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

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

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

اختر التصنيف

التاريخ: اضغط هنا لإضافة نص

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

اعتماد الوثيقة

الدور	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل الاسم الكامل للشخص>	اضغط هنا لإضافة نص	<أدخل التوقيع>

نسخ الوثيقة

النسخة	التاريخ	عُدلَ بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة نص	<أدخل الاسم الكامل للشخص>	<أدخل وصف التعديل>

اختر التصنيف

الإصدار 1.0

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية الأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة> على خدمات الحوسبة السحابية والاستضافة (Cloud Computing Services and Hosting). وذلك، لضمان معالجة المخاطر السيبرانية أو تقليلها من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٤-٢-١ من الضوابط الأساسية للأمن السيبراني (ECC – 1: 2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة> على خدمات الحوسبة السحابية التي تتم استضافتها أو معالجتها أو إدارتها بواسطة أطراف خارجية، وتنطبق هذه السياسة على جميع العاملين في <اسم الجهة>.

بنود السياسة

1- البنود العامة

1-1 تُطبَق جميع متطلبات الأمن السيبراني الخاصة بالأطراف الخارجية في سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية على جميع مقدمي خدمات الحوسبة السحابية والاستضافة.

2-1 يجب على <الإدارة المعنية بالأمن السيبراني> التحقق من كفاءة وموثوقية مقدم خدمات الحوسبة السحابية والاستضافة بالإضافة إلى حصوله على ترخيص ووجود سجل رسمي له داخل المملكة العربية السعودية.

3-1 يجب تطبيق متطلبات الأمن السيبراني الخاصة بخدمات الحوسبة السحابية والاستضافة وفقاً للسياسات والإجراءات التنظيمية الخاصة بـ<اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة.

4-1 يجب على <اسم الجهة> إجراء تقييم لمخاطر الأمن السيبراني المترتبة على استضافة التطبيقات أو الخدمات في الحوسبة السحابية قبل اختيار مقدم خدمات الحوسبة السحابية والاستضافة.

5-1 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. (CSCC-4-2-1-1)

6-1 يجب على <الإدارة المعنية بالأمن السيبراني> تطوير وتوثيق واعتماد إجراءات خاصة باستخدام الخدمات السحابية.

7-1 يجب أن تتضمن عقود مقدمي خدمات الحوسبة السحابية والاستضافة بحد أدنى ما يلي:

1-7-1 متطلبات الأمن السيبراني وبنود اتفاقية مستوى الخدمة (Service Level Agreement "SLA").

2-7-1 بنود المحافظة على سرية المعلومات (Non-disclosure Clauses) بما في ذلك حذف البيانات وإتلافها بالاتفاق بين مقدم الخدمة و<اسم الجهة> بناء على تصنيف تلك البيانات ومع مراعاة سياسة تصنيف البيانات.

3-7-1 متطلبات استمرارية الأعمال والتعافي من الكوارث.

4-7-1 يجب أن تتضمن عقود مقدمي خدمات الحوسبة السحابية والاستضافة إمكانية <اسم الجهة> إنهاء الخدمة دون مبرر أو اشتراطات .

8-1 يجب مراجعة تطبيق متطلبات الأمن السيبراني مع مقدمي خدمات الحوسبة السحابية والاستضافة دورياً، مرة واحدة في السنة، على الأقل.

2- متطلبات الأمن السيبراني المتعلقة باستضافة/تخزين البيانات

1-2 يجب تصنيف البيانات قبل استضافتها/تخزينها لدى مقدمي خدمات الحوسبة السحابية والاستضافة. (ECC-4-2-3-1)

2-2 يجب على مقدمي خدمات الحوسبة السحابية والاستضافة إعادة البيانات (بصيغة قابلة للاستخدام) وحذفها بشكل غير قابل للاسترجاع عند إنهاء/انتهاء الخدمة. (ECC-4-2-3-1)

3-2 يجب أن يكون موقع واستضافة وتخزين معلومات <اسم الجهة> داخل المملكة العربية السعودية (ECC-4-2-3-3) مع مراعاة التنظيمات والجوانب التشريعية بعدم خضوع تلك البيانات لأي قوانين دول أخرى.

