هذا المربع مخصّص لأغراض توجيهية. احذف جميع المربعات التوجيهية بعد تعبئة النموذج. يجب تحرير البنود الملوّنة باللون الأزرق بصورة مناسبة. ويجب إزالة التظليل الملون بعد إجراء التعديلات.

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج سياسة الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة

اختر التصنيف

التاريخ: اضغط هنا لإضافة تاريخ

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

استبدل <اسم الجهة> باسم الجهة في مجمل صفحات الوثيقة. وللقيام بذلك، اتبع الخطوات التالية:

- اضغط على مفتاحي "Ctrl" و"H" في الوقت نفسه.
- أضف "<اسم الجهة>" في مربع البحث عن النص.
- أدخل الاسم الكامل لجهتك في مربع "استبدال" النص.
- اضغط على "المزيد" وتأكّد من اختيار "Match case".
- اضغط على "استبدل الكل".
- أغلق مربع الحوار.

إخلاء المسؤولية

طُور هذا النموذج عن طريق الهيئة الوطنية للأمن السيبراني كمثال توضيحي يمكن استخدامه كدليل ومرجع للجهات. يجب أن يتم تعديل هذا النموذج ومواءمته مع أعمال <اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة. كما يجب أن يُعتمد هذا النموذج من قبل رئيس الجهة أو من يقوم/تقوم بتفويضه. وتخلي الهيئة مسؤوليتها من استخدام هذا النموذج كما هو، وتؤكد على أن هذا النموذج ما هو إلا مثال توضيحي.

اختر التصنيف

الإصدار <١,٠>

اعتماد الوثيقة

الدور	المسمى الوظيفي	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل المسمى الوظيفي>	<أدخل الاسم الكامل للموظف>	اضغط هنا لإضافة تاريخ	<أدخل التوقيع>

نسخ الوثيقة

النسخة	التاريخ	عُدِّلَ بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة تاريخ	<أدخل الاسم الكامل للموظف>	<أدخل وصف التعديل>

جدول المراجعة

معدل المراجعة	التاريخ لأخر مراجعة	تاريخ المراجعة القادمة
مره واحدة كل سنة	اضغط هنا لإضافة تاريخ	اضغط هنا لإضافة تاريخ

اختر التصنيف

الإصدار <١,٠>

قائمة المحتويات

الغرض

الغرض من هذه السياسة هو تحديد متطلبات الأمن السيبراني المتعلقة بحماية الأصول المعلوماتية والتقنية الخاصة ب<اسم الجهة> على خدمات الحوسبة السحابية والاستضافة (Cloud Computing Services and Hosting). وكذلك تقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية في <اسم الجهة> بغرض تحقيق الأهداف الرئيسية للحماية وهي: سرية المعلومات، وسلامة أنظمة المعلومات، وتوافرها.

تمت موائمة هذه السياسة مع الضوابط والمعايير الصادرة من الهيئة الوطنية للأمن السيبراني والمتطلبات التنظيمية والتشريعية ذات العلاقة.

نطاق العمل

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة ب<اسم الجهة> على خدمات الحوسبة السحابية التي تتم استضافتها أو معالجتها أو إدارتها بواسطة أطراف خارجية، وتنطبق هذه السياسة على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>. علمًا بأن قابلية تطبيق المتطلبات يعتمد على نوع خدمات الحوسبة السحابية المقدمة في <اسم الجهة>.

بنود السياسة

١- البنود العامة

١-١ يجب تحديد أدوار الأمن السيبراني، متضمنة المسؤولية والمحاسبة والاستشارة والتبليغ (RACI) لكل أصحاب العلاقة في خدمات الحوسبة السحابية.

١-٢ يجب إدارة مخاطر الأمن السيبراني على نحو ممنهج يهدف إلى حماية البيانات والأصول المعلوماتية والتقنية المستضافة في خدمات الحوسبة السحابية، وذلك وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٣ يجب إجراء تقييم لمخاطر الأمن السيبراني المترتبة على استضافة التطبيقات أو الخدمات في الحوسبة السحابية قبل اختيار مقدم خدمات الحوسبة السحابية والاستضافة.

