	يتعين على الجهة الحكومية أن تتأكد من تبني مزود خدمة السحاب والتزامه بإجراءات إدارة التغيير والاستجابة للحوادث وفقاً لما هو محدد في مكتبة البنية التحتية لتكنولوجيا المعلومات (ITIL)
15-2-2 خطة التعافي من الكوارث	يتعين على الجهة الحكومية مراجعة خطة مزود خدمة السحاب للتعافي من الكوارث والتأكد من استيفائها متطلبات الجهة الحكومية، مثل ما يلي: 1- القدرة على استعادة واسترداد البيانات بعد حوادث فقدان البيانات. 2- أن يقوم مزود خدمة السحاب بتزويد الجهة بتقارير اختبار التعافي من الكوارث بصفة سنوية على الأقل، ويجب أن تكون التقارير شاملة تغطي نطاق الاختبار حتى النتيجة والتوصيات النهائية. 3- التأكد من قدرة حل التعافي من الكوارث على الحفاظ على نفس مستويات تدابير وضوابط الأمن المستخدمة في وضع التشغيل الطبيعي. 4- التأكد من أن حل التعافي من الكوارث مملوك ويدار بصورة شاملة من قبل مز ود خدمة السحاب المتعاقد معه.
15-2-3 الالتزام	يوصى بمزودي خدمة السحاب الحاصلين على شهادة BS25999 أو شهادة ISO 22301

16- استخلاص المعلومات لأغراض قانونية أو جنائية

16-1 غرض السياسة

قد يطلب من الجهات الحكومية استتراج بيانات محددة لمتقاسمها مع طرف ثالث كجزء من دعوى قضائية أو لدعم تحقيق مستمر، وهذا النوع من المهمات يطرح تحدياً حتى بالنسبة للبيانات المتزنة داخلياً، وبالتالي، وبالتأكيد فهو يشكل تحدياً أكبر عندما تكون البيانات مخزنة من قبل مزود خدمة سحاب.

16-2 السياسة والضوابط الأساسية

16-2-1 أصل البيانات	تقوم الجهة الحكومية بتحديد ما إذا كانت ملتزمة بتقديم "الأصل الموجود على القرص الصلب/ الشريط الأصلي" أو يمكن الاكتفاء بنسخة. 1- إذا كانت النسخة "الأصلية "هي التي ستكون مطلوبة قانون اً، يجب توصيل هذه المعلومة والنص عليها في العقد مع مزود خدمة السحاب. 2- في حالة كان من الممكن قبول "نسخة" ذات سلسلة حفظ مقبولة، يتعين نقل "متطلبات " سلسلة الحفظ والنص عليها في العقد مع مزود خدمة السحاب.
16-2-2 اتفاقيات مستوى الخدمة لاستخلاص المعلومات	يجب على الجهة الحكومية التأكد من النص في العقد على تفاصيل تكاليف استخلاص المعلومات ومتطلبات البحث الجنائي، بما في ذلك التكلفة ووقت الاستجابة.

17- المنصات متعددة المستخدمين

17-1 غرض السياسة

تتحدى الحوسبة السحابية المفاهيم التقليدية لتجزئة وفصل البيانات، ويتمثل غرض هذه السياسة في التأكد من تضمين ذلك في برامج المخاطر والأمن والتدقيق.

17-2 السياسة والضوابط الأساسية

17-2-1 تجزئة البيانات	يتعين على الجهة الحكومية توثيق وتحديث/ مراجعة ضوابط تجزئة وفصل البيانات بشكل دوري وذلك في كل من الطبقات الأربع الرئيسية لدى مزود خدمة السحاب: (1) طبقة الشبكة, (2) الطبقة الملموسة, (3) طبقة النظام, (4) طبقة التطبيق.
17-2-2 تقييم ضوابط تجزئة	يتعين على الجهة الحكومية تقييم كل ضابط من ضوابط تجزئة البيانات في كل **البيانات** طبقة، بالإضافة إلى عدد ونوع الضوابط في كل طبقة كل 3 شهور وبعد التعديلات والتحديثات الهامة التي تجرى على النظام.

	ملحوظة: عادة ما تكون ضوابط تجزئة بيانات السحاب أضعف على الطبقة الملموسة (حيث غالبا ما لا يكون هناك تجزئة ملموسة)، مما يتطلب أن تكون الضوابط على الطبقات الثلاث الأخرى أكثر قوة.
17-2-3 تصنيف البيانات	يتعين على الجهة الحكومية التأكد من استيفاء مزود خدمة السحاب لمتطلبات تصنيف البيانات المنصوص عليها في سياسة تأمين المعلومات الوطنية.
17-2-4 تشفير البيانات	يتعين على الجهة الحكومية التأكد من تشفير البيانات عند التخزين وأثناء النقل وذلك في إطار من الالتزام الكامل (في أي نقطة زمنية) بسياسة تأمين المعلومات الوطنية والملحق (ب) لسياسة تأمين المعلومات الوطنية بالنسبة للتوارزميات والبروتوكولات التشفيرية المعتمدة من الحكومة.
17-2-5 مفاتيح التشفير المقدمة من مزود الخدمة	يتعين على الجهة الحكومية أن تتأكد من استخدامها لمجموعة فريدة من مفتاح (مفاتيح) التشفير. وتساعد مفاتيح التشفير الفريدة على حماية البيانات من الوصول إليها في حالة تسربها سهواً من أحد عملاء مزود خدمة السحاب إلى عميل آخر.
17-2-6 مفاتيح تشفير البرامج مقابل مفاتيح تشفير الاجهزة	يجب أن تختار الجهة الحكومية مفاتيح تشفير الأجهزة (المتوافقة مع المنشور رقم 3-2 140 من منشورات المعيار الفيدرالي لمعالجة البيانات FIPS وما بعده) متى كانت مدعوماً.
17-2-7 إضافة علامات مفتاحية (Tagging) لبيانات العميل	يوصى بأن تتأكد الجهة الحكومية من أن مزود خدمة السحاب يدعم، ويمكنه كذلك أن يثبت ،إضافة علامات مفتاحية بعيدة (meta-tagging) لبيانات العميل، وهو ما يعد هاماً بالنسبة لتجزئة البيانات وللاكتشاف الالكتروني.

18- إدارة السحاب

18-1 غرض السياسة

إن نقل أصول البيانات إلى السحاب قد يتطلب عملية إعادة تنظيم جوهرية لإدارات دعم العميل. وغالباً ما تتغير الأدوار والمسؤوليات بدرجة مؤثرة عندما تبدأ الجهة في استخدام خدمات السحاب. ولهذا السبب، يتعين على الجهات أن تحدد بوضوح الأدوار المتعلقة بإدارة علاقات مورد خدمات السحاب وتقديم خدمات السحاب.

18-2 السياسة والضوابط الأساسية

18-2-1 التدريب والوعي	يتعين على الجهة الحكومية تدريب موظفيها المسؤولين على إدارة علاقات الموردين وتكنولوجيا السحاب.
18-2-2 الأدوار والمسؤوليات	يتعين على الجهة الحكومية تحديد وتوثيق الأدوار والمسؤوليات المختلفة للموظفين المسؤولين عن إدارة خدمة السحاب. مثال: موظفي الشؤون القانونية، المشتريات، لجنة إدارة التغيير ،ملاك العمل، الأمن والمخاطر.
18-2-3 مصفوفة المسؤولية والمساءلة والتشاور والإعلام (RACI)	يتعين على الجهة الحكومية وضع مصفوفة المسؤولية والمساءلة والتشاور والإعلام (RACI) تشمل الجهة الحكومية ومزود خدمة السحاب وذلك لتحديد المساءلة والالتزامات.
18-2-4 شجرة التصعيد	يتعين على الجهة الحكومية تطوير شجرة تصعيد لمزود خدمة السحاب وتوزيعها على أعضاء فريق العمل المسؤول.

