جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

السياسة العامة للأمن السيبراني

الإصدار: Version 2.0

رمز السياسة: DICT.I.06-01.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
8. منهجية الأمن السيبراني 7
9. مبادئ الأمن السيبراني 7
10. القيادة والالتزام اتجاه الأمن السيبراني 8
11. برنامج الأمن السيبراني 9
2.11 تشمل برامج الأمن السيبراني مجموعة من الاختصاصات ومنه أهمها ما يلي: 9
12. الأدوار والمسؤوليات 11
13. الاستثناءات 13
14. ملكية السياسة 13
15. تغييرات السياسة 13
16. الالتزام 14
17. السياسات والمعايير والإجراءات ذات العلاقة 15
18. المراجع 19

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
السياسة العامة للأمن السيبراني	مقيد	V2.0	فعال

2.3 تاريخ الإعداد والتّحديث

الإصدار	المؤلفون	تاريخ الإصدار	التغييرات
V1.0	د. بشار الذيب	2021/01/04	إنشاء
V1.1	د. سامر بني عواد	2022/03/07	مراجعة وتحديث
V2.0	بهاء نوافله	2023/12/16	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

أنشأ الجامعة إدارة أمن المعلومات للعمل على تطوير وإدارة العمليات لحماية بياناته وأصوله ولحماية البيانات الشخصية، نظرًا لأهمية ذلك في استمرارية عمل الجامعة بنجاح. تحدد هذه الوثيقة السياسة داخل الجامعة والمتطلبات الأمنية بناءً على أفضل الممارسات والمعايير واللوائح المعمول بها في هذا المجال.

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

5. الهدف

تحدد سياسة الأمن السيبراني الأنظمة والأحكام التي من شأنها المحافظة على أمن وسرية البيانات والبنية التحتية التقنية للجامعة، وتُعد جميع البيانات وأصول تقنية المعلومات ضرورية لعمليات الجامعة وتساهم في تحقيق أهدافه الاستراتيجية. ولذلك، فإنه من الضروري حوكمة هذه البيانات وحماية سريتها وسلامتها وتوافرها، وتهدف سياسة الأمن السيبراني إلى حماية أصول الجامعة من التهديدات وتخفيف أثر المخاطر بشكل فاعل.

تُطبق أحكام هذه السياسة وفقًا لسياسات حوكمة البيانات الوطنية الصادرة عن مكتب إدارة البيانات الوطنية ولمتطلبات الهيئة الوطنية للأمن السيبراني المتمثلة في الضوابط الأساسية للأمن السيبراني ونظام حماية البيانات الشخصية ومعيار الآيزو (27001) ومعايير المعهد الوطني للمعايير والتقنية (NIST) وأفضل الممارسات الدولية المعمول بها في المجال.

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.

7. السياسة

1.7 متطلبات السياسة العامة

1.1.7 يجب حماية البيانات وأصول تقنية المعلومات من التسريب، أو الوصول غير المصرح به، أو التهديدات، سواء كانت داخلية أو خارجية، مُتعمدة أو عَرضية.

2.1.7 يجب المحافظة على وثائق الأمن السيبراني والوثائق المساندة التي تمكن من إعداد وتنفيذ سياسات الأمن السيبراني داخل الجامعة. على أن تتضمن هذه الوثائق السياسات والإجراءات والمعايير والإرشادات المتعلقة بالمخاطر الأمنية وتقييمها.

3.1.7 على إدارة الأمن السيبراني إعداد سياسات وإجراءات ومعايير ومسؤوليات الأمن السيبراني وفقاً الأنظمة واللوائح والتشريعات وأفضل المعايير العالمية وتعميمها أو نشرها والالتزام بها، ويجب تطبيقها من قبل جميع العاملين في الجامعة والأطراف الخارجية/المتعاقدة كلاً فيما يخصه.

4.1.7 يجب التحكم في تتبع المستندات باستخدام معلومات الإصدار وتاريخ المستند وتفاصيل المراجعة، إن وجدت.

5.1.7 يجب استخدام وسيلة اتصال فاعلة لتعميم سياسات الأمن السيبراني داخل الجامعة.

6.1.7 يجب مراجعة جميع وثائق سياسات الأمن السيبراني من قبل الإدارات ذات العلاقة، وتحديثها بشكل دوري أو حسب الحاجة أو عند حدوث تغييرات في المتطلبات التشريعية والتنظيمية.

7.1.7 يجب التعامل مع المعلومات حسب التصنيف المحدد، وبما يتوافق مع سياسة تصنيف البيانات وسياسة حماية البيانات في الجامعة بشكل يضمن حماية سرية المعلومات وسلامتها وتوافرها.

8.1.7 يُمنع انتهاك حقوق أي شخص، أو شركة محمية بحقوق النشر، أو براءة الاختراع، أو أي ملكية فكرية أخرى، أو قوانين أو لوائح مماثلة؛ بما في ذلك، على سبيل المثال لا الحصر، تثبيت برامج غير مصرح بها أو غير قانونية.

8. منهجية الأمن السيبراني

1.1.8 يجب على إدارة الأمن السيبراني تطبيق منهجية (Plan-Do-Check-Act) الفاعلة في تحديد وإعداد ضوابط وإجراءات الأمن السيبراني ومراقبتها والمحافظة عليها وتحسينها بشكل مستمر.

2.1.8 تركز مرحلة التخطيط (Plan) على تحديد وتقييم مخاطر الأمن السيبراني وتحديد ضوابط المعالجة من أجل إدارة المخاطر.

3.1.8 تركز مرحلة التنفيذ (Do) على نشر الضوابط وتنفيذ خطط معالجة المخاطر للتخفيف من المخاطر وإدارتها.

4.1.8 تركز مرحلة التحقق (Check) على إجراء تدقيق الأمن السيبراني داخل الجامعة، والمزيد من المراقبة ومراجعة وتحديث الأدوات المستخدمة في ذلك، لضمان تطبيق الالتزامات والمتطلبات القانونية أو التنظيمية أو التعاقدية.

5.1.8 تركز مرحلة المباشرة (Act) على التعديل على ضوابط وإجراءات الأمن السيبراني داخل الجامعة، والتحسين المستمر لها.

9. مبادئ الأمن السيبراني

1.1.9 يجب المحافظة على سرية وسلامة وتوافر البيانات وأصول تقنية المعلومات، ووضع الضوابط اللازمة للسماح باستخدام هذه المعلومات والوصول إليها والإفصاح عنها وفقًا للأنظمة واللوائح والتشريعات وأفضل المعايير العالمية ذات الصلة.

2.1.9 تعتمد سياسات الأمن السيبراني في الجامعة على المبادئ العامة الآتية:

- **السرية**: ضمان عدم الوصول إلى البيانات إلا من قبل الأشخاص المصرح لهم فقط، وحماية البيانات السرية والبيانات الشخصية بالشكل اللازم.
- **السلامة**: ضمان الحفاظ على دقة واكتمال البيانات وطرق معالجة البيانات المرتبطة بها.
- **التوافر**: ضمان إمكانية وصول المستخدمين المصرح لهم إلى البيانات والأصول أو الأنظمة المرتبطة بها، في الوقت المناسب وإذا لزم الأمر.

3.1.9 يجب تحقيق متطلبات الأمن السيبراني من خلال فرض مجموعة مناسبة من الضوابط من قبل إدارة الأمن السيبراني، ويجب تنفيذ هذه الضوابط ومراجعتها عند الحاجة لذلك، لتحقيق أهداف الجامعة الخاصة بالأمن السيبراني.

10. القيادة والالتزام اتجاه الأمن السيبراني

1.1.10 يجب أن تحتفظ إدارة الأمن السيبراني بسجلات تثبت التزامه بضوابط الأمن السيبراني وتنفيذها وتفعيلها ومراقبتها ومراجعتها والمحافظة عليها، وذلك من خلال:

2.1.10 إعداد سياسات ومعايير وإجراءات الأمن السيبراني بما يتوافق مع متطلبات الجهات التنظيمية والتشريعية بالإضافة إلى الأهداف الاستراتيجية للجامعة.

3.1.10 وضع آلية لضمان وفاء الجامعة بمتطلبات الهيئة الوطنية للأمن السيبراني ومعيار الآيزو (27001) وكذلك متطلبات مكتب إدارة البيانات الوطنية والأحكام ذات العلاقة من نظام حماية البيانات الشخصية.

4.1.10 تحديد الأدوار والمسؤوليات لتحقيق أهداف الأمن السيبراني داخل الجامعة، ومراجعة تلك الأدوار والمسؤوليات بشكل دوري أو حسب الحاجة أو عند حدوث تغييرات في المتطلبات التشريعية والتنظيمية.

5.1.10 على إدارة الأمن السيبراني تحقيق أهداف الأمن السيبراني للجامعة، وفقًا لسياسات الأمن السيبراني ومسؤوليات الجامعة بموجب الأحكام النظامية واللوائح ذات الصلة، ومراجعتها وتحسينها بشكل مستمر.

6.1.10 توفير موارد كافية لإعداد ممارسات الأمن السيبراني، وتنفيذها وتفعيلها ورصدها ومراجعتها وتحسينها والمحافظة عليها.

7.1.10 توجيه ودعم المشاركين في تنفيذ سياسات الأمن السيبراني من العاملين في الجامعة أو الأطراف (الأخرى/المتعاقد معهم)، وتقديم الدعم اللازم لهم.

8.1.10 تحديد إجراءات ومعايير إدارة وتقييم مخاطر الأمن السيبراني ومستويات الخطر، ومراجعتها بشكل دوري أو حسب الحاجة أو عند حدوث تغييرات في المتطلبات التشريعية والتنظيمية.

9.1.10 التأكد من إجراء عمليات التدقيق الداخلي للأمن السيبراني.

10.1.10 اتخاذ الإجراءات التصحيحية بناءً على نتائج عمليات التدقيق الداخلي، والحوادث الأمنية، وعمليات التدقيق الخارجية، لضمان التحسين المستمر، والتأكد من أن ممارسات الأمن السيبراني تحقق النتائج المرجوة منها.

11. برنامج الأمن السيبراني

1.1.11 يجب على إدارة الأمن السيبراني تحديد إجراءات ومعايير الأمن السيبراني وتوثيق سياساته وبرامجه، بناءً على نتائج تقييم مخاطر الأمن السيبراني، وبشكل يضمن نشر متطلبات الأمن السيبراني، والتزام الجامعة بها، وذلك وفقاً لمتطلبات الأعمال التنظيمية للجامعة، والمتطلبات التشريعية والتنظيمية ذات العلاقة. واعتمادها من قبل صاحب الصلاحية في الجامعة. كما يجب إطلاع العاملين المعنيين في الجامعة عليها وتأكيد الالتزام بها.

2.11 تشمل برامج الأمن السيبراني مجموعة من الاختصاصات ومنه أهمها ما يلي:

1.2.11 استراتيجية الأمن السيبراني

يهدف إلى ضمان إنفاذ خطط العمل والمبادرات والمشاريع المتصلة بالأمن السيبراني، وفقًا للأهداف الاستراتيجية المعتمدة، والمتطلبات التشريعية والتنظيمية، والأحكام النظامية واللوائح ذات الصلة.

2.2.11 إدارة مخاطر الأمن السيبراني

إدارة مخاطر الأمن السيبراني على نحو ممنهج، بما يكفل حماية المعلومات والبيانات والأصول التقنية، وفقًا للأهداف والسياسات المعتمدة، والمتطلبات التشريعية والتنظيمية، والأحكام النظامية واللوائح ذات الصلة.

3.2.11 حماية البيانات

المحافظة على أمن المعلومات وسرية البيانات وحماية البيانات الشخصية، بما يكفل وسلامتها ودقتها وتوافرها، وفقًا للأهداف والسياسات المعتمدة، والمتطلبات التشريعية والتنظيمية، والأحكام النظامية واللوائح ذات الصلة.

4.2.11 إدارة التحكم في الوصول

رفع مستوى حماية أمن المعلومات من خلال وضع ضوابط محددة للوصول إلى البيانات واستخدام أصول تقنية المعلومات، ومنع الوصول غير المصرح به، وتقييد الوصول إلى الحد المطلوب للقيام بالمهام الأنشطة ذات الصلة بأعمال الجامعة.

5.2.11 إدارة سجلات الأحداث ومراقبة الأمن السيبراني

ضبط عمليات جمع سجلات أحداث الأمن السيبراني وتحليلها ومراقبتها في الوقت المناسب؛ وذلك لاستشراف الهجمات السيبرانية واكتشافها وإدارة مخاطرها بفاعلية؛ للحد من أي آثار سلبية محتملة على البيانات أو أعمال الجامعة.

6.2.11 إدارة حوادث وتهديدات الأمن السيبراني

تمكين إدارة الأمن السيبراني من استشراف حوادث الأمن السيبراني واكتشافها وتحديدها في الوقت المناسب، وإدارتها بشكل فاعل، والتعامل مع هجمات أو تهديدات الأمن السيبراني استباقياً، للحد من أي آثار سلبية محتملة على البيانات أو أعمال الجامعة، وفقاً للمتطلبات التنظيمية والتشريعية.

7.2.11 الالتزام بالأمن السيبراني

رصد مخالفات عدم الالتزام بضوابط ومتطلبات الأمن السيبراني، بما في ذلك أي مخالفة للسياسات أو للمعايير المعمول بها أو للأحكام النظامية أو اللوائح ذات الصلة، ومعالجتها وفقاً للسياسات والمعايير والإجراءات المعتمدة، بما يكفل التحسين المستمر لممارسات الأمن السيبراني في الجامعة.

8.2.11 التدريب والتوعية بالأمن السيبراني

- يهدف هذا البرنامج إلى رفع مستوى الوعي لدى العاملين بالجامعة وتعزيز الدراية الكافية بمسؤولياتهم في مجال الأمن السيبراني، وتطوير مهارات العاملين في الجامعة، وتقديم البرامج التوعوية اللازمة لهم؛ بما يكفل قيامهم بمسؤولياتهم لحماية الأصول المعلوماتية والتقنية للجامعة.
- يجب أن يكون التحسين المستمر للوعي بين العاملين في الجامعة أحد المبادرات الرئيسة نحو تحسين الجودة العامة للأمن السيبراني.
- يجب تقييم وعي المستخدم بناءً على طرق التقييم المناسبة التي تقدمها إدارة الأمن السيبراني.
- يجب أن يشمل برنامج التوعية بالأمن السيبراني في الجامعة على ما يلي:
  - الاستخدام الآمن للأجهزة المخصصة للعمل عن بعد والمحافظة عليها وحاميتها
  - التعامل الآمن مع هويات الدخول وكلمات المرور.

- حماية البيانات التي يتم حفظها على الأجهزة المستخدمة للعمل عن بعد والتعامل معها حسب تصنيفها وإجراءات وسياسات الجامعة.
- التعامل الآمن مع التطبيقات والحلول المستخدمة للعمل عن بعد كالاجتماعات الافتراضية، والتعاون ومشاركة الملفات.
- التعامل الآمن مع الشبكات المنزلية والتأكد من إعداد الحماية الخاصة بها.
- تجنب العمل عن بعد باستخدام أجهزة أو شبكات عامة غير موثوقة أو أثناء التواجد في أماكن عامة.
- الوصول المادي غير المصرح به والفقدان والتخريب للأصول التقنية وأنظمة العمل عن بعد.
- التواصل مباشرة مع إدارة الأمن السيبراني في حال الاشتباه بتهديد أمن سيبراني.

12. الأدوار والمسؤوليات

يجب على إدارة الأمن السيبراني القيام بالآتي:

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

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

3.1.12 على مدير الأمن السيبراني التوصية بإنشاء لجنة إشرافية للأمن السيبراني ويكون مدير الأمن السيبراني أحد أعضائها.

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

5.1.12 على مدير الأمن السيبراني حل أي تعارضات تنشأ عن هذه السياسة.

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

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

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

يجب على المدير التنفيذي للشؤون القانونية:

9.1.12 التأكد من أن جميع سياسات الأمن السيبراني تتوافق مع الممارسات الحالية داخل الجامعة ومع المتطلبات التشريعية والتنظيمية، والأحكام النظامية واللوائح من الناحية القانونية ومن منطلق الالتزام.

10.1.12 التأكد من أن شروط ومتطلبات الأمن السيبراني وسرية المعلومات وحماية البيانات الشخصية الواردة في بنود تعهد المحافظة على السرية وعقود العاملين لدى الجامعة والأطراف (الخارجية/المتعاقد معها) مُلزمة نظاماً.

يجب على مدير ضمان الجودة:

11.1.12 مراجعة دورية لتطبيق ضوابط الأمن السيبراني وفقاً للمعايير العامة المعمول بها للمراجعة والتدقيق، والمتطلبات التشريعية والتنظيمية، والأحكام النظامية واللوائح ذات الصلة.

يجب على المدير التنفيذي لإدارة الموارد البشرية:

12.1.12 تطبيق متطلبات سياسة أمن الموارد البشرية.

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

13.1.12 التأكد من إقرار جميع عاملي الإدارة بقراءة وفهم سياسات الأمن السيبراني.

14.1.12 تعزيز مستوى الالتزام والامتثال من قبل جميع العاملين لسياسات الأمن السيبراني الخاصة بالجامعة.

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

13. الاستثناءات

- يُمنع تجاوز سياسات الأمن السيبراني والمعايير والإجراءات، دون الحصول على تصريح رسمي مسبق من مدير الأمن السيبراني، ما لم يتعارض مع المتطلبات التشريعية والتنظيمية والأحكام النظامية واللوائح ذات الصلة.
- إذا كانت هناك حاجة ملحة للإعفاء من مسؤوليات في أحد سياسات الأمن السيبراني مع عدم وجود بديل قابل للتطبيق وآمن، يتعين طلب الاستثناء من قبل مدير الأمن السيبراني مع توضيح سبب ومدة الحاجة للصلاحية ووصف تفصيلي لنطاق ومبرراته.
- تتولى إدارة الأمن السيبراني مسؤولية مراجعة الطلب وتحديد المخاطر والضوابط الإضافية وفق للمنهجية المعتمدة لإدارة مخاطر الأمن السيبراني في الجامعة وقد تطلب من مقدم الطلب الموافقة على المخاطر المحددة والضوابط الإضافية عند الحاجة.
- يجوز لإدارة الأمن السيبراني استشارة جهات داخلية وخارجية معنية بالمسائل القانونية والتنظيمية.
- يتم توثيق جميع الاستثناءات للأمن السيبراني وإشعار اللجنة الإشرافية للأمن السيبراني بجميع طلبات الاستثناءات.
- تمتلك إدارة الأمن السيبراني صلاحية إلغاء الاستثناءات بعد زوال الأسباب التي تستدعي وجودها.

14. ملكية السياسة

المسؤول عن هذه السياسة هو مدير الأمن السيبراني بالجامعة.

15. 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.

16. 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.

17. السياسات والمعاييروالإجراءات ذات العلاقة

- DICT.I.06-02.CS.A. V2.0- سياسة الالتزام بالأمن السيبراني
- DICT.I.06-24.CS.A. V2.0- سياسة إدارة مخاطر الأمن السيبراني
- DICT.I.06-28.CS.A. V2.0- سياسة الأمن السيبراني ضمن استمرارية الأعمال
- DICT.I.06-25.CS.A. V2.0- سياسة أمن الموارد البشرية
- DICT.I.06-41.CS.A. V2.0- سياسة أمن الأطراف الخارجية والموردين
- DICT.I.06-32.CS.A. V2.0- سياسة الأمن المادي والبيئي
- DICT.I.06-03.CS.A. V2.0- سياسة حماية البيانات
- DICT.I.06-20.CS.A. V2.0- سياسة تخزين واستبقاء البيانات
- DICT.I.06-21.CS.A. V2.0- سياسة تصنيف البيانات
- DICT.I.06-13.CS.A. V2.0- سياسة حماية البيانات الشخصية
- DICT.I.06-29.CS.A. V2.0- سياسة التشفير
- DICT.I.06-09.CS.A. V2.0- سياسة إدارة حوادث الأمن السيبراني
- DICT.I.06-10.CS.A. V2.0- سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني
- DICT.I.06-05.CS.A. V2.0- سياسة إدارة الثغرات واختبار الاختراق
- DICT.I.06-30.CS.A. V2.0- سياسة الحماية من البرمجيات الضارة
- DICT.I.06-42.CS.A. V2.0- سياسة أمن الأجهزة المحمولة والأجهزة الشخصية
- DICT.I.06-43.CS.A. V2.0- سياسة أمن الحوسبة السحابية
- DICT.I.06-22.CS.A. V2.0- سياسة اقتناء النظام وتطويره وصيانته
- DICT.I.06-07.CS.A. V2.0- سياسة إدارة النسخ الاحتياطي
- DICT.I.06-08.CS.A. V2.0- سياسة إدارة حزم التحديثات والإصلاحات
- DICT.I.06-26.CS.A. V2.0- سياسة الجامعة النظيف والشاشة الخالية

- DICT.I.06-04.CS.A. V2.0- سياسة إدارة الأصول
- DICT.I.06-06.CS.A. V2.0- سياسة إدارة التغيير
- DICT.I.06-27.CS.A. V2.0- سياسة الاستخدام المقبول للأصول
- DICT.I.06-33.CS.A. V2.0- سياسة التحكم في الوصول
- DICT.I.06-44.CS.A. V2.0- سياسة أمن البريد الإلكتروني
- DICT.I.06-15.CS.A. V2.0- سياسة كلمة المرور
- DICT.I.06-14.CS.A. V2.0- سياسة حماية تطبيقات الويب
- DICT.I.06-12.CS.A. V2.0- سياسة ملفات تعريف الارتباط
- DICT.I.06-38.CS.A. V2.0- سياسة الإعدادات والتحصين
- DICT.I.06-34.CS.A. V2.0- سياسة الأمن السيبراني ضمن إدارة المشاريع
- DICT.I.06-11.CS.A. V2.0- سياسة مشاركة البيانات
- DICT.I.06-37.CS.A. V2.0- سياسة الأمن السيبراني للعمل عن بعد
- DICT.I.06-40.CS.A. V2.0- سياسة أمن العمليات
- DICT.I.06-35.CS.A. V2.0- سياسة الأمن السيبراني لحسابات التواصل الاجتماعي
- DICT.I.06-36.CS.A. V2.0- سياسة الأمن السيبراني لحماية الطابعات والماسحات الضوئية و وآلات التصوير
- DICT.I.06-45.CS.A. V2.0- سياسة مراجعة وتدقيق الأمن السيبراني
- DICT.I.06-46.CS.A. V2.0- سياسة أمن وسائط التخزين
- DICT.I.06-47.CS.A. V2.0- سياسة دورة حياة تطوير البرمجيات الآمنة
- DICT.I.06-48.CS.A.V2.0- معايير أجهزة المستخدم ذات الصلاحيات الهامة والحساسة
- DICT.I.06-49.CS.A.V2.0- معايير إدارة هويات الدخول والصلاحيات
- DICT.I.06-50.CS.A.V2.0- معايير الأمن المادي
- DICT.I.06-51.CS.A.V2.0- معايير التطوير الآمن للتطبيقات

- DICT.I.06-52.CS.A.V2.0- معايير الحماية من التهديدات المستمرة المتقدمة
- DICT.I.06-53.CS.A.V2.0- معايير الحماية من فقدان البيانات
- DICT.I.06-54.CS.A.V2.0- معايير الكشف عن تهديدات الشبكات والاستجابة لها
- DICT.I.06-55.CS.A.V2.0- معايير أمن البريد الإلكتروني
- DICT.I.06-56.CS.A.V2.0- معايير أمن البيانات
- DICT.I.06-57.CS.A.V2.0- معايير أمن البيئة الافتراضية
- DICT.I.06-58.CS.A.V2.0- معايير أمن قواعد البيانات
- DICT.I.06-59.CS.A.V2.0- معايير أمن وسائل التواصل الاجتماعي
- DICT.I.06-60.CS.A.V2.0- معايير تصنيف الأصول
- DICT.I.06-61.CS.A.V2.0- معايير حماية البيانات
- DICT.I.06-62.CS.A.V2.0- معايير إدارة الأصول
- DICT.I.06-63.CS.A.V2.0- معايير إدارة الثغرات واختبار الاختراق
- DICT.I.06-64.CS.A.V2.0- معايير إدارة التغيير
- DICT.I.06-65.CS.A.V2.0- معايير إدارة النسخ الاحتياطي
- DICT.I.06-66.CS.A.V2.0- معايير إدارة حزم التحديثات والإصلاحات
- DICT.I.06-67.CS.A.V2.0- معايير إدارة حوادث الأمن السيبراني
- DICT.I.06-68.CS.A.V2.0- معايير إدارة سجلات الأحداث ومراقبة الأمن السيبراني
- DICT.I.06-69.CS.A.V2.0- معايير كلمة المرور
- DICT.I.06-70.CS.A.V2.0- معايير اقتناء النظام وتطويره وصيانته
- DICT.I.06-71.CS.A.V2.0- معايير التشفير
- DICT.I.06-72.CS.A.V2.0- معايير الحماية من البرمجيات الضارة
- DICT.I.06-73.CS.A.V2.0- معايير حماية تطبيقات الويب

- DICT.I.06-74.CS.A.V2.0- معايير الأمن السيبراني ضمن إدارة المشاريع
- DICT.I.06-75.CS.A.V2.0-معايير الإعدادات والتحصين
- DICT.I.06-76.CS.A.V2.0-معايير أمن الخوادم
- DICT.I.06-77.CS.A.V2.0- معايير أمن الشبكات
- DICT.I.06-78.CS.A.V2.0- معايير أمن الاطراف الخارجية والموردين
- DICT.I.06-79.CS.A.V2.0- معايير أمن الأجهزة المحمولة والأجهزة الشخصية
- DICT.I.06-80.CS.A.V2.0- معايير أمن الخادم الوكيل
- DICT.I.04-34.CS.A.V2.0- إجراءات إدارة التغيير
- DICT.I.04-35.CS.A.V2.0- إجراءات إدارة النسخ الاحتياطي
- DICT.I.04-36.CS.A.V2.0- إجراءات اقتناء النظام وتطويره وصيانته
- DICT.I.04-37.CS.A.V2.0- إجراءات الحماية من البرمجيات الضارة
- DICT.I.04-38.CS.A.V2.0- إجراءات تدقيق الأمن السيبراني
- DICT.I.04-39.CS.A.V2.0- إجراءات تقييم الثغرات الأمنية
- DICT.I.04-40.CS.A.V2.0- إجراءات إدارة مخاطر الأمن السيبراني
- DICT.I.04-41.CS.A.V2.0- إجراءات تطوير وثائق الأمن السيبراني
- DICT.I.04-42.CS.A.V2.0- إجراءات التخلص من الأصول واتلاف الوسائط

18. المراجع

اسم القسم	الضوابط الأساسية للأمن السيبراني	ضوابط الأمن السيبراني للأنظمة الحساسة	ضوابط الأمن السيبراني للعمل عن بعد	ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات	ضوابط الأمن السيبراني للحوسبة السحابية	الآيزو 27001:2013	المعهد الوطني للمعايير والتقنية
سياسة ضوابط الوصول	2-2	2-2	2-2	2-2	2-2	A.9.1.1	AC-1, MP-1
سياسة تصنيف المعلومات	7-2	6-2	6-2	5-2	-	A.8.2	RA-2, AC-3, AC-4, AC-16, MP-2, MP-3, SC-16
سياسة تخفيف التهديد الداخلي	-	-	-	-	-	A.12.2.1	PM-12
سياسة أمن العمليات	-	-	-	-	-	A.12.1	SC-38
سياسة الاستخدام المقبول للأصول	1-2	-	-	-	-	A.8.1.3	AC-20, PL-4, PS-6
سياسة أمن الموردين والأطراف الخارجية	1-4	1-4	-	1-3	1-4	A.15.1.1	PL-8, SA-12
سياسة إدارة الحوادث	13-2	-	12-2	7-2	-	A.16	AU-6, IR-1, IR-6
سياسة إدارة الأصول	1-2	1-2	1-2	1-2	1-2	A.8	PM-5, CM-8, CM-9
سياسة أحضر الجهاز الخاص بك (BYOD)	6-2	5-2	5-2	4-2	5-2	A.6.2.1	AC-19
سياسة أمن كلمة المرور	2-2	2-2	2-2	2-2	-	A.9.2.3	IA-5
سياسة الجامعة النظيف والشاشة الخالية	-	-	-	-	-	A.11.2.9	AC-1, AC-11, MP-1, MP-2, MP-4
سياسة إدارة التغيير	6-1	3-1	-	-	-	A.12.1.2	CM-2, CM-3, CM-4, CM-5, CM-9, SA-10
سياسة النسخ الاحتياطي	9-2	8-2	8-2	-	-	A.12.3.1	CP-9
سياسة أمن الموارد البشرية	9-1	5-1	3-1	3-1	4-1	A.7	XX-1 controls, PL-4, PS-2, PS-6, PS-7
سياسة التشفير	8-2	7-2	7-2	-	7-2	A.10.1.1	SC-12, SC-13

		15-2					
سياسة الأمن المادي والبيئي	14-2	-	-	-	-	A.11	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.9.1.4, A.9.1.5, A.10.1.1, A.15.1.1, A.15.2.1
سياسة ملكية النظام وتطويره وصيانته	6-1	3-1 13-2	-	-	-	A.14	SA-1, SA-4
سياسة الحماية من البرمجيات الضارة	3-2	3-2	-	3-2	-	A.12.2.1	SI-3
سياسة أمن الشبكات	5-2	4-2	4-2	-	-	A.13.1	AC-3, AC-17, AC-18, AC-20, CA-3, SC-5, SC-7, SC-8, SC-10
سياسة استمرارية الاعمال والأمن السيبراني	1-3	1-3	-	-	-	A.17.1	CP-1, CP-2, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13
سياسة الالتزام بالأمن السيبراني	-	-	-	-	-	A.18	XX-1 controls, CA-2, CA-7
سياسة البريد الإلكتروني	4-2	-	-	-	-	A.13.2.1, A.13.2.3	AC-3, PT-4, DS-2
سياسة أمن الحوسبة السحابية	2-4	2-4	1-3	1-3	-	A.13.1.2	AC-20
سياسة إدارة سجلات الأحداث والمراقبة	12-2	11-2	11-2	6-2	11-2	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4	PT-1, AE-2, AE-3, CM-3, CM-7,
إدارة حزم التحديثات والإصلاحات	3-2	3-2	3-2	3-2	-	A.12.6.1, A.8.2.1	RA-5
سياسة حماية تطبيقات الويب	15-2	12-2	-	-	-	A.14.1.2, A.14.1.3, A.14.2.8	-
سياسة إدارة الثغرات واختبار الاختراق	10-2 11-2	9-2 10-2	9-2	-	9-2	A.12.6.1	IP-12, CM-8, MI-3, RA-1
سياسة حماية البيانات	7-2	6-2	6-2	5-2	6-2	-	-

سياسة ملفات الارتباط(Cookie)	-	-	-	-	-	-	-
سياسة العمل عن بعد	-	-	4-2	-	-	A.6.2.2	-
سياسة أمن العمليات	-	-	-	-	-	-	-
سياسة مشاركة البيانات	-	-	-	-	-	-	-
سياسة إدارة البيانات	-	-	-	-	-	-	-
سياسة تخزين البيانات	-	-	-	-	-	-	-
سياسة الأمن السيبراني لحماية الطابعات والماسحات الضوئية بالآلات التصوير	-	-	-	-	-	-	-

---------- نهاية الوثيقة ----------