جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

سياسة أمن الحوسبة السحابية

الإصدار: Version 2.0

رمز السياسة:DICT.I.06-43.CS. A. V2.0

جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY
عمادة الاتصالات وتقنية المعلومات
Deanship of Information and Communication Technology

1. جدول المحتويات

1. جدول المحتويات 2
2. معلومات ذات ملكية فكرية 3
3. الرقابة على الوثيقة 4
1.3 معلومات عن الوثيقة 4
2.3 تاريخ الإعداد والتّحديث 4
3.3 المراجعة والتدقيق 4
4.3 قائمة التوزيع 4
5.3 الاعتماد 4
4. المقدمة 5
5. الهدف 5
6. قابلية التطبيق ونطاق العمل 5
7. السياسة 6
1.7 متطلبات السياسة العامة 6
2.7 إنشاء الخدمات السحابية 6
3.7 ضوابط الوصول 9
4.7 تخزين البيانات الحساسة 10
8. الأدواروالمسؤوليات 10
9. ملكية السياسة 11
10. تغييرات السياسة 11
11. الالتزام 11
12. السياسات والمعاييروالإجراءات ذات العلاقة 12
13. المراجع 12

2. معلومات ذات ملكية فكرية

هذه الوثيقة هي عبارة عن معلومات خاصة بعمادة الاتصالات وتقنية المعلومات في جامعة الإمام عبد الرحمن بن فيصل. وهي وثيقة موجهة للجهات المعنية فقط حيث لا يتم توزيعها أو الكشف عنها أو نشرها أو نسخها دون إذن كتابي من عمادة الاتصالات وتقنية المعلومات.

3. الرقابة على الوثيقة

1.3 معلومات عن الوثيقة

العنوان	التصنيف	الإصدار	الحالة
سياسة أمن الحوسبة السحابية	مقيد	V2.0	فعال

2.3 تاريخ الإعداد والتّحديث

الإصدار	المؤلفون	تاريخ الاصدار	التغييرات
V1.0	د. بشار الذيب	2021/03/23	إنشاء
V1.1	د. سامر بني عواد	2022/02/20	مراجعة وتحديث
V2.0	بهاء نوافله	2023/12/17	مراجعة وتحديث

3.3 المراجعة والتدقيق

تاريخ المراجعة القادمة
2025/01/01

4.3 قائمة التوزيع

الرقم	المستفيد
1	جميع أقسام عمادة الاتصالات وتقنية المعلومات
2	الشؤون القانونية
3	الموقع الإلكتروني
4	

5.3 الاعتماد

الاسم	الوظيفة	رقم القرار	التاريخ
د. نهاد بنت عبد الله العمير	نائب الرئيس للتطوير والشراكة المجتمعية	61945	2024/03/06

4. المقدمة

من الضروري أن يحمي الجامعة أصوله المعلوماتية والتقنية من أجل ضمان نجاحها واستمرارية عملها. ونظراً لطبيعة أعماله، فإن الجامعة يعتمد بشكل كبير على مزودي الخدمات السحابية، مما يؤكد ضرورة اتباع وتنفيذ الضوابط الأمنية المطلوبة لضمان حمايتها من التهديدات.

تُدرج هذه السياسة في إطار سياسة الجامعة وتحت الصلاحيات الممنوحة من صاحب الصلاحية ابتداءً من تاريخ اعتمادها.

5. الهدف

تحدد هذه السياسة متطلبات الأمن السيبراني وحوكمة البيانات المقررة لإنشاء واستخدام الخدمات السحابية لتخزين أو معالجة أصول معلومات الجامعة دون تعريض بياناتها وموارد الحوسبة للمخاطر الأمنية.

6. قابلية التطبيق ونطاق العمل

تنطبق أحكام هذه السياسة على جميع العاملين أو المكلفين الذين يعملون في الجامعة سواء بعقود دائمة أو مؤقتة وبشكل مباشر أو غير مباشر بما في ذلك الموردين والمقاولين الخارجيين وأي شخص لديه صلاحية الوصول الدائم أو المؤقت إلى بيانات الجامعة مهما كان مصدرها أو شكلها أو طبيعتها وإلى أنظمة وأجهزة وقواعد بيانات الجامعة.