19- المتطلبات التعاقدية لمزود خدمة السحاب

19-1 غرض السياسة

قبل نقل أي خدمة إلى خارج الجهة لأي طرف ثالث، يجب إجراء تحليل وتقييم قانوني صارم .

19-2 السياسة والضوابط الأساسية

19-2-1 اتفاقية عدم إفشاء المعلومات	يتعين على الجهة الحكومية توقيع اتفاقية عدم إفشاء المعلومات (الملحق ب) مع مزود خدمة السحاب قبل تشغيل أي خدمة.
19-2-2 ملكية البيانات	يتعين على الجهة الحكومية ضمان احتفاظها بالحق" الحصري "في ملكية البيانات طوال مدة سريان العقد .وتشمل الملكية كافة نسخ البيانات المتوفرة لدى مزود خدمة السحاب؛ بما في الك النسخ الاحتياطية إن وجدت .كما يجب أن تشترط الجهات الحكومية عدم السماح لمزودي خدمة السحاب باستخدام البيانات الخاصة بتلك الجهات لأغراض الإعلان أو أي غرض ثان وي آخر غير مصرح به.
19-2-3 موقع البيانات	يتعين على الجهة الحكومية أن "تحدد" في العقد الدولة (الدول) التي يكون تخزين البيانات فيها مقبولاً.
19-2-4 القانون الحاكم	يتعين على الجهة الحكومية أن تتأكد من أن سياسة خصوصية البيانات لدى مزود خدمة السحاب تتفق مع القوانين المعمول بها في قطر.
19-2-5 توفر البيانات بدرجة عالية	**1-** يتعين على الجهة الحكومية أن تتأكد من أن اتفاقيات مستوى الخدمة **عالية** تعكس متطلبات توفر التطبيقات والبيانات بدرجة عالية (وفقاً لتحليل التأثير على العمل أو متطلبات العمل لدى الجهة الحكومية) في حالة حدوث انقطاع مخطط أو غير مخطط أو تعطل، مع ضرورة مراجعة الجهة الحكومية لخطط استمرارية العمل والتعافي من الكوارث وإعداد النسخ الاحتياطية وآليات التكرار . **2-** يجب أن تحدد اتفاقيات مستوى الخدمة التعويضات المالية في حالة تعطل العمل.
19-2-6 إخطار خرق البيانات	**1-** يتعين على الجهة الحكومية أن تتأكد من الناحية التعاقدية بأنه سيتم إخطارها "على الفور" بأي خرق مؤكد دون أي تأخير . **2-** يتعين على الجهة الحكومية أن تتأكد من الناحية التعاقدية بأنه سيتم إخطارها خلال 4 ساعات من وقوع أي خرق "مشكوك فيه" من وقت اكتشاف ذلك الخرق.

19-2-7 عقوبة خرق البيانات	يتعين على الجهة الحكومية أن تنص في التعاقد على أن مزود خدمة السحاب هو المسؤول عن أي خسائر مالية أو عقوبات (حتى سقف متفق عليه) قد تحدث نتيجة لأي إخلال من جانب مزود خدمة السحاب.
19-2-8 الحق في الحذف الكامل للبيانات	يتعين على الجهة الحكومية أن تنص في التعاقد على التزام مزود خدمة السحاب بحذف/ إزالة أي أثر للبيانات/ المعلومات بشكل كامل في نهاية العقد وفقاً لما يتم الاتفاق عليه في ذلك العقد.
19-2-9 إتلاف الوسائط	يتعين على الجهة الحكومية أن تنص في التعاقد وتتأكد من التزام مزود خدمة السحاب بضوابط إتلاف وتطهير البيانات والوسائط وفقاً لما تنص عليه سياسة تأمين المعلومات الوطنية
19-2-10 قابلية البيانات	يتعين على الجهة الحكومية أن تتأكد من دعم مزود خدمة السحاب لإعادة البيانات إلى الجهة الحكومية. ويجب ألا يكون هناك اعتماد على مزود خدمة سحاب واحد فقط.

20- توصيات عامة للجهات الحكومية

- يتعين على الجهات الحكومية وضع خارطة طريق لاستخدام وإضافة الحوسبة السحابية نظراً لتعقد بيئة السحاب التي تطرح عدداً من المتغيرات غير المعروفة التي سوف تحتاج إليها الحكومة والخدمات العامة لوضع أساليب جديدة لتقييم وإدارة المخاطر المرتبطة بها.
- يوصى بعدم افتراض أن الاستخدام الناجح لأحد التطبيقات في بيئة سحابية يعتبر إشارة إيجابية بشكل تلقائي للمضي قدماً في المزيد من الاستخدامات الأخرى؛ حيث يجب بحث متطلبات الأمن والمرونة لكل تطبيق بعناية وعلى حدة.
- يوصى بأن تحافظ الجهات الحكومية على القدرة على العودة إلى ما قبل استخدام حلول السحاب.

21- المراجع:

1- سياسة تأمين المعلومات الوطنية (وزارة المواصلات و الاتصالات، أبريل 4024).
2- سياسة تصنيف البيانات الحكومية (وزارة المواصلات و الاتصالات، أبريل 4024).
3- مزايا ومخاطر وتوصيات لأمن المعلومات في الحوسبة السحابية (الوكالة الأوروبية لأمن الشبكات والمعلومات ENISA، نوفمبر 4000).
4- إرشادات للأمن والخصوصية في الحوسبة السحابية العامة (المعهد الوطني للمعايير والتكنولوجيا NIST، منشور رقم SP-800-144)
5- الدليل الأمني لنقاط التركيز الحساسة في الحوسبة السحابية (اتحاد أمن السحاب CSA، النسخة 0.6).
6- مسودة ملخص وتوصيات الحوسبة السحابية (المعهد الوطني للمعايير والتكنولوجيا NIST، منشور رقم SP-800-146)
7- مقدمة لضوابط الأمن في ضوء البرنامج الفيدرالي لإدارة المخاطر والصلاحيات FedRAMP (إدارة الأمن الداخلي بالولايات المتحدة الأمريكية ،2012).
8- ورقة عن التوجيه الاستراتيجي للحوسبة السحابية (الحكومة الاسترالية، أبريل 2011).
9- تقرير هايب سايكل Hype Cycle عن أمن السحاب (جارتنر Garnter، 2011).
10- مشروع السحاب (تقييمات مشتركة، أكتوبر 2010).
11- الأمن والمرونة في خدمات السحاب في الحكومة (الوكالة الأوروبية لأمن الشبكات والمعلومات ENISA، يناير 2011)
12- تعاريف المعهد الوطني للمعايير والتكنولوجيا NIST للحوسبة السحابية (المعهد الوطني للمعايير والتكنولوجيا NIST، المنشور رقم SP-800-145).

22- الملحق أ (استبيان تقييم مزود خدمة السحاب المتعاقد معه)

الغرض من استبيان التقييم أن يكون بمثابة "مرشد" لبيان مجالات الاهتمام والإجراءات التنفيذية التي يجب فهمها، وتقييمها خلال مرحلة تقييم مزود خدمة السحاب.