4-2 يجب على <الإدارة المعنية بالأمن السيبراني> التأكد من فصل البيئة الخاصة بـ<اسم الجهة> (ويشمل ذلك الخوادم الافتراضية، والشبكات وقواعد البيانات) عن غيرها من البيئات التابعة لجهات أخرى في خدمات الحوسبة السحابية. (ECC-4-2-3-2)

5-2 يجب الحصول على موافقة <الإدارة المعنية بالأمن السيبراني> لاستضافة الأنظمة الحساسة أو أي جزء من مكوناتها التقنية.

6-2 يجب على <اسم الجهة> التأكد من تطبيق متطلبات خصوصية البيانات على البيانات المستضافة في الحوسبة السحابية.

7-2 يجب تشفير البيانات والمعلومات المنقولة إلى الخدمات السحابية، أو المخزنة فيها، أو المنقولة منها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة في <اسم الجهة>.

8-2 يجب على <اسم الجهة> التأكد من أن مقدم خدمات الحوسبة السحابية والاستضافة يقوم بعمل النسخ الاحتياطي دورياً وحماية النسخ الاحتياطية وفقاً لسياسة النسخ الاحتياطية المعتمدة في <اسم الجهة>.

9-2 يجب على <اسم الجهة> التأكد من أن مقدم خدمات الحوسبة السحابية والاستضافة لا يمكنه الاطلاع على البيانات المخزنة وأن صلاحية الوصول الخاصة بمقدم الخدمة محدودة بالصلاحيات اللازمة للقيام بأنشطة إدارة خدمة الاستضافة وصيانتها، أو حسب متطلبات الأعمال.

2-10 يجب على مقدم خدمات الحوسبة السحابية والاستضافة تقييد الدخول إلى الخدمات السحابية الخاصة بـ<اسم الجهة> على المستخدمين المصرح لهم فقط وباستخدام وسائل التحقق من هوية المستخدم وفقاً لسياسة إدارة هويات الدخول والصلاحيات المعتمدة في <اسم الجهة>.

2-11 يجب على مقدم خدمات الحوسبة السحابية والاستضافة توفير التقنيات والأدوات اللازمة لـ<اسم الجهة> لإدارة ومراقبة خدماتها السحابية.

2-12 يجب على <الإدارة المعنية للأمن السيبراني> و<الإدارة المعنية بالشؤون القانونية> تضمين بنود متطلبات الأمن السيبراني المتعلقة باستضافة البيانات في العقد مع مقدم خدمة الحوسبة السحابية.

3- متطلبات أخرى

3-1 يجب على <اسم الجهة> التأكد من تفعيل سجلات الأحداث على الأصول المعلوماتية المستضافة.

3-2 يجب على <اسم الجهة> مراقبة سجلات الأحداث الخاصة بالأمن السيبراني دورياً.

3-3 يجب على <اسم الجهة> التأكد من مزامنة التوقيت (Clock Synchronization) الخاص بالبنية التحتية للخدمة السحابية مع التوقيت الخاص بـ<اسم الجهة>.

3-4 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لحماية الأصول المعلوماتية والتقنية على خدمات الحوسبة السحابية.

3-5 يجب مراجعة متطلبات الأمن السيبراني الخاصة بخدمات الحوسبة السحابية والاستضافة دورياً.

3-6 يجب مراجعة هذه السياسة مرة واحدة في السنة؛ على الأقل.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** <رئيس الإدارة المعنية بالأمن السيبراني>.

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

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

الالتزام بالسياسة

1- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> ضمان التزام <اسم الجهة> بهذه السياسة بشكل دوري.

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

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