١-٤ يجب التحقق من كفاءة وموثوقية مقدم خدمات الحوسبة السحابية بالإضافة الى ضمان الالتزام بمتطلبات الأمن السيبراني للحوسبة السحابية الصادرة من الهيئة الوطنية للأمن السيبراني، وذلك وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٥ يجب التحقق من حصول مقدم خدمات الحوسبة السحابية على ترخيص ووجود سجل رسمي له داخل المملكة العربية السعودية وذلك وفقًا لتصنيف وسجل الجهات المختصة للحوسبة السحابية داخل المملكة العربية السعودية.

١-٦ يجب مراقبة والتأكد من تطبيق جميع متطلبات الأمن السيبراني الخاصة بالأطراف الخارجية في سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية على جميع مقدمي خدمات الحوسبة السحابية

والاستضافة وفقًا للسياسات والإجراءات التنظيمية الخاصة بـ<اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٧ يجب التأكد من أن مخاطر الأمن السيبراني المتعلقة بالعاملين لمقدم خدمات الحوسبة السحابية، تعالج بفعالية قبل وأثناء وعند انتهاء/إنهاء عملهم، وذلك وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٨ يجب تطوير قائمة جرد دقيقة للأصول المعلوماتية والتقنية المستضافة في خدمات الحوسبة السحابية، لتحقيق سرية وسلامة الأصول المعلوماتية والتقنية ودقتها وتوافرها في خدمات الحوسبة السحابية، وذلك وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٩ يجب تقييد الدخول إلى الخدمات السحابية الخاصة بها على المستخدمين المصرح لهم فقط وفقًا لسياسة إدارة هويات الدخول والصلاحيات المعتمدة لدى <اسم الجهة>.

١-١٠ يجب التأكد من أن مقدم خدمات الحوسبة السحابية قام بفصل البيئة الخاصة بـ<اسم الجهة> (ويشمل ذلك الخوادم الافتراضية، والشبكات وقواعد البيانات) عن غيرها من البيئات التابعة لجهات أخرى.

١-١١ يجب ضمان حماية الشبكات مثل عزل وحماية الشبكة الخاصة بالأنظمة التقنية السحابية من الشبكات الأخرى من المخاطر السيبرانية وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-١٢ يجب ضمان حماية الأجهزة المحمولة التي يتم استخدامها للدخول للخدمات السحابية من المخاطر السيبرانية، وضمان التعامل الآمن مع المعلومات والبيانات الحساسة وحذف البيانات والمعلومات على الأجهزة المحمولة قبل التخلص منها وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-١٣ يجب ضمان حماية البيانات، وسريتها، وسلامتها، ودقتها، وتوافرها وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-١٤ يجب ضمان تشفير البيانات والمعلومات المنقولة إلى الخدمات السحابية، أو المخزنة فيها، أو المنقولة منها باستخدام طرق تشفير محدثة وفقًا للمعايير الوطنية للتشفير وسياسة تصنيف البيانات المعتمدة لدى <اسم الجهة>.

١-١٥ يجب تقييم كفاءة إدارة الثغرات لدى مقدم خدمات الحوسبة السحابية حسب نوع الخدمة المقدمة وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-١٦ يجب التأكد من تفعيل سجلات الأحداث على الأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة> المستضافة في خدمات الحوسبة السحابية. وذلك وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-١٧ يجب على مقدم خدمات الحوسبة السحابية والاستضافة توفير التقنيات والأدوات اللازمة لـ<اسم الجهة> لإدارة ومراقبة خدماتها السحابية.