	نطاق الضوابط	CID	أسئلة تقييم مزود خدمة السحاب المتعاقد معه	الإجابة (نعم/لا)	كيفية تنفيذها
	(*) تشير إلى الضوابط الإلزامية				
	عمليات التدقيق المستقلة	CO.01	*هل تتيح للعملاء الاطلاع على تقارير التدقيق المعدة من قبل أطراف ثالثة عنك؟		
		CO.02	*هل تقوم بإجراء اختبارات اختراق الشبكة للبنية التحتية لخدمة السحاب لديك بانتظام؟ إذا كانت الإجابة بنعم يرجى توضيح الاختبار وعملية المعالجة.		
		CO.03	*هل تقوم بإجراء اختبارات اختراق التطبيق لخدمة السحاب بانتظام ووفقاً لأفضل الممارسات؟ إذا كانت الإجابة بنعم يرجى توضيح الاختبار وعملية المعالجة.		
		CO.04	*هل تقوم بإجراء عمليات تدقيق داخلي بانتظام وفقًا لأفضل ممارسات الصناعة؟ إذا كانت الإجابة بنعم يرجى		

			توضيح الاختبار وعملية المعالجة.		
		CO.05	*هل تقوم بإجراء عمليات تدقيق خارجي بانتظام وفقًا لأفضل ممارسات الصناعة؟ إذا كانت الإجابة بنعم يرجى توضيح الاختبار وعملية المعالجة.		
		CO.06	هل نتائج اختبارات اختراق الشبكة متاحة للعملاء عند طلبها؟		
		CO.07	*هل نتائج التدقيق الداخلي والخارجي متاحة للعملاء عند طلبها؟		
		CO.08	هل تسمح للعملاء بتنفيذ عمليات تقييم مستقلة للثغرات؟		
		CO.09	هل تحتفظ بجهات تنسيق واتصال محدثة مع السلطات المحلية. إذا كانت الإجابة بنعم فما هو معدل تكرار التحقق من جهات الاتصال؟		

		CO.10	*هل لديك القدرة على تقسيم أو تشفير بيانات العميل بحيث يمكن تقديم تلك البيانات لعميل واحد فقط، دون الوصول إلى بيانات عميل آخر دون قصد؟		
		CO.11	*هل لديك القدرة على تقسيم وفصل واسترداد البيانات الخاصة بعميل محدد بشكل منطقي في حالة تعطل النظام أو فقدان البيانات؟		
	الملكية الفكرية	CO.12	*هل لديك سياسات وإجراءات قائمة تصف الضوابط التي لديك لحماية بيانات العميل المصنفة كملكية فكرية؟		
		CO.13	إذا استخدمت خدمات العملاء المستضافة في السحاب لصالح مزود خدمة السحاب، فهل تتم المحافظة على حقوق الملكية الفكرية الخاصة بالعملاء؟		

		CO.14	إذا استخدمت خدمات العملاء المستضافة في السحاب لصالح مزود خدمة السحاب، فهل تسمح للعملاء خايار الانسحاب من الخدمة ؟		
حوكمة المعلومات	الملكية	IG.01	*هل تتبع أو تدعم معيارا للتصنيف الهيكلي لتصنيف البيانات (مثال: ISO 15489 ، الكتيب التعريفي لمواصفات لغة الترميز الموسعة الصادر عن مؤسسة أوسيز ، دليل أنواع البيانات الصادر عن اتحاد أمن السحاب)؟ إذا كانت الإجابة بنعم، يرجى تحديد المعيار.		
	التصنيف	IG.02	*هل توفر القدرة على التعرف على الآلات الافتراضية عبر علامات مفتاحية/بيانات تعريف للسياسة؟		
		IG.03	هل توفر القدرة على التعرف على الأجهزة عبر علامات مفتاحية/بيانات تعريف/علامات مفتاحية للأجهزة؟		

		IG.04	هل لديك القدرة على استخدام الموقع الجغرافي للنظام كعامل توثيق؟		
		IG.05	*هل يمكنك توفير الموقع الملموس/جغرافية تخزين بيانات العميل عند طلب ذلك ؟		

		IG.06	*هل تسمح للعملاء بتحديد المواقع الجغرافية المقبولة لتوجيه البيانات أو إنشاء مصادر مثيلة؟		
	سياسة التعامل/التصنيف /الأمن	IG.07	هل تعتبر كافة بيانات العميل "حساسة للغاية "وتوفر نفس الحماية والضوابط عليها جميعاً أو تطبق الضوابط حسب التصنيف أو تبويب البيانات؟		
		IG.08	*هل يتم تنفيذ آليات لتوارث تبويب البيانات للعناصر التي تعمل كحاويات تجميع للبيانات؟		

	سياسة الاستبقاء	IG.09	*هل لديك قدرات ضبط تقني لتنفيذ سياسات استبقاء بيانات العميل؟		
		IG.10	*هل لديك إجراء موثق للرد على الطلبات الخاصة ببيانات العملاء من الحكومات أو الأطراف الثالثة؟		
	التخلص الآمن	IG.11	*هل تدعم الحذف الآمن (مثال: إزالة المغنطة /مسح رمز الشفرة) للبيانات الأرشيفية الخاصة بالعميل؟		
		IG.12	*هل يمكنك تقديم إجراء منشور لترتيبات الخروج من الخدمة، بما في ذلك التأكيد على تطهير جميع موارد الحوسبة الخاصة ببيانات العميل بمجرد خروج العميل من بيئتك أو قيامه بإخلاء مورد ما؟		
		IG.13	*هل لديك إجراءات لضمان عدم تكرار نسخ بيانات الإنتاج أو استخدامها في بيئات الاختبار لديك؟		

	تسريب المعلومات	IG.14	*هل لديك ضوابط قائمة لمنع تسريب المعلومات أو الإخلال بها على نحو مقصود أو عرضي بين العملاء في بيئة متعددة العملاء؟		
		IG.15	هل لديك حل لمنع فقدان البيانات (DLP) أو حل لمنع حذف البيانات لكافة الأنظمة التي تتصل بتقديم خدمة السحاب لديك ؟		

	السياسة	PA. 01	*هل يمكنك تقديم دليل على وجود سياسات وإجراءات للمحافظة على بيئة عمل تتسم بالأمن والسلامة في المكاتب والغرف والمرافق والمناطق الآمنة؟		
	وصول المستخدم	PA.02	*بموجب القوانين واللوائح والأخلاقيات المحلية والقيود التعاقدية هل يخضع جميع المرشحين للتوظيف والمقاولين والأطراف الثالثة لفحص خلفياتهم؟		

الوصول الملموس

	نقاط وصول مراقبة	PA.03	*هل يتم تنفيذ مقاييس الأمن الملموس (الأسوار والحوائط والحواجز والحراس والبوابات وآليات المراقبة الألكترونية و آليات التحقق الملموس ومكاتب الاستقبال ودوريات الأمن)؟		
	اعتماد المنطقة الآمنة	PA.04	*هل تسمح للعملاء بتحديد أي من مواقعك الجغرافية التي يسمح فيها بإدخال أو إخراج بياناتهم (لتناول اعتبارات الولاية القانونية بناء على مكان تخزين البيانات مقابل الوصول اليها)؟		

	دخول الأشخاص المفوضين	PA.05	*هل نقاط الدخول والخروج مثل مناطق الخدمة والنقاط الأخرى حيث يمكن للأفراد غير المتولين الدخول إلى المقار، مراقبة و متحكم فيها ومنفصلة عن تخزين ومعالجة البيانات؟		

	اعتماد نقل البيانات خارج الموقع	PA.06	هل توفر للعملاء وثائق تصف سيناريوهات امكانية نقل البيانات من موقع ملموس إلى آخر؟ (مثال: النسخ الاحتياطية خارج الموقع، استمرار العمل عن طريق أنظمة احتياطية ،النسخ)		
	أجهزة خارج الموقع	PA.07	هل توفر للعملاء وثائق تصف سياساتك وإجراءاتك التي تحكم إدارة الأصول وإعادة تحديد الغرض من الأجهزة؟		
	إدارة الأصول	PA.08	*هل تحتفظ بقائمة كاملة لجميع أصولك الهامة؟		

الموارد البشرية	اتفاقيات التوظيف	HR.01	*هل تقوم بتدريب موظفيك على أدوارهم بالتحديد مقابل دور العميل في توفير ضوابط أمن المعلومات؟		
		HR.02	هل تقوم بتوثيق إقرار الموظفين بالتدريب الذي تلقوه؟		

	إنهاء التوظيف	HR.03	*هل يتم تحديد وتوثيق وشرح الأدوار والمسؤوليات الواجب اتباعها في حالات إنهاء التوظيف أو تغيير إجراءات التوظيف؟		
امن المعلومات	برنامج الإدارة	IS.01	*هل تقوم بتزويد العملاء بوثائق تصف نظام إدارة أمن المعلومات لديك (ISMS)؟		
	دعم/مشاركة الإدارة	IS.02	*هل هناك سياسات موجودة لضمان اتخاذ الإدارة التنفيذية والمباشرة إجراءات رسمية لدعم أمن المعلومات من خلال توجيه واضح وموثق والتزام وتكليف واضح وتحقق من تنفيذ التكليف؟		

