جامعة الإمام عبد الرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

سياسة الالتزام بالأمن السيبراني وحوكمة البيانات

الإصدار: Version 2.0

رمز السياسة: DICT.I.06-02.CS.A. V2.0

1. جدول المحتويات

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 الالتزام بالأمن السيبراني وحوكمة البيانات	مقيد	V2.0	فعال

2.3 تاريخ الإعداد والتّحديث

الإصدار	المؤلفون	تاريخ الاصدار	التغييرات
V1.0	د. بشار الذيب	2021/02/02	إنشاء
V1.1	د. سامر بني عواد	2022/03/14	مراجعة وتحديث
V2.0	بهاء نوافله	2023/12/15	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

حماية الأصول المعلوماتية والتقنية أمر ضروري لنجاح الجامعة ولهذه الغاية؛ تقوم إدارة الأمن السيبراني بالعمل على تطوير حوكمة أمن المعلومات والاشراف على إدارة العمليات الأمنية المطلوبة لحماية بياناته وأصوله ولحماية البيانات الشخصية، نظراً لأهمية ذلك في استمرارية عمل الجامعة بنجاح. تحدد هذه الوثيقة سياسة الالتزام بالأمن السيبراني وحوكمة البيانات بناءً على أفضل الممارسات العالمية والمعايير واللوائح.

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

5. الهدف

الهدف من سياسة الالتزام هو ضمان امتثال الجامعة للالتزامات النظامية والتعاقدية فيما يتعلق بمتطلبات الأمن السيبراني وحوكمة البيانات وحقوق الملكية الفكرية وحقوق النشر بالنسبة لاستخدام أنظمة تقنية المعلومات وكافة أنواع البيانات وأصول تقنية المعلومات الخاصة بالجامعة.

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 بنود السياسة

1.1.7 يجب تحديد ومراجعة سياسات الأمن السيبراني وحوكمة البيانات بشكل دوري بناء على خطة زمنية محددة ومعتمدة ومتابعة تطبيقها.

2.1.7 يجب تحديد مسؤوليات الجامعة ومسؤوليات الممثلين النظاميين المعتمدين التي تتعلق بالتعامل مع مسائل وقضايا الالتزام، والإبلاغ عنها وحلها.

3.1.7 يجب على الإدارة العليا وإدارة الأمن السيبراني في الجامعة العمل مع الإدارة المعنية بالمراجعة الداخلية لضمان تحقيق مستويات الالتزام المطلوبة.

4.1.7 يجب الالتزام بجميع المتطلبات التنظيمية والأحكام النظامية واللوائح ذات الصلة بأعمال الجامعة والسياسات واللوائح والتعاميم والتعليمات والمتطلبات المعمول بها على المستوى الوطني التي تصدرها وتنشرها حكومة المملكة العربية السعودية.

5.1.7 يجب حصر الأنظمة واللوائح والوثائق التنظيمية والتشريعية ذات العلاقة بالأمن السيبراني وحوكمة البيانات، والمتطلبات ذات الصلة.

6.1.7 يجب توفير التقنيات اللازمة والكفاءات اللازمة؛ للتحقق من الالتزام بمتطلبات الجهات التشريعية والتنظيمية ومتطلبات الجامعة المتعلقة بالأمن السيبراني وحوكمة البيانات.

7.1.7 يجب التأكد من تطبيق سياسات الأمن السيبراني وحوكمة البيانات وإجراءاته بشكل دوري بناءً على خطة زمنية محددة ومعتمدة من قبل صاحب الصلاحية في الجامعة عن طريق استخدام الأدوات المناسبة مثل:

- أنشطة تقييم أخطار الأمن السيبراني (Cybersecurity Risk Assessment).
- أنشطة إدارة الثغرات (Vulnerabilities Management).
- أنشطة اختبار الاختراقات (Penetration Test).
- مراجعة معايير الأمن السيبراني وحوكمة البيانات.
- المراجعة الأمنية للشفرة المصدرية (Security Source Code Review).
- استبيانات المستخدمين.
- مراجعة الصلاحيات على النظام والشبكة.
- مراجعة سجلات الأمن السيبراني وحوادثه.

8.1.7 يجب تحديد الإجراءات التصحيحية اللازمة والعمل على تطبيقها؛ لتصحيح الثغرات لجميع متطلبات الالتزام من قبل إدارة الأمن السيبراني.

9.1.7 يجب أن يتم إرفاق إشعار إخلاء المسؤولية وبيان السرية والخصوصية مع المعلومات المنشورة بواسطة البريد الإلكتروني والتعاميم والإشعارات وجميع أشكال الاتصالات الأخرى لضمان معرفة المستلمين بالقيود الموضوعة على البيانات المرسلة.

10.1.7 يجب تنفيذ الإجراءات المناسبة لضمان الالتزام بالمتطلبات التشريعية والتنظيمية، المتعلقة بسرية وخصوصية البيانات وبحقوق الملكية الفكرية، واستخدام البرمجيات.

11.1.7 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر للالتزام بالأمن السيبراني وحوكمة البيانات.

2.7 حقوق الملكية الفكرية

1.2.7 يجب الالتزام بالقيود النظامية المفروضة على حقوق الملكية الفكرية (مثل حقوق النشر والعلامات التجارية وتطبيقات البرمجيات وغيرها) بناءً على المتطلبات التنظيمية.

2.2.7 يُمنع منعًا باتًا استخدام نُسخ مقرصنة من البرمجيات داخل الجامعة.

3.2.7 يجب أن يقوم الجامعة بتوعية مختلف الإدارات/أصحاب المصلحة لحماية حقوق الملكية الفكرية وإخطارهم باتخاذ إجراءات تأديبية ضد الأفراد الذين ينتهكون هذه الحقوق.

4.2.7 يجب تحديد جميع أصول تقنية المعلومات التي تتطلب حماية حقوق الملكية الفكرية.

5.2.7 يجب أن يحتفظ الجامعة بالإثباتات والأدلة على ملكية التراخيص والأقراص الرئيسية والأدلة الإرشادية التي تحتوي على مواد متعلقة بحقوق الملكية الفكرية، على أن يتم الاحتفاظ بها وفقاً لأحكام سياسة تخزين واستبقاء البيانات.

3.7 حماية وثائق الجامعة

1.3.7 يجب تحديد وتنفيذ إجراءات للتعامل مع بيانات الجامعة وإجراءات الاحتفاظ بها وآلية التخلص منها وفقًا للمتطلبات القانونية والتشريعية والتنظيمية والتعاقدية ذات العلاقة ولسياسة حوكمة البيانات وسياسة حماية البيانات المعمول بها في الجامعة.

2.3.7 يجب الاحتفاظ بوثائق الجامعة وتخزينها وفقاً سياسة تخزين واستبقاء البيانات.

3.3.7 يجب تصنيف وثائق الجامعة بناءً على نوعها وأهميتها وسريتها وفقاً لسياسة تصنيف البيانات.

4.7 حماية البيانات الشخصية

1.4.7 يجب مراعاة حماية البيانات الشخصية حسب متطلبات التنظيمية والتشريعات واللوائح ذات الصلة، وعلى إدارة الأمن السيبراني اقتراح البنود اللازمة لإضافتها في الوثائق التعاقدية وبقية مستندات الجامعة ذات العلاقة.

2.4.7 يجب تطبيق الضوابط الأمنية لحماية البيانات الشخصية بناءً على مستوى تصنيف البيانات ودرجة الأثر وفقاً لسياسة تصنيف البيانات في الجامعة.

3.4.7 يجب إجراء التدريبات التوعوية للمستخدمين لاطلاعهم على أنظمة حماية البيانات الشخصية المعمول بها.

4.4.7 يجب حماية البيانات الشخصية من التسرب، أو التلف، أو الفقدان، أو الاختلاس، أو النقل، أو النسخ، أو الاقتباس، أو إساءة الاستخدام، أو التعديل، أو الوصول غير المصرح به وفقاً لسياسات الجامعة المعتمدة ولما يصدر عن مكتب إدارة البيانات الوطنية والهيئة الوطنية للأمن السيبراني ونظام حماية البيانات الشخصية والجهات ذات الاختصاص.

5.7 منع إساءة استخدام مرافق معالجة المعلومات

1.5.7 يمنع استخدام مرافق معالجة معلومات الجامعة لأغراض غير مصرح بها.

2.5.7 يجب اتخاذ الإجراءات اللازمة لضمان حصول مرافق تقنية المعلومات على الحماية الكافية بموجب التشريعات ذات الصلة، وكحد أدنى:

- إجراء توعية للمستخدمين عن مسائل الالتزام وتشجيعهم على الإبلاغ عن عدم الالتزام.
- مراقبة أنظمة البيانات والمعلومات لرصد الاستخدام غير المصرح به.

6.7 الالتزام بالسياسات والمعايير الأمنية

1.6.7 يجب إطلاع العاملين على سياسات الأمن السيبراني وحوكمة البيانات، وإتاحتها للمتعاقدين والأطراف الخارجية

2.6.7 يجب إتاحة جميع سياسات الأمن السيبراني وحوكمة البيانات في الشبكة الداخلية الخاصة بالجامعة للرجوع إليها.

3.6.7 يجب التأكد من تنفيذ العاملين لجميع الإجراءات والإرشادات المتعلقة بمسؤولياتهم.

4.6.7 يجب التأكد من تطبيق سياسات الأمن السيبراني وحوكمة البيانات وإجراءاتها بشكل دوري بناءً على خطة زمنية محددة.

5.6.7 يجب وضع الإجراءات التصحيحية المناسبة والضوابط الوقائية وتحديد أولوياتها وتنفيذها في الوقت المناسب لمعالجة نقاط الضعف الأمنية التي تم تحديدها من قبل إدارة الأمن السيبراني.

6.6.7 يجب وضع المقاييس والأدوات اللازمة للمساعدة في تقييم برنامج الالتزام وتحسينه.

7.6.7 يجب التأكد من عمليات التحسين المستمر عن طريق تفعيل المراقبة والمتابعة.

8.6.7 يجب تحديث سجلات تقييم أخطار الأمن السيبراني بشكل دوري لتشمل التهديدات الجديدة والثغرات.

7.7 التقييمات التقنية للالتزام

1.7.7 يجب على إدارة الأمن السيبراني إجراء تقييم تقني للالتزام بشكل منتظم على أن يشمل فحص الأنظمة التشغيلية لضمان التنفيذ الصحيح لضوابط الأجهزة والبرمجيات.

2.7.7 يجب أن يشمل التقييم التقني اختبارات الاختراق وتقييمات الثغرات الأمنية التي يمكن إجراؤها داخليًا أو بواسطة خبراء مستقلين تم التعاقد معهم خصيصًا لهذا الغرض.

3.7.7 يجب إجراء تقييم تقني بشكل دوري لضمان الالتزام بمتطلبات المعايير الأمنية لدى الجامعة بما يتوافق مع الحد الأدنى من التحكم الأمني (Minimum Security Baseline).

8.7 الوعي بالواجبات القانونية

1.8.7 يجب أن يكون جميع العاملين على علم بمسؤولياتهم فيما يتعلق باستخدامهم للبيانات والأصول التقنية والمعلوماتية لتجنب المسائلات القانونية في حال مخالفة ذلك.

2.8.7 يترتب على عدم التزام العاملين بالجوانب القانونية لاستخدام البيانات وأصول تقنية المعلومات اتخاذ الاجراءات التأديبية المنصوص عليها في اللوائح والسياسات ذات العلاقات، إضافة إلى أي عقوبات أخرى نصت عليها الأنظمة أو اللوائح ذات الصلة، بما فيها نظام عقوبات نشر الوثائق والمعلومات السرية وإفشائها.

9.7 الالتزام بالتشريعات العامة لحقوق النشر

1.9.7 يعد نسخ المواد المحفوظة بموجب حقوق النشر انتهاكًا للأنظمة واللوائح ذات الصلة، ويُعتبر التعدي على حق المؤلف أمرًا جنائيًا.

2.9.7 يترتب على عدم الإلمام بأنظمة حقوق النشر وحدوث انتهاكات غير مقصودة؛ اتخاذ الإجراءات القانونية اللازمة وفقاً للأحكام النظامية واللوائح ذات الصلة.

3.9.7 يترتب على عدم الالتزام بالمتطلبات القانونية المتعلقة بتراخيص البرمجيات؛ اتخاذ الإجراء النظامي ضد المستخدم.

4.9.7 تلتزم هذه السياسة أيضًا بحماية حقوق نشر المعلومات المتعلقة بقواعد البيانات.

10.7 تشريعات ترخيص حقوق النشر والبرمجيات

1.10.7 يجب عدم نسخ البرمجيات وتوزيعها ما لم يمنح المسؤول عن إدارة الأمن السيبراني إذنًا صريحًا بذلك.

2.10.7 يجب عدم مشاركة أو توزيع نسخ البرمجيات بدون وجود ترخيص من مالك البرمجيات.

3.10.7 يجب عدم نسخ البرمجيات وتوزيعها عبر الشبكة وأي نشاط غير قانوني يهدد سلامة الجامعة أو إمكانية اتخاذ إجراء قانوني ضده.

4.10.7 يترتب على استخدام البرمجيات غير المرخصة من قبل المتعاقدين والمستشارين داخل مباني الجامعة؛ اتخاذ الإجراءات النظامية اللازمة بحقهم.

5.10.7 يجب أن تُحفظ تراخيص البرمجيات في مكان آمن، وأن تُبرَز لفحصها إذا لزم الأمر، وإلا قد يكون المستخدم معرضًا للعقوبة.

6.10.7 يجب أن تحصل إدارة الأمن السيبراني على المشورة القانونية بشأن المتطلبات والتشريعات التي تحكم حقوق الملكية الفكرية وتراخيص البرمجيات.

7.10.7 في الحالات التي لا يمكن نقل البرمجيات المثبّتة على أجهزة الحاسب القديمة أو الزائدة عن الحاجة والتي قد تؤدي إلى انتهاك قانون حقوق النشر، فإنه يجب مسح جميع البرمجيات الموجودة على وسائط التخزين ومن ثم اتباع الإجراءات اللازمة للتخلص من الاصول الصادرة عن الإدارة العامة للشؤون المالية والإدارية.

8.10.7 يحظر حيازة البرمجيات برخص غير نظامية أو تعديلها بما يغير مواصفاتها القانونية.

11.7 التدقيق والمراجعة

1.11.7 يجب التدقيق على تنفيذ الضوابط المطبقة لحماية سرية المعلومات والبيانات في الجامعة وسلامتها وتوافرها وخصوصية البيانات الشخصية من خلال إدارة جهة مختلفة عن إدارة الأمن السيبراني.

2.11.7 يجب توثيق نتائج المراجعة والملحوظات ورفع تقرير بالنتائج ومناقشته مع الأطراف ذات العلاقة.

3.11.7 يجب أن يشتمل تقرير التدقيق على نطاق التدقيق والملاحظات والتوصيات والأنشطة التصحيحية وخطة المعالجة المقترحة.

4.11.7 يجب عرض نتائج المراجعة والملحوظات المتعلقة بالتدقيق على اللجنة الإشرافية لأمن المعلومات.

5.11.7 يجب تنفيذ إجراءات استباقية وتصحيحية لنتائج التدقيق وملحوظاته.

6.11.7 يجب تحديد العناصر التي أدت لهذه النتائج والملحوظات وتحليلها وتحديد أسبابها.

7.11.7 يجب تحديد عدد من الإجراءات لتفادي أو تقليل احتمالية حدوث أو تكرار الملاحظات.

8.11.7 يجب تحديد خطة زمنية لحل البنود غير المتوافقة المبلغ عنها على أن يراقب تطبيق الحلول المقترحة بشكل مستمر لضمان كفاءة الحل.

9.11.7 يجب أن تكون صلاحيات الوصول للبيانات والأنظمة من قبل المدقق وفقا لمبدأ الحاجة الى المعرفة والاستخدام.

8. الأدوار والمسؤوليات

يجب على إدارة الأمن السيبر اني القيام بالآتي:

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 إن أمكن.

6.1.8 على موظفي إدارة الأمن السيبراني ضمان 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 موظفي إدارة الأمن السيبراني التنسيق مع الإدارات ذات العلاقة لمتابعة الالتزام والتنفيذ.

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

يجب على المدير التنفيذي لإدارة الشؤون القانونية:

9.1.8 في حالة حدوث انتهاك للالتزام بهذه السياسة بناء على تحقيق إدارة الأمن السيبراني، يجب على المدير التنفيذي للشؤون القانونية اتخاذ الإجراءات اللازمة.

يجب على مدير ضمان الجودة:

10.1.8 مراجعة ضوابط الأمن السيبراني وحوكمة البيانات وتدقيق تطبيقها وفقاً للمعايير العامة المقبولة للمراجعة والتدقيق، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

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

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

12.1.8 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 أو عدم 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.06-24.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.06-43.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

13. 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
تحديد التشريعات المعمول بها	7-1	-	-	-	-	A.18.2.1
حقوق الملكية الفكرية	-	-	-	-	-	A.18.2.2
حماية سجلّات الجامعة	-	-	-	-	-	A.18.2.3
حماية البيانات وخصوصية البيانات الشخصية	3-7-2	7-2	-	-	-	A.18.2.4
الالتزام بالسياسات والمعايير الأمنية	8-1	4-1	-	-	-	A.18.1.2
الالتزام التقني	8-1	4-1	-	-	-	A.18.1.3

----------نهاية الوثيقة----------