تنطبق هذه السياسة على جميع الخدمات السحابية الخارجية، مثل البريد الإلكتروني الرسمي، وتخزين المستندات، والبرمجيات كخدمة (SaaS) والبنية التحتية كخدمة (IaaS) والنظام الأساسي كخدمة (PaaS).

7. السياسة

1.7 متطلبات السياسة العامة

1.1.7 يجب أن يُصرح رسمياً باستخدام خدمات الحوسبة السحابية لأغراض أعمال الجامعة من قبل مدير الأمن السيبراني. لا يُسمح للعاملين بإنشاء حسابات خدمات سحابية أو الدخول في عقود خدمة سحابية لتخزين أو معالجة أو تبادل الاتصالات المتعلقة بالجامعة أو البيانات المملوكة للجامعة دون الحصول على الموافقات المطلوبة وفقاً لهذه السياسة.

2.1.7 يجب أن تتم الموافقة على جميع موردي خدمات المعالجة (السحابية) التابعين لجهات خارجية من قبل إدارة الأمن السيبراني وعمادة الاتصالات وتقنية المعلومات في الجامعة، كما يجب على مدير الأمن السيبراني بالتشاور مع العميد، تقييم واعتماد متطلبات الضوابط المتعلقة بالأمن والخصوصية والتقنية من قبل مورد خدمات الحوسبة السحابية بالشكل المناسب.

2.7 إنشاء الخدمات السحابية

1.2.7 أي خدمات سحابية تتطلب موافقة المستخدمين على شروط الخدمة، يجب مراجعة هذه الاتفاقيات والموافقة عليها من قبل رؤساء التنفيذيين لتقنية المعلومات والشؤون القانونية وأمن المعلومات واستمرارية الأعمال.

2.2.7 لا يُسمح لمزود الخدمة السحابية استخدام بيانات الجامعة للأغراض الثانوية، كما يجب أن يضمن مزود الخدمة السحابية تطبيق أدوات أمان متعددة على مستويات مختلفة داخل الشبكة الداخلية، على سبيل المثال لا الحصر، أنظمة منع اختراق الشبكة (IPS) لاكتشاف الأنشطة الضارة وحظرها، ومراقبة أنظمة كشف الاختراقات (IDS) وتوفير التنبيهات الفورية، ومراقبة سلامة الملفات (FIM) لضمان سلامة البيانات ومنع التغييرات غير المصرح بها، منع تسرب البيانات (DLP) لضمان مراقبة وحظر جميع أنواع تسرب البيانات المشتبه بها، وتطبيق القائمة المحددة (whitelisting) على البنية التحتية.

3.2.7 يجب أن تتضمن العقود المبرمة مع مزود الخدمة السحابية حقوق التدقيق والمراجعة والمراقبة.

4.2.7 يجب تصنيف البيانات قبل استضافة أي منها على السحابة.

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

6.2.7 يجب أن يضمن مزود الخدمة السحابية قيام طرف خارجي مستقل بإجراء اختبار أمني للتأكد من تنفيذ العزل بشكل آمن وإعداد التوجيه الافتراضي وإعادة التوجيه (VRF) بشكل صحيح، ويجب مشاركة نسخة من التقرير مع الجامعة.

7.2.7 يجب استضافة التطبيقات، أو الخدمات، أو البيانات، أو أي مكون فني ذو صلة بواسطة مزود خدمة السحابة في المملكة العربية السعودية.

8.2.7 يجب أن يكون موقع استضافة الأنظمة الحساسة، أو أي جزء من مكوناتها التقنية، داخل الجامعة، 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.

9.2.7 يجب على الجامعة التأكد من تطبيق متطلبات خصوصية البيانات على البيانات المستضافة في الحوسبة السحابية.

10.2.7 يجب تشفير البيانات والمعلومات المنقولة إلى الخدمات السحابية، أو المخزنة فيها، أو المنقولة منها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة في الجامعة.

11.2.7 يجب أن يوفر مزود الخدمة السحابية صلاحيات الوصول لتأمين أجهزة الشبكات التي تعمل على حماية بيئة الجامعة. يجب التعامل مع أنشطة الإدارة المتعلقة بجدار الحماية وأجهزة الشبكة من خلال موارد أمان مخصصة للخدمات السحابية.

12.2.7 يجب على مزود الخدمة السحابية توفير قائمة ثابتة ومفصلة للأنشطة التي تم إجراؤها من قِبلهم لضمان حماية وأمن بيئة الجامعة وتقديم مزيد من التفاصيل في اتفاقية مستوى الخدمة الحالية.

13.2.7 يجب أن يضمن مزود الخدمة السحابية اختبار أمان وتنفيذ بروتوكول البوابة الحدودية (BGP) والتأكد من تنفيذ ضوابط أمنية إضافية لضمان حمايتها.

14.2.7 يجب على الجامعة التأكد من أن مقدم خدمات الحوسبة السحابية والاستضافة يقوم بعمل النسخ الاحتياطي دورياً وحماية النسخ الاحتياطية وفقاً لسياسة النسخ الاحتياطي المعتمدة في الجامعة.

15.2.7 يجب أن تُحدد العقود بنود الفسخ التي تتضمن حق الجامعة في فسخ العقد وتطلب من مزود الخدمة السحابية إعادة بيانات الجامعة بتنسيق قابل للاستخدام ومن ثم حذفها بشكل نهائي عند فسخ العقد.

16.2.7 يجب استخدام الخدمات السحابية الموجودة في المملكة العربية السعودية فقط. ويجب الحصول على موافقة العميد في حال الحاجة لاستخدام الخدمات السحابية خارج المملكة العربية السعودية مع اتباع الاجراءات التنظيمية والتشريعية في هذا الخصوص.

17.2.7 يجب على مزود الخدمة السحابية تنفيذ ومراقبة ضوابط الأمن السيبراني لحماية سرية وسلامة وتوافر بيانات الجامعة.

18.2.7 يجب فصل بيانات الجامعة منطقياً عن البيانات الأخرى التي يحتفظ بها مزود الخدمة السحابية. بالإضافة إلى ذلك، يجب أن يكون مزود الخدمة السحابية قادراً على تحديد وتمييز بيانات الجامعة عن البيانات الأخرى بشكل دائم. يجب على مزود الخدمة السحابية تنفيذ ضوابط أمنية إضافية، على سبيل المثال لا الحصر، استخدام جدران الحماية (firewalls) وتطبيق قيود عنوان بروتوكول الإنترنت (IP)، مما يحد من نشاط الأنظمة التي تكتب وتقرأ البيانات من الذاكرة لضمان العزل والتقسيم الكامل عن مستخدمي الشبكة.

19.2.7 يجب على مزود الخدمة السحابية تقديم دليل على الفصل الملائم والآمن بين بيئة الإنتاج والتطوير والاختبار في حال كانت الخدمة مدارة من قبله.

20.2.7 يجب تطوير وتنفيذ إجراءات التعافي من الكوارث واستمرارية الأعمال، المتعلقة بالحوسبة السحابية، بصورة آمنة.

21.2.7 يجب على مقدم خدمات الحوسبة السحابية والاستضافة توفير التقنيات والأدوات اللازمة للجامعة لإدارة ومراقبة خدماتها السحابية.

22.2.7 يجب على الجامعة 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.

23.2.7 يجب أن يضمن مزود الخدمة السحابية الالتزام بسياسات حوكمة البيانات الصادرة من مكتب إدارة البيانات الوطنية وتقديم الضمان المطلوب للجامعة.

24.2.7 يجب على العاملين إنشاء حسابات خدمة سحابية فقط مع موردي الخدمات السحابية المعتمدين من قبل الجامعة.

25.2.7 يجب أن تتضمن عقود مقدمي خدمات الحوسبة السحابية والاستضافة بحد أدنى ما يلي:

- متطلبات الأمن السيبراني وبنود اتفاقية مستوى الخدمة (Service level Agreement "SLA")
- بنود المحافظة على سرية المعلومات (Non-disclosure Clauses) بما في ذلك حذف البيانات وإتلافها بالاتفاق بين مقدم الخدمة والجامعة بناء على تصنيف تلك البيانات ومع مراعاة سياسة تصنيف البيانات.
- متطلبات استمرارية الأعمال والتعافي من الكوارث.
- يجب أن تتضمن عقود مقدمي خدمات الحوسبة السحابية والاستضافة إمكانية الجامعة إنهاء الخدمة دون مبرر أو اشتراطات.
- متطلبات إعادة البيانات بصيغة قابلة للاستخدام عند إنهاء/انتهاء الخدمة.

3.7 ضوابط الوصول

1.3.7 يجب إنشاء حسابات المستخدمين وفقاً لسياسة التحكم في الوصول الخاصة بالجامعة.

2.3.7 يجب على مقدم خدمات الحوسبة السحابية والاستضافة تقييد الدخول إلى الخدمات السحابية الخاصة بالجامعة على المستخدمين المصرح لهم فقط وباستخدام وسائل التحقق من هوية المستخدم وفقاً لسياسة التحكم في الوصول في الجامعة.

3.3.7 يجب أن تتوافق حسابات المستخدمين في خدمات الأطراف الخارجية (السحابية) مع المتطلبات الأمنية الحالية للجامعة الخاصة بكلمات مرور آمنة وفقاً لسياسة كلمة المرور.

4.7 تخزين البيانات الحساسة

1.4.7 يوافق مدير الأمن السيبراني أو من ينوب عنه على أنواع البيانات التي قد يتم تخزينها في بيئات (سحابية) تابعة لجهات خارجية.

2.4.7 يجب الحصول على موافقة مدير الأمن السيبراني لاستضافة الأنظمة الحساسة أو أي جزء من مكوناتها التقنية.

3.4.7 لا يُسمح باستخدام حسابات الخدمات السحابية الشخصية لتخزين أو معالجة أو تبادل الاتصالات ذات الصلة بالجامعة أو البيانات المملوكة لها.

8. الأدوار والمسؤوليات

يجب على إدارة الأمن السيبراني:

1.1.8 على مدير الأمن السيبراني اعتماد السياسة من صاحب الصلاحية والعمل على تنفيذها.

2.1.8 على مدير الأمن السيبراني اعتماد المعايير والإجراءات والتوجيهات لضمان الالتزام الضروري بمتطلبات أمن عمليات الجامعة.

3.1.8 على مدير الأمن السيبراني ضمان التوافق بين هذه السياسة وأعمال الجامعة.

4.1.8 على مدير الأمن السيبراني حل أي متعارضات تنشأ عن هذه السياسة.

5.1.8 على مدير الأمن السيبراني توفير الموارد اللازمة لتحديد وشراء وتنفيذ الحلول التقنية وذلك لتنفيذ متطلبات السياسة حيثما أمكن.

6.1.8 على إدارة الأمن السيبراني تعميم سياسة الالتزام بالأمن السيبراني وحوكمة البيانات على جميع إدارات وعاملي ومستخدمي الجامعة المصرح لهم أو الذين سيصرح لهم الوصول إلى الأصول التقنية والمعلوماتية.

7.1.8 على إدارة الأمن السيبراني التنسيق مع الإدارات ذات العلاقة لمتابعة الالتزام والتنفيذ.

8.1.8 على إدارة الأمن السيبراني مراجعة السياسة بشكل دوري وفقًا للخطة الزمنية التي تم تحديدها.

يجب على عمادة الاتصالات وتقنية المعلومات:

9.1.8 الالتزام بهذه السياسة، وتنفيذ الضوابط المذكورة في هذه السياسة وكذلك الإبلاغ عن أي حادث أمني لإدارة الأمن السيبراني.

يجب على الإدارة العليا ومدراء الإدارات ورؤساء الوحدات والمستشارين ما يلي:

10.1.8 التأكد من مشاركة هذه السياسة لجميع العاملين داخل الجامعة أو الملف.

11.1.8 إبلاغ إدارة الأمن السيبراني عن أي تجاوزات أو عدم التزام بهذه السياسة.

يجب على العاملين في الجامعة الالتزام بأحكام هذه السياسة والإبلاغ عن أي حادث أمني أوعدم التزام بأي أحكام واردة في هذه السياسة الى مدير الأمن السيبراني.

9. ملكية السياسة

المسؤول عن هذه السياسة هو مدير الأمن السيبراني في الجامعة.

10. تغييرات السياسة

يجب مراجعة السياسة سنويًا على الأقل أو عند حدوث تغييرات في المتطلبات التشريعية والتنظيمية، وتوثيق التغييرات واعتمادها من قبل صاحب الصلاحية في الجامعة.

11. الالتزام

يجب على جميع العاملين في الجامعة والأطراف (الخارجية/المتعاقد معهم) الالتزام بأحكام هذه السياسة، ويجب على مدير الأمن السيبراني في الجامعة ضمان المراقبة المستمرة للالتزام، ورفع التقارير اللازمة بهذا الشأن لصاحب الصلاحية بشكل دوري.

يجب اتخاذ الإجراءات اللازمة لضمان الالتزام بأحكام هذه السياسة، وذلك من خلال قيام إدارة الأمن السيبراني أو الإدارات ذات العلاقة بمراجعة دورية، واتخاذ إجراءات تصحيحية من قبل صاحب الصلاحية في الجامعة وفقاً للتوصيات المقدمة من قبل مدير الأمن السيبراني حيال أي انتهاك لأي من أحكام هذه السياسة، على أن تكون الإجراءات التأديبية متناسبة مع خطورة الحادثة وفقًا لما يسفر عنه التحقيق بهذا الخصوص، وتتضمن الإجراءات التأديبية على سبيل المثال لا الحصر الآتي:

- سحب صلاحية الوصول إلى البيانات وأصول تقنية المعلومات وأنظمة الجامعة المتصلة بها.

- توجيه إنذار خطي، أو إنهاء خدمة العامل أو حسب ما يراه الجامعة من إجراءات مناسبة.

يستوجب عدم الالتزام بأي من أحكام هذه السياسة -دون الحصول على استثناء مسبق من إدارة الأمن السيبراني - اتخاذ الإجراءات المناسبة وفقًا للسياسات واللوائح المعمول بها في الجامعة، أو حسبما يكون مناسبًا، ووفقًا للشروط التعاقدية مع أي أشخاص أو جهات متعاقد معهم.

12. السياسات والمعايير والإجراءات ذات العلاقة

- DICT.I.06-01.CS.A. V2.0- السياسة العامة للأمن السيبراني وحوكمة البيانات
- DICT.I.06-02.CS.A. V2.0- سياسة الالتزام بالأمن السيبراني وحوكمة البيانات
- DICT.I.06-33.CS.A. V2.0- سياسة التحكم في الوصول
- DICT.I.06-27.CS.A. V2.0 - سياسة الاستخدام المقبول للأصول
- DICT.I.06-04.CS.A. V2.0- سياسة إدارة الأصول
- DICT.I.06-15.CS.A. V2.0- سياسة كلمة المرور
- DICT.I.06-21.CS.A. V2.0- سياسة تصنيف البيانات
- DICT.I.06-07.CS.A. V2.0- سياسة إدارة النسخ الاحتياطي
- DICT.I.06-49.CS.A.V2.0- معايير إدارة هويات الدخول والصلاحيات
- DICT.I.06-60.CS.A.V2.0- معايير تصنيف الأصول
- DICT.I.06-62.CS.A.V2.0- معايير إدارة الأصول
- DICT.I.06-65.CS.A.V2.0- معايير إدارة النسخ الاحتياطي
- DICT.I.06-69.CS.A.V2.0- معايير كلمة المرور
- DICT.I.04-35.CS.A.V2.0- إجراءات إدارة النسخ الاحتياطي

13. المراجع

اسم القسم	الضوابط الأساسية للأمن السيبراني	ضوابط الأمن السيبراني للأنظمة الحساسة	ضوابط الأمن السيبراني للعمل عن بعد	ضوابط الأمن السيبراني التواصل للجهات	الأمن لحسابات الاجتماعي	ضوابط الأمن السيبراني للحوسبة السحابية	الآيزو 27001:2013	المعهد الوطني للمعايير والتقنية
متطلبات السحابة	3-4-2	1-2-4	1-1-3	-		1-ش-1-3	A.13.1.2	AC-20

----------نهاية الوثيقة----------