	السياسة	IS.03	هل تتوافق سياسات الخصوصية وأمن المعلومات الخاصة بك مع معايير محددة ((- ISO27001, ، تأمين المعلومات الوطنية NIA، أهداف التحكم بالمعلومات والتكنولوجيا ذات الصلة CoBIT وغيرها) ؟		
		IS.04	هل لديك اتفاقيات تضمن التزام مزوديك بسياسات الخصوصية وأمن المعلومات لديك؟		
		IS.05	هل يمكنك تقديم دليل على قيامك بالاستقصاء المطلوب لتخطيط الضوابط والتصميم والعمليات لديك وفق اللوائح أو المواصفات القياسية؟		
	المتطلبات الأساسية	IS.06	*هل لديك قواعد أساسية موثقة لأمن المعلومات لكل مكون من مكونات البنية التحتية لديك (مثال: المراقب الافتراضي، نظم التشغيل، جهاز		

				التوجيه ،خوادم أسماء النطاقات (DNS)وخلافه)؟	
		IS.07		هل لديك القدرة على مراقبة التزام البنية التحتية لديك وتقديم تقارير عنها باستمرار فيما يتعلق بأساسيات أمن المعلومات لديك؟	
		IS.08		*هل تسمح لعملائك باستخدام الصور الصادرة من آلتهم الافتراضية الموثوقة لضمان التطابق مع المعايير الداخلية الخاصة بهم؟	
	مراجعة السياسات	IS.09		هل تقوم بإخطار عملائك عندما تقوم بعمل تغييرات جوهرية في سياسات أمن المعلومات أو الخصوصية لديك؟	
	تنفيذ السياسات	IS.10		*هل توجد سياسات تأديب أو معاقبة الموظفين الذين ينتهكون سياسات وإجراءات الأمن؟	
		IS.11		*هل يتم توعية الموظفين بالإجراءات التي قد يتم	

				اتخاذها في حالة مخالفة السياسات والاجراءات المذكورة؟	
	سياسة وصول المستخدم	IS.12		*هل لديك ضوابط لضمان وقف حقوق وتصاريح الوصول التي لم تعد مطلوبة دون تأخير؟	
		IS.13		*هل لديك معلومات بالأرقام عن سرعتك في وقف حقوق الوصول بناء على طلبنا؟	
	تقيد/اعتماد وصول المستخدم	IS.14		هل تقوم بتوثيق كيفية منحك وموافقتك للوصول لبيانات العميل؟	
		IS.15		هل لديك طريقة لدمج منهجيات تصنيف بيانات العميل والمزود لأغراض ضبط الوصول؟	
	إيقاف وصول المستخدم	IS.16		*هل يتم تنفيذ الإيقاف الفوري لوصول المستخدم أو تعديل وصوله إلى أنظمة المؤسسات وأصول المعلومات والبيانات عند أي تغيير في حالة الموظفين أو المقاولين أو العملاء أو شركاء العمل أو أطراف ثالثة في الوقت المناسب؟	

	مراجعات وصول المستخدم	IS.17	*هل تطلب اعتماداً سنويا كحد أدنى لاستحقاقات جميع مستخدمي ومسؤلي النظام (باستثناء المستخدمين التابعين لعملائك) ؟		
		IS.18	*إذا وجد أن لدى المستخدمين حقوقاً وامتيازات غير ملائمة، هل يتم تسجيل جميع إجراءات المعالجة والتوثيق؟		
		IS.19	هل ستتقاسم تقارير معالجة وتوثيق امتيازات المستخدم مع عملائك، إذا كان قد تم السماح بوصول غير ملائم إلى بيانات العملاء؟		
	التدريب/الوعي	IS.20	*هل توفر أو تتيح برنامجا رسميا تدريبيا لزيادة الوعي بالأمن فيما يتعلق بقضايا الوصول وإدارة بيانات السحاب (أي اشتراك العملاء ، الجنسية، نموذج تسليم السحاب، فصل المهام والآثار وتضارب المصالح) لجميع الأشتاص		

			ممن لديهم وصول لبيانات العميل؟		
		IS.21	*هل الإداريون لديهم المعرفة المناسبة عن مسؤولياتهم القانونية فيما يتعلق بأمن وسلامة البيانات؟		
	الإلمام بالصناعة /القياس المعياري	IS.22	هل تشارك في مجموعات الصناعة والاتحادات المهنية المعنية بأمن المعلومات؟		
	الأدوار/المسؤوليات	IS.23	*هل تعمل على مقايسة ضوابط الأمن لديك مقابل معايير الصناعة؟		
		IS.24	هل توفر للعملاء مستند لتعريف الأدوار يوضح مسؤولياتك الإدارية مقابل مسؤوليات العميل؟		
	إشراف الإدارة	IS.25	هل المدراء مسؤولون عن المحافظة على الوعي والالتزام بسياسات وإجراءات ومعايير الأمن الخاصة بمجال مسؤوليتهم؟		
	فصل المهام	IS.26	هل توفر للعملاء وثائق عن كيفية المحافظة على فصل المهام في إطار تقديمك لخدمة السحاب؟		

	مسؤولية المستخدم	IS.27	*هل يعي فريقك مسؤولياتهم في المحافظة على الوعي والإلتزام بإجراءات وسياسات ومعايير الأمن المنشورة الخاصة بنا والمتطلبات التنظيمية المعمول بها؟		

		IS.28	المستخدمين بمسؤولياتهم في المحافظة على بيئة عمل تتسم بالأمن والسلامة ؟		
		IS.29	هل تتم توعية المستخدمين بمسؤولياتهم بشأن ترك الأجهزة غير المراقبة بطريقة آمنة؟		
	مكان العمل	IS.30	*هل تتناول سياسات وإجراءات إدارتك للبيانات متطلبات مستوى أمن العميل والخدمة؟		
		IS.31	هل تتضمن سياسات وإجراءات إدارتك للبيانات تدقيقًا للتلاعب أو وظيفة سلامة البرمجيات للوصول غير المرخص لبيانات العميل؟		
		IS.32	*هل البنية التحتية لإدارة الآلة الافتراضية تشمل تدقيقًا للتلاعب أو لوظيفة سلامة البرمجيات لاكتشاف التغييرات في بناء/تهيئة الآلة الافتراضية؟		
	التشفير	IS.33	*هل لديك القدرة التي تسمح لك بإنشاء مفاتيح تشفير خاصة لكل عميل على حدة؟		

		IS.34	هل تدعم مفاتيح تشفير أنشأها العملاء أو تسمح للعملاء بتشفير البيانات إلى هوية ما دون الوصول إلى شهادة المفتاح العام (مثل التشفير القائم على الهوية)؟		
	إدارة مفتاح التشفير	IS.35	*هل تقوم بتشفير بيانات العميل المتزنة (على قرص / تخزين) في بيئتك؟		
		IS.36	*هل ترفع مستوى التشفير لحماية البيانات وصور الآلة الافتراضية أثناء الانتقال عبر الشبكات وبينها ونماذج الآلة الافتراضية؟		
		IS.37	هل لديك القدرة على إدارة مفاتيح التشفير نيابةً عن العملاء؟		
		IS.38	هل تحتفظ بإجراءات إدارة مفاتيح التشفير؟		
	الثغرات/إدارة تصحيح البرامج	IS.39	*هل تجري مسح لثغرات طبقة الشبكة بانتظام؟		
		IS.40	*هل تجري مسحًا لثغرات طبقة التطبيقات بانتظام ؟		
		IS.41	*هل تجري مسحًا لثغرات طبقة نظام التشغيل المحلي بانتظام؟		

		IS.42	*هل لديك القدرة على تصحيح الثغرات بسرعة عبر جميع أجهزة الحواسب والتطبيقات والأنظمة لديك؟		
		IS.43	هل ستوضح لعملائك الأطر الزمنية الخاصة بك لتصحيح للأنظمة المعرضة للخطر عند طلبهم؟		
	برمجيات مكافحة للفيروسات/البرمجيات الخبيثة	IS.44	هل تقوم باستخدام محركات متعددة مضادة للبرمجيات الخبيثة في البنية التحتية لديك ؟		
		IS.45	هل تتأكد من أن نظم اكتشاف تهديد الأمن التي تستخدم التوقيعات والقوائم أو الأنماط السلوكية يتم تحديثها عبر جميع مكونات البنية التحتية في الأطر الزمنية المقبولة في الصناعة؟		
	إدارة الحوادث	IS.46	*هل لديك خطة استجابة موثقة لحوادث الأمن؟		
		IS.47	هل تقوم بإضافة متطلبات العميل المتصصة إلى خطط الاستجابة لحوادث الأمن لديك؟		

		IS.48	هل لديك وظيفة فريق استجابة طوارئ الحاسب الآلي؟		
		IS.49	هل تقوم بنشر مستند خاص بالأدوار والمسؤوليات يحدد مسؤوليتك مقابل مسؤولية عملائك أثناء حوادث أمن المعلومات؟		
	الإبلاغ عن الحوادث	IS.50	هل يقوم نظام إدارة معلومات وأحداث أمن المعلومات(SIEM) لديك بدمج مصادر البيانات (سجلات التطبيقات، سجلات الجدار الناري، سجلات نظام كشف التسلل (IDS) وسجلات الوصول الملموس وخلافه) من أجل التحليل والإنذار الدقيق ؟		
		IS.51	هل يسمح إطار عمل تسجيلك ومراقبتك بعزل حادث ما لعملاء محددين؟		

	الإعداد القانوني للاستجابة للحادث	IS.52	*هل تتفق خطتك للاستجابة للحادث مع معايير الصناعة فيما يتعلق بعمليات وضوابط إدارة تسلسل العهدة المقبولة قانوناً؟		

		IS.53	*هل قدرة الاستجابة للحادث لديك تشمل استخدام أساليب جمع وتحليل البيانات لأغراض التحقيق الجنائي المقب ولة قانونا ؟		
		IS.54	*هل أنت قادر على دعم عمليات الإيقاف لأغراض التقاضي (تجميد البيانات عند وقت معين) لعميل محدد دون تجميد بيانات عميل آخر؟		
		IS.55	هل تفرض فصل بيانات العميل وتشهد عليها عند تقديم بيانات بناء على أمر استدعاء المحكمة؟		
	مقاييس الاستجابة للحادث	IS.56	هل تقوم بمراقبة وقياس أنواع وأحجام وتأثيرات حوادث أمن المعلومات؟		
		IS.57	هل ستقوم بتقاسم بيانات إحصائية عن حوادث أمن		

			المعلومات مع عملائك عند الطلب؟		
	الاستخدام المقبول	IS.58	هل توفر وثائق بشأن كيفية استخدامك أو وصولك لبيانات العميل أو بيانات التعريف؟		
		IS.59	هل تقوم بجمع أو إنشاء بيانات تعريف عن استخدام بيانات العميل		

			من خلال استخدام تقنيات الفحص (محركات البحث وخلافه)؟		
		IS.60	هل تسمح للعملاء بالانسحاب من الوصول إلى بياناتهم أو بيانات تعريفهم عبر تقنيات الفحص؟		
	عوائد الأصول	IS.61	*هل توجد أنظمة لمراقبة انتهاك الخصوصية وإخطار العملاء على وجه السرعة إذا أثر حادث الخصوصية على بياناتهم؟		
		IS.62	*هل تتفق سياسة الخصوصية لديك مع معايير الصناعة وقانون دولة قطر؟		

	معاملات التجارة الألكترونية	IS.63	*هل توفر منهجيات تشفير قياسية (3DESخوارزمية تشفير البيانات الثلاثية، AES معيار التشفير المتقدم وغيرها) للعملاء من أجل حماية بياناتهم إذا وجب نقلها خلال الشبكات العامة؟ (مثل شبكة الإنترنت)		
		IS.64	*هل تستخدم منهجيات تشفير قياسية في أي وقت تحتاج فيه مكونات البنية التحتية لديك للتواصل مع بعضها البعض عبر شبكات عامة مثل نسخ البيانات عبر شبكة الإنترنت من بيئة لأخرى؟		
	الوصول لأدوات التدقيق	IS.65	هل تقيد، أو تسجل أو تراقب الوصول إلى نظم إدارة أمن المعلومات لديك؟ (مثال، الآلات الافتراضية، والجدار الناري ،وأجهزة مسح الثغرات و مراقب الشبكات ،APIs واجهات برمجة التطبيقات وغيرها)		

	الوصول إلى منافذ التشخيص/التهيئة	IS.66	*هل تضمن تقوية محطات عمل الادارة والتحكم في الوصول القائم على الدور من أجل تفعيل مبدأ "أقل الصلاحيات"؟		
	خدمات الشبكة/البنية التحتية	IS.67	هل تقوم بجمع بيانات الطاقة الاستيعابية والاستخدام لجميع المكونات المتعلقة بتقديم خدمة السحاب لديك؟		

		IS.68	هل توفر للعملاء تقارير عن تخطيط الطاقة الاستيعابية والاستخدام ؟		
	أجهزة محمولة/نقالة	IS.69	*هل تسمح بالأجهزة المحمولة في مرفقك لأغراض الإدارة (مثل الكمبيوتر اللوحي)؟		
	تقييد الوصول إلى رمز المصدر	IS.70	*هل توجد ضوابط لمنع الوصول غير المرخص لتطبيقك أو برنامجك أو رمز المصدر والتأكد من اقتصاره على الموظفين المصرح لهم فقط؟		

		IS.71	*هل توجد ضوابط لمنع الوصول غير المرخص لتطبيق أو برنامج العميل أو رمز المصدر والتأكد من اقتصاره على الموظفين المصرح لهم فقط؟		
	الوصول إلى برامج الأدوات المساعدة	IS.72	*هل يتم تقييد ومراقبة برامج الأدوات المساعدة التي يمكن أن تدير الأقسام الافتراضية (مثل الإغلاق والاستنساخ وغيره) بشكل ملائم؟		
		IS.73	هل لديك القدرة على اكتشاف الهجمات التي تستهدف البنية التحتية الافتراضية بشكل مباشر (مثال: Shimmingشيمينج ، Blue Billبلو بيل ، Hyper Gamblingهايبر جامبلنج وغيرها)؟		
		IS.74	*هل يتم منع الهجمات التي تستهدف البنية التحتية الافتراضية بالضوابط التقنية؟		

الجوانب القانونية	اتفاقيات عدم الإفصاح	LG.01	*هل يتم تحديد وتوثيق ومراجعة متطلبات اتفاقيات السرية وعدم الإفصاح التي تعكس احتياجات المؤسسة لحماية البيانات والتفاصيل التشغيلية على فترات محددة؟		
	اتفاقيات الأطراف الثالثة	LG.02	*هل يمكنك تقديم قائمة بمؤسسات الطرف الثالث الحالية والتي سيكون بوسعها الوصول إلى بيانات العميل (بياناتي)؟		

	السياسة	OM.01	هل تم وضع وطرح السياسات والإجراءات لجميع الموظفين من أجل توفير الدعم الكافي لأدوار عمليات الخدمات ؟		

	الوثائق	OM.02	هل تطرح وثائق نظام المعلومات (مثل دليل المسؤول والمستخدم ،والرسوم البيانية للتصميمات وغيرها) للأفراد المصرح لهم للتأكد من تهيئة وتركيب وتشغيل نظام المعلومات؟		
	تخطيط الطاقة الاستيعابية/الموارد	OM.03	هل توفر معلومات موثائقة بشأن مستويات الاشتراكات الزائدة عن طاقة النظام الذي تتبعه (الشبكة، والتخزين والذاكرة والعمليات على شبكة الإنترنت وغيرها) وتحت أي ظرف / سيناريو؟		
		OM.04	*هل تقيد استخدام إمكانات الاشتراك الزائد للذاكرة الموجودة في برنامج تشغيل الآلات الافتراضيةhypervisor؟		
	صيانة الأجهزة	OM.05	إذا كنت تستخدم البنية التحتية الافتراضية، هل يشمل حل السحاب لديك استعادة مستقلة للأجهزة و قدرات		

		الاسترداد بما في ذلك التخزين الخارجي للنسخ الاحتياطية؟			
	OM.06	*إذا كنت تستخدم البنية التحتية الافتراضية، فهل توفر للعملاء القدرة على اعادة آلة افتراضية ما إلى حالتها السابقة في الوقت المطلوب؟			
	OM.07	*إذا كنت تستخدم البنية التحتية الافتراضية، فهل تسمح بتحميل صور الآلة الافتراضية ونقلها إلى مزود سحاب جديد؟			
	OM.08	*إذا كنت تستخدم البنية التحتية الافتراضية، فهل تتم إتاحة صور الآلة للعميل بطريقة تسمح للعميل نسخ تلك الصور في مكان تخزينه الخارجي الخاص؟			
	OM.09	هل تتقاسم التقارير الخاصة بنتائج عمليات النسخ الاحتياطيي/ الاسترداد؟			

	OM.10	هل يشمل الحل السحابي لديك قدرات التعافي			

			والاسترداد المستقلة للمزود/البرنامج؟		
إدارة المخاطر	البرامج	RM.01	*هل مؤسستك مؤمن عليها من طرف ثالث ضد الخسائر ؟		
		RM.02	*هل اتفاقيات مستوى الخدمة لديك توفر تعويض للعميل عن الخسائر التي قد يتكبدها بسبب انقطاع الخدمة أو الخسائر التي تحدث بسبب بنيتك التحتية؟		
	التقييمات	RM.03	*هل التقييمات الرسمية للمخاطر متوافقة مع إطار عمل المؤسسة ويتم تنفيذها سنوياً على الأقل أو على فترات محددة، بشكل يحدد احتمال وتأثير جميع المخاطر المحددة باستخدام وسائل كمية وكيفية؟		
		RM.04	هل يتم تحديد الاحتمال والتأثير المصاحب للمخاطر الكامنة والمتبقية بشكل مستقل، مع أخذ جميع فئات المخاطر في الاعتبار (مثل نتائج		

		التدقيق وتحليل التهديدات والثغرات والالتزام بمتطلبات الجهات التنظيمية)؟			
	التنفيف/القبول	RM.05	*هل يتم تخفيف المخاطر إلى المستويات المقبولة بناء على المعايير المحددة من قبل الشركة وفقًا للأطر الزمنية المعقولة للحل؟		
		RM.06	*هل يتم اجراء المعالجة عند مستويات مقبولة بناء على المعايير المحددة من قبل الشركة وفقًا للأطر الزمنية المعقولة للحل؟		
	تأثيرات تغيير الأعمال/السياسة	RM.07	*هل تشمل نتائج تقييم المخاطر تحديثات لسياسات وإجراءات ومعايير وضوابط الأمن لضمان بقاءها مناسبة وفعالة؟		
	وصول الأطراف الثالثة	RM.08	هل تراقب استمرارية الخدمة مع مزودي الإنترنت المعنيين بنقل البيانات من العملاء إلى الخادم في حالة فشل مزود الخدمة؟		

		RM.09	هل لديك أكثر من مزود تعتمد عليه لكل خدمة على حدة ؟		

		RM.10	هل توفر وصولًا للطاقة الفائضة للعمليات وملخصات استمرارية العمل والتي تشمل الخدمات التي تعتمد عليها؟		
		RM.11	هل توفر للعميل القدرة على إعلان كارثة ما؟		
		RM.12	هل تتيح للعميل خياراً يمكنه استخدامه بنفسه للتغلب على تعطل العمل؟		
		RM.13	*هل تتقاسم خطط استمرارية العمل والخطط الاحتياطية مع عملائك ؟		

تطوير البرمجيات	تطوير جديد/استحواذ	SD.01	*هل تم وضع السياسات والإجراءات من أجل تفويض الإدارة لتطوير أو شراء تطبيقات و نظم و قواعد بيانات و بنية تحتية و خدمات و عمليات و مرافق جديدة؟		
	التغييرات في الانتاج	SD.02	*هل توفر للعملاء وثائق تصف إجراءات إدارة تغيير المنتجات لديك وأدوارهم وحقوقهم ومسؤولياتهم ذات الصلة؟		
	اختبار الجودة	SD.03	هل توفر لعملائك وثائق تصف عملية ضمان الجودة؟		
	التطوير المسند إلى جهات خارجية	SD.04	*هل لديك ضوابط لضمان تحقيق معايير الجودة لتطوير جميع البرمجيات؟		
		SD.05	*هل لديك ضوابط لاكتشاف عيوب أمن رمز المصدر لأي أنشطة تطوير برمجيات مسندة إلى جهات خارجية ؟		

	عمليات تثبيت البرمجيات غير المصرح بها	SD.06	*هل لديك ضوابط لحظر ومراقبة تثبيت البرامج غير المصرح بها على نظامك؟		

DR / إستمرارية العمل	تحليل التأثير	DR.01	هل توفر للعملاء رؤية مستمرة وتقارير عن أداءك التشغيلي وفقاً لاتفاقية مستوى الخدمة(SLA)؟		
		DR.02	هل تضع العملاء دائماً في الصورة وتوفر لهم تقارير عن أداءك التشغيلي وفقاً لاتفاقية مستوى الخدمة (SLA)؟		
	تخطيط استمرارية العمل	DR.03	هل أنت حاصل على شهادة BS25999 أو ISO 22301 ؟		
		DR.04	هل توفر للعملاء خيارات استضافة تتسم بالمرونة الجغرافية؟		
	اختبار استمرارية العمل	DR.05	*هل خطط استمرارية العمل خاضعة للاختبار على فترات محددة أم عند حدوث تغييرات تنظيمية أو بيئية لضمان استمرارية فاعليتها؟		

	المخاطر البيئية	DR.06	*هل تم تصميم الحماية الملموسة ووضع الإجراءات المضادة ضد التلف الناتج عن الأسباب الطبيعية والكوارث والهجمات المقصودة ؟		
	انقطاع الطاقة عن الأجهزة	DR.07	*هل يتم تنفيذ آليات واحتياطات الأمن لحماية الأجهزة من انقطاع خدمة الأدوات المساعدة (مثل انقطاع الطاقة وتعطل الشبكة وغيره)؟		
	الطاقة/الاتصالات	DR.08	هل توفر للعملاء وثائق توضح مسار انتقال بياناتهم بين أنظمتك؟		
		DR.09	هل يمكن للعملاء تحديد كيفية نقل بياناتهم ومن خلال أي ولاية قانونية؟		
	متطلبات وصول العميل	AR.01	*هل تمت معالجة جميع المتطلبات الأمنية و التعاقدية والتنظيمية لوصول العميل قبل منح		

			العملاء وصوًلا للبيانات والأصول ونظم المعلومات؟		
		AR.02	هل تستخدم معايير مفتوحة لتفويض قدرات التوقيق لعملائك؟		

		AR.03	*هل تدعم معايير توحيد الهوية (اللغة الترميزية لتأكيد الأمن SAMLSPML لغة ترميز تزويد الخدمة، WS-federation لغة توحيد خدمات الويب وغيره) كوسيلة لتوثيق/تفويض المستخدمين؟		
		AR.04	هل لديك القدرة على تنفيذ السياسة في نقطة معينة (مثال: لغة الترميز الموسعة للتحكم في الوصولXACML) لتفعيل القيود القانونية الإقليمية وقيود السياسة على وصول المستخدمين؟		

		AR.05	هل لديك نظام إدارة هوية يتيح حق الحصول على البيانات القائم على الدور والقائم على السياق (يتيح تصنيف البيانات للعميل) إذا طلب ذلك ؟		
		AR.06	*هل توفر للعملاء خيارات توثيق قوية (متعددة العوامل) (شهادات رقمية و بيانات شخصية ورموز وغيرها) لوصول المستخدم؟		
		AR.07	هل تسمح للعملاء باستخدام خدمات تأكيد الهوية المقدمة من أطراف ثالثة؟		
		AR.08	هل تستخدم أداة آلية لتحليل رمز مصدر لاكتشاف عيوب أمن الرمز قبل انتاجه؟		
		AR.09	*هل تتحقق من أن جميع موردي برمجياتك يلتزمون بمعايير الصناعة الخاصة بأمن دورة حياة تط وير النظم/البرمجيات؟		
	سلامة البيانات	AR.10	*هل يتم تنفيذ الإجراءات الروتينية لسلامة مدخلات ومخرجات البيانات (مثل		

			المطابقة ومراجعات التحرير) لواجهات التطبيقات وقواعد البيانات لمنع أخطاء المعالجة اليدوية أو الآلية أوتلف البيانات؟		
	بيئات الإنتاج/عدم الإنتاج	AR.11	*بالنسبة لتقديم المنصةكخدمةPaaS ، هل توفر للعملاء بيئات منفصلة لعمليات الإنتاج والاختبار؟		

		AR.12	بالنسبة لتقديم البنية التحتية كخدمةIaaS ، هل توفر للعملاء توجيه عن كيفية إنشاء بيئات إنتاج واختبار مناسبة ؟		
	التوثيق متعددة العوامل للمستخدم عن بعد	AR.13	*هل التوثيق متعدد العوامل مطلوب لوصول المستخدم عن بعد؟		
	أمن الشبكة	AR.14	بالنسبة لتقديم البنية التحتية كخدمةIaaS ، هل تقدم للعملاء توجيه عن كيفية إيجاد تكافؤ في تصميم الأمن الطبقي باستخدام حل افتراضي؟		

	الأمن اللاسلكي	AR.15	*هل تم وضع السياسات والاجراءات و تنفيذالآليات لحماية محيط بيئة الشبكات و تهيئتها لمنع المرور غير المرخص؟		
		AR.16	*هل تم وضع السياسات والاجراءات و تنفيذالآليات لضمان تمكين إعدادات أمن ملائمة بتشفير قوي لتوثيق ونقل واستبدال إعدادات الافتراضية المحددة من المورد؟ (مثال: مفاتيح التشفير، كلمات السر سلسلة المصادقة للبرتوكول البسيط لإدارة الشبكة SNMP وغيرها)		

		AR.17	*هل تم وضع السياسات والاجراءات و تنفيذ الآليات لحماية بيئات الشبكات وكشف وجود أي أجهزة غير مرخصة (خادعة) على الشبكة من أجل فصلها على الفور عن الشبكة؟		
	الشبكات المشتركة	AR.18	*هل الوصول إلى الأنظمة ذات البنية التحتية للشبكة المشتركة مقصور على الموظفين المتولين فقط وفقًا		

			لسياسات وإجراءات ومعايير الأمن. و هل سيكون للشبكات المشتركة ذات الكيانات الخارجية خطة موثقة تفصل ضوابط التعويض المستخدمة لفصل مرور الشبكة بين المؤسسات؟		
	مزامنة الساعة	AR.19	*هل تستخدم بروتوكول خدمة زمنية متزامنة (مثل NTP برتوكول وقت الشبكة) لضمان مرجعية زمنية مشتركة لجميع الأنظمة؟		

	تحديد الأجهزة	AR.20	هل يستخدم التعريف الآلي للأجهزة كوسيلة لتوثيق الاتصال للتحقق من صحة توثيق الاتصال المبني على الموقع المعلوم للأجهزة ؟		
	تسجيل التدقيق /اكتشاف الاختراق	AR.21	*هل الأدوات المستخدمة لتحقيق سلامة الملفات (الاستضافة) واكتشاف اختراق الشبكات تساعد على تسهيل الكشف في وقت مناسب و التحقيق بتحليل الأسباب الجذرية والاستجابة للحوادث؟		

		AR.22	*هل الوصول المادي والمنطقي للمستخدم لسجلات التدقيق مقصورة على الموظفين المتولين فقط؟		
		AR.23	*هل يمكنك تقديم دليل على أنه قد تم القيام بتنطيط يستند إلى الاستقصاء المطلوب عن اللوائح والمعايير التي تنطبق على ضوابطك وتصميمك وعملياتك في الوقت الحالي؟		
	الرمز المتنقل	AR.24	*هل يتم اختبار الرمز المتنقل (من حيث الأمن) قبل تثبيته واستخدامه وفحص تهيئة الرمز لضمان أن الرمز المتنقل المصرح به يعمل وفقًا لسياسة أمنية محددة بوضوح؟		
		AR.25	*هل يحظر تنفيذ كافة الرموز المتنقلة غير المصرح بها؟		
يقوم الاستبيان المذكور أعلاه على أسئلة CAI الصادرة عن اتحاد أمن السحاب(CSA) www.cloudsecurityalliance.org					

23- الملحق ب: نموذج اتفاقية سرية معلومات

ملاحظة: يستخدم النموذج التالي عند التعاقد مع طرف ثالث كمزود لخدمات السحاب.

حررت هذه الاتفاقية بتاريخ ..... بين كل من ..... (يشار إليه في هذه الاتفاقية باسم" **المالك**") ومزود خدمة السحاب ..... (يشار إليها في هذه الاتفاقية باسم" **مزود خدمة السحاب**").

حيث أن المالك يمتلك ويحوز بعض المعلومات السرية (يشار إليها في هذه الاتفاقية باسم" **المعلومات السرية**").
وحيث يرغب المالك في التعاقد مع مزود خدمة السحاب لتقديم خدمات الحوسبة السحابية أو تنفيذ مشروعات الحوسبة السحابية (يشار إليها في هذه الاتفاقية باسم" **الغرض**")، وقد يتضمن ذلك الإفصاح عن المعلومات السرية من جانب المالك إلى مزود خدمة السحاب، بالإضافة إلى التزامات قانونية أخرى .

وبناءً على ما سبق، حررت هذه الاتفاقية لإثبات تعهد مزود خدمة السحاب واتفاقه مع المالك على ما يلي بالنظر إلى إفصاح المالك عن المعلومات السرية إلى مزود خدمة السحاب، والاتفاقات المتبادلة وغير ذلك من الاعتبارات السائغة أو القيمة أو الشكلية التي تم الإقرار باستلامها وكفايتها بموجب هذه الاتفاقية:

1- التعاريف

الاتفاقية: أي إشارة في هذه الاتفاقية إلى كلمة "اتفاقية" يقصد بها هذه الاتفاقية التي تمثل التفاهم الكامل بين الطرفين وتلغي كافة الاتفاقات الأخرى صريحةً كانت أم ضمنية بين الطرفين فيما يتعلق بالإفصاح عن المعلومات السرية.

المعلومات السرية: في هذه الاتفاقية، يقصد "بالمعلومات السرية" ما يلي:
أي معلومات (سواءً كانت مكتوبة أو شفهية أو في شكل الكتروني أو في أي وسيط آخر) يتم الإفصاح عنها فيما يتعلق بالغرض من قبل المالك أو بالنيابة عنه إلى مزود خدمة السحاب في تاريخ هذه الاتفاقية أو بعده؛ و/أو وجود الغرض أو أي مناقشات أو وثائق تتعلق به (بما في ذلك شروط هذه الاتفاقية.)

ولا تشمل المعلومات السرية المعلومات التي:
تكون غير مقيدة الاستعمال وقت الإفصاح، أو تصبح كذلك بعد ذلك بطريق آخر بخلاف الإخلال المباشر أو غير المباشر بهذه الاتفاقية من جانب مزود خدمة السحاب؛ أو التي يستطيع مزود خدمة السحاب أن يثبت أنه قد استلمها

في أي وقت من طرف ثالث لم يحصل عليها تحت شرط الحفاظ على سريتها ويحق له تقديمها إلى مزود خدمة السحاب دون قيد؛ أو تم إعدادها بشكل مستقل من قبل الطرف المتلقي دون وقوع أي إخلال بهذه الاتفاقية.

2- الأطراف الثالثة

يلتزم مزود خدمة السحاب بعدم الإفصاح عن المعلومات السرية لأي طرف ثالث ، ويستثنى من ذلك جواز إفصاح مزود خدمة السحاب عن المعلومات السرية في الحالات التالية:

- الإفصاح عن المعلومات السرية إلى أي من مسؤوليه أو مديريه أو موظفيه أو مستشاريه أو مقاوليه من الباطن أو مستشاريه المهنيين (الأطراف التابعة لمزود خدمة السحاب) الذين يحتاجون بصورة معقولة للاطلاع على تلك المعلومات السرية من أجل تحقيق الغرض. ويلتزم مزود خدمة السحاب باتخاذ الخطوات المعقولة لضمان عدم قيام أي طرف تابع له بأي تصرف أو إغفاله القيام بأي تصرف من شأنه إذا تم القيام به أو إغفال القيام به من جانب مزود خدمة السحاب أن يمثل إخلالاً بهذه الاتفاقية. ويتحمل مزود خدمة السحاب مسؤولية التصرفات والإغفالات التي ترتكبها الأطراف التابعة له كما لو كانت تلك التصرفات أو الإغفالات قد صدرت عن مزود خدمة السحاب نفسه.
- الإفصاح عن المعلومات السرية إلى الحد الذي يتطلبه القانون أو محكمة ذات اختصاص قضائي أو القواعد الخاصة بأي جهة إصدار أو تداول للأوراق المالية أو جهة حكومية أو تنظيمية. ويلتزم مزود خدمة السحاب، حيثما كان ذلك عملياً بصورة معقولة، ووفقاً للقانون ،بأن يخطر المالك خطياً بذلك الإفصاح مقدماً، وأن يستشير المالك فيما يتعلق بمحتوى وغرض ووسيلة الإفصاح، وأن يسعى لجعل ذلك الإفصاح خاضعاً لالتزامات المحافظة على السرية بما يتفق مع شروط هذه الاتفاقية إلى أقصى حد ممكن.
- إذا وافق المالك على الإفصاح موافقة خطية.

3- الإقرار بالملكية والسرية

يقر مزود خدمة السحاب ويوافق على أن المعلومات السرية التي يفصح له المالك عنها، أو التي يحصل عليها مزود خدمة السحاب أو يراها أو يصبح على علم بها كنتيجة مباشرة أو غير مباشرة للمناقشات الواردة في هذه الاتفاقية هي ملكية حصرية للمالك، وأن مزود خدمة السحاب سيحافظ على السرية التامة لتلك المعلومات.

4- عدم جواز تحويل الحقوق

يقر مزود خدمات السحاب ويوافق على أنه لن يحصل على أي حق أو ملكية في المعلومات السرية، وأن المالك يظل هو المالك الوحيد للمعلومات السرية، بما في ذلك على سبيل المثال لا الحصر كافة براءات الاختراع وحقوق النشر والتأليف

والعلامات التجارية والأسرار التجارية والأسماء التجارية وغير ذلك من حقوق الملكية المتعلقة بها، في أي مكان في العالم. ولا يحق لمزود خدمة السحاب إنتاج أو استخدام أو بيع أو توزيع المعلومات السرية دون تصريح خطي من المالك.

5- إنتفاء عرض البيع

يقر الطرفان ويوافقان على أن الإفصاح عن المعلومات السرية من جانب المالك لمزود خدمة السحاب لا يمثل عرضاً من المالك لبيع أو ترخيص أو نقل ملكية المعلومات السرية بأي شكل آخر. ويتعين أن يعد أي عرض لبيع أو ترخيص أو نقل ملكية المعلومات السرية بأي شكل آخر وفقاً لاتفاقية مستقلة.

6- التعويضات

يوافق كل طرف من الطرفين على أنه في حالة وقوع أي إخلال بهذه الاتفاقية من جانبه، يحق للطرف الآخر كمسألة حق أن يتقدم إلى محكمة ذات اختصاص قضائي للحصول على تعويض عن طريق أمر تقييد بما يتوافق مع أحكام هذه الاتفاقية؛ وذلك بالإضافة إلى كافة التعويضات الأخرى المتاحة للطرف الآخر بموجب القانون القطري.

7- التعديل

يجوز للطرفين تعديل أي شرط أو حكم منصوص عليه في هذه الاتفاقية بشرط الموافقة المتبادلة وكتابة تلك التعديلات وتوقيعها من قبل الطرفين.

8- الخلفاء

هذه الاتفاقية ملزمة وسارية المفعول لصالح كلا الطرفين وورثتهما وخلفائهما ومن يتنازلا إليهما وممثليهما

9- التنازل

أي تنازل أو تأجيل أو تسامح أو إخفاق في التصرف من قبل أحد الطرفين بشأن أي إخلال أو إهمال معين يقع من الطرف الآخر لن يؤثر على أي حقوق أو تعويضات تتعلق بذلك الإخلال أو الإهمال أو أي إخلال أو إهمال لاحق تم التنازل عنه صراحةً وخطياً.

10- القانون الحاكم

تخضع هذه الاتفاقية وتفسر وفقاً لقوانين دولة قطر. وتخضع النزاعات الناشئة عن عدم الالتزام بأي من الشروط المنصوص عليها في هذه الاتفاقية للاختصاص القضائي لمحاكم دولة قطر.

11- بدء الإجراءات القضائية

يوافق طرفا هذه الاتفاقية على أن مباشرة أي قضية أو دعوى أو إجراء قضائي أمام أي محكمة تقع في دولة قطر يجوز أن تبدأ بإخطار يسلم شخصياً إلى الطرف الخصم في هذه الاتفاقية أو إلى وكيل الإخطار الملائم.

12- الالتزام المستمر

كافة الحقوق والالتزامات المنصوص عليها في هذه الاتفاقية التي تتجاوز بحكم طبيعتها حدود شروط ومدة هذه الاتفاقية تستمر سارية المفعول على الرغم من أي انتهاء أو إنهاء لهذه الاتفاقية، وتظل سارية المفعول لمدة عامين بعد ذلك الانتهاء أو الإنهاء. وعلى الرغم من ذلك ، يجوز لأي من الطرفين أن يطلب مدة سرية أطول لبعض المعلومات التي يجب أن تصنف وتحدد للطرف الآخر.

13- أتعاب المحاماة

إذا نشأ أي تقاضي عن هذه الاتفاقية، يحق للطرف المحكوم لصالحه استرداد أتعاب وتكاليف ومصروفات المحاماة في الحدود المعقولة، بالإضافة إلى أي تعويض آخر قد يستحق لذلك الطرف.

14- العناوين

كافة الفهارس والعناوين وعناوين الموضوعات وعناوين البنود والمصطلحات المشابهة وردت لغرض الإشارة وسهولة الرجوع فقط، ولا يقصد منها أن تكون شاملة أو محددة، كما أنها لا تؤثر على معنى أو نطاق هذه الاتفاقية.

15- صلاحية التنفيذ

يقر الطرفان الموقعان أدناه بأنهما مخولين لإبرام هذه الاتفاقية بالنيابة عن الطرف الذي يوقعان عنه.

وإشهاداً على ما تقدم، حرر الطرفان هذه الاتفاقية.

المالك	**مزود خدمة السحاب**
(.....)	**(.....)**
التوقيع:	**التوقيع:**
الاسم:	**الاسم:**
الوظيفة:	**الوظيفة:**
التاريخ:	**التاريخ:**