١-١٨ يجب على مقدم خدمات الحوسبة السحابية إدارة المفاتيح بما يتوافق مع متطلبات الأمن السيبراني الخاصة بإدارة المفاتيح لدى <اسم الجهة> وفقًا لمعيار/سياسة إدارة المفاتيح في الجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-١٩ يجب ضمان توافر متطلبات صمود الأمن السيبراني في إدارة استمرارية الأعمال وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٢٠ يجب أن يكون لدى <اسم الجهة> الحق في إجراء اختبارات وتقييمات سيبرانية على مقدم الخدمة السحابية أو الاستضافة أو طلب تقارير ونتائج التقييمات السيبرانية المنفذة من جهات مستقلة وموثوقة، على ان يتم تضمين هذا البند في العقود الموقعة مع مقدم الخدمة السحابية والاستضافة.

١-٢١ يجب على <الإدارة المعنية بالأمن السيبراني> و<الإدارة المعنية بالشؤون القانونية> أن تُضمن متطلبات الأمن السيبراني المعتمدة في <اسم الجهة> والمتعلقة باستضافة البيانات في عقود مقدمي خدمات الحوسبة السحابية والاستضافة وفقًا للسياسات والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٢٢ يجب تطوير وتوثيق واعتماد إجراءات خاصة باستخدام الخدمات السحابية.

١-٢٣ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات حماية الأصول المعلوماتية والتقنية المستضافة على خدمات الحوسبة السحابية.

٢- متطلبات الأمن السيبراني المتعلقة باستضافة/تخزين البيانات

٢-١ يجب تصنيف البيانات حسب التشريعات والأنظمة ذات العلاقة قبل استضافتها/تخزينها لدى مقدمي خدمات الحوسبة السحابية والاستضافة.

٢-٢ يجب الحصول على إفادة رسمية وموثقة من مقدم خدمة الحوسبة السحابية والاستضافة بمستوى الترخيص الممنوح له من قبل الجهات المعنية لاستضافة البيانات حسب تصنيفها، وأن يقوم باستضافة ومعالجة بيانات <اسم الجهة> المصنفة بحسب الترخيص الممنوح له فقط.

٢-٣ يجب إلزام مقدمي خدمات الحوسبة السحابية والاستضافة على إعادة البيانات (بصيغة قابلة للاستخدام) وحذفها بشكل غير قابل للاسترجاع عند إنهاء/انتهاء الخدمة على ان يتم تضمين هذا البند في العقود الموقعة مع مقدم الخدمة السحابية والاستضافة.

٢-٤ يجب على مقدمي خدمات الحوسبة السحابية والاستضافة إجراء اختبارات دورية للتحقق من فعالية استعادة النسخ الاحتياطي.

٢-٥ يجب أن يكون موقع واستضافة وتخزين معلومات <اسم الجهة> داخل المملكة العربية السعودية مع مراعاة التنظيمات والجوانب التشريعية بعدم خضوع تلك البيانات لأي قوانين دول أخرى.

٢-٦ يجب أن يكون موقع استضافة الأنظمة الحساسة، أو أي جزء من مكوناتها التقنية، داخل <اسم الجهة>، أو في خدمات الحوسبة السحابية المقدمة من قبل جهة حكومية، أو شركة وطنية محققة لضوابط الهيئة الوطنية للأمن السيبراني المتعلقة بخدمات الحوسبة السحابية والاستضافة، مع مراعاة تصنيف البيانات المستضافة.

الأدوار والمسؤوليات

١- **مالك السياسة:** <رئيس الإدارة المعنية بالأمن السيبراني>.

٢- **مراجعة السياسة وتحديثها:** <الإدارة المعنية بالأمن السيبراني>.

٣- **تنفيذ وتطبيق السياسة:** <الإدارة المعنية بتقنية المعلومات> و<الإدارة المعنية بالأمن السيبراني>.

٤- **قياس الالتزام بالسياسة:** <الإدارة المعنية بالأمن السيبراني>.

اختر التصنيف

الإصدار <١,٠>

التحديث والمراجعة

يجب على <الإدارة المعنية بالأمن السيبراني> مراجعة السياسة سنويًا على الأقل أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في <اسم الجهة> أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بالسياسة

١- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذه السياسة بشكل دوري.

٢- يجب على كافة العاملين في <اسم الجهة> الالتزام بهذه السياسة.

٣- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في <اسم الجهة>.