الدار للتعليم

دليل سياسة أمن المعلومات للدار للتعليم

التصنيف: للاستخدام الداخلي العام

معلومات الوثيقة	
الاسم	دليل سياسة أمن المعلومات للدار للتعليم
الرقم المرجعي	ALDED-EDT-GEN-PL-00004

مراقبة إصدار الوثيقة		
الإصدار	**التاريخ**	ملخص التغيير
الإصدار 1	2 سبتمبر 2025	الإصدار الأولي

التصنيف: للاستخدام الداخلي العام

جدول المحتويات

أ- مقدِّمة

1- العنوان:

1-1 تُعرَف هذه الوثيقة باسم "دليل سياسة أمن المعلومات للدار للتعليم" (يُشار إليها بـ"السياسة").

2- الغرض

2-1 تضع هذه السياسة الضوابط اللازمة الضوابط اللازمة لتحقيق حوكمة فعالة وإدارة أفضل لأمن المعلومات داخل الدار للتعليم. وهي تُركِّز على ضوابط أمن المعلومات المتعلقة بالأفراد والعمليات والتقنية.

3- الوثيقة الحاكمة

3-1 يجب قراءة دليل السياسة هذا بالاقتران مع الوثائق التالية:

1-1-3 سياسة دائرة التعليم والمعرفة الرقمية،

2-1-3 سياسة سجلات دائرة التعليم والمعرفة،

3-1-3 أهداف التحكم في المعلومات وتقنيات المعلومات ذات الصلة 2019، و

4-1-3 آيزو 27001:2022.

4- النطاق

1-4 تُلزِم هذه السياسة وتُطبق على جميع الموظفين في المقر الرئيسي للدار للتعليم، وأكاديمية الدار للتدريب (ATA)، ومدارسها المُشغَّلة (يشار إليها فيما بعد بلفظ أكاديمية الدار للتدريب")، والمقاولين، والموردين، الذين يتعاملون مع أصول معلومات الدار للتعليم، بما في ذلك على سبيل المثال لا الحصر المعلومات التي تُنشأ أو تُعالج أو تُخزن أو تُحتفظ بها من قبل الدار للتعليم كجزءٍ من وظائفها وخدماتها بغض النظر عن الموقع الجغرافي. بالنسبة للمدارس المُدارة، يُرجع إلى هذه السياسة في المجالات التي تقع ضمن مسؤولية الدار للتعليم وفقًا للاتفاقية القانونية ذات الصلة.

2-4 ليس في هذه السياسة ما يبطل أي إجراءات سابقة اتُّخذت بصورة صحيحة بموجب وثائق سابقة.

3-4 تُعالِج السياسة المجالات التالية:

1-3-4 أمن المعلومات - عام،

2-3-4 إدارة المخاطر،

3-3-4 أنظمة أو مرافق معالجة المعلومات،

4-3-4 التواصل مع السلطات / المجموعات الأخرى،

5-3-4 إدارة الأصول،

6-3-4 إدارة الهوية والوصول،

7-3-4 مزود خدمات الجهات الخارجية،

8-3-4 إدارة حوادث وتهديدات أمن المعلومات،

9-3-4 إدارة التعافي من الكوارث،

10-3-4 أمن الموارد البشرية،

11-3-4 العمل عن بُعد،

12-3-4 الأمن المادي والبيئي،

13-3-4 أمن الأجهزة الطرفية،

14-3-4 إدارة كلمات المرور،

15-3-4 إدارة مكافحة الفيروسات،

16-3-4 تسجيل النظام،

17-3-4 استخدامات البرمجيات، و

18-3-4 التشفير.

5- الامتثال

1-5 يجب ضمان الامتثال للوائح ومعايير حماية البيانات المحلية والدولية.

2-5 قد تؤدي مخالفة هذه السياسة والوثائق الداعمة لها إلى إجراءات تصحيحية من جانب السلطات الإدارية المعنية. ويجرى التحقيق التأديبي بما يتناسب مع خطورة الحادثة، حسبما يحدده التحقيق.

3-5 يجب الإبلاغ فورًا عن أي حالة عدم امتثال أو خرق لهذه السياسة إلى مكتب خدمة الدار للتعليم على sd@aldareducation.com لاتخاذ الإجراءات الفورية وحل المشكلة.

4-5 توجه جميع الاستفسارات المتعلقة بتفسير دليل السياسة هذا إلى مكتب خدمة الدار للتعليم على sd@aldareducation.com.

5-5 بمجرد اعتماد النسخة المعتمدة من هذا الدليل، يجب استخدام النسخ المطبوعة، والنسخ المطبوعة غير الخاضعة للرقابة لن تُعتبر سارية.

ب- بيانات السياسة

1- أمن المعلومات - عام

1-1 المسؤوليات

1-1-1 يتحمل المستخدمون مسؤولية ما يلي:

- الالتزام بسياسات وإجراءات أمن المعلومات.
- المشاركة في أنشطة التوعية والتدريب الأمني.
- معرفة الأصول أو أجزاء الأصول التي يتحملون مسؤوليتها بشكل مباشر (مثل الطابعة، والحاسوب المكتبي، وخدمات الدعم المحدَّدة، وما إلى ذلك).
- إبلاغ الدار للتعليم بالحوادث.

2- إدارة المخاطر

1-2 تتبنى الدار للتعليم نهجًا قائمًا على المخاطر لإدارة أمن المعلومات. يتطلب هذا النهج ما يلي:

1-1-2 تحديد جميع أصول المعلومات المهمة.

2-1-2 تحديد الثغرات الأمنية في هذه الأصول المعلوماتية.

3-1-2 رصد التهديدات واحتمالاتها التي قد تؤدي إلى استغلال الثغرات.

4-1-2 تحديد المجموعة المناسبة من الضوابط لحماية هذه الأصول من التهديدات المحددة. ويجب أيضًا تحديد الضوابط بما يتماشى مع أي إرشادات للعملاء أو بنود تعاقدية بشأن أمن المعلومات، إن وجدت.

5-1-2 التقييم الدوري لإدارة المخاطر وإغلاق المخاطر المحددة.

3- أنظمة أو مرافق معالجة المعلومات

1-3 عند الموافقة رسميًا على حيازة أو تطوير أو نشر أو تنفيذ نظام أو مرفق جديد لمعالجة المعلومات، تأخذ الدار للتعليم في الاعتبار ما يلي:

1-1-3 امتثال نظام أو مرفق معالجة المعلومات لسياسة أمن المعلومات والمعايير والمقاييس الخاصة بالدار للتعليم والتي صُمِّمت خصيصًا للنظام أو المرفق.

2-1-3 مدى التوافق الفني للنظام الجديد مع مكونات النظام الحالية.

2-3 يجب على المستخدمين التأكد من استخدام أنظمة أو مرافق معالجة مُعتمدة فقط للحصول على بيانات الدار للتعليم أو معالجتها.

3-3 يُمنع منعًا باتًا استخدام المعدات الشخصية، مثل أجهزة الكمبيوتر المحمولة أو الأجهزة المُستخدمة عن بعد / المحمولة، لمعالجة بيانات الدار للتعليم، ما لم تُصرّح الدار للتعليم بذلك.

4-3 تصفية الويب

1-4-3 يخضع الوصول إلى موارد الويب لضوابط مُدارة مركزيًا تمنع الوصول إلى المحتوى غير الملائم أو الضار أو الذي لا يتماشى مع الأهداف التشغيلية والتعليمية للشركة. تشمل هذه الضوابط ما يلي:

- هناك آليات لتصنيف وحظر المواقع الإلكترونية التي تندرج تحت فئات محظورة محددة مسبقًا مثل محتوى للبالغين، أو المقامرة، أو خطاب الكراهية، أو مصادر البرامج الضارة المعروفة.

- تُراقب الدار للتعليم فعالية أنظمة تصفية الويب بشكل منتظم، وتضع آليات لمراجعة وتحديث السياسات الآمنة لتطبيق مرشحات الويب عبر شبكات وأجهزة المقر الرئيسي والمدارس المُدارة.
- المراجعة والتعديل الدوري لمرشحات الويب والاستثناءات لتعكس بيئات المخاطر المتغيرة والاحتياجات التشغيلية.
- تسجيل ومراقبة تصفية الويب للكشف عن الانتهاكات أو التهديدات المحتملة.

5-3 نشرت الدار للتعليم وحافظت على حلول جدار حماية قائمة على الهوية تمكّن من الرؤية والتحكم على مستوى المستخدم في استخدام الويب.

4- التواصل مع السلطات / المجموعات الأخرى

1-4 تدرك الدار للتعليم أن الحفاظ على المستوى المطلوب من أمن المعلومات قد يتطلب التعاون والدعم والمساعدة من بعض الوكالات الخارجية (السلطات والمنظمات الأخرى).

2-4 يجب إضفاء الطابع الرسمي على مدى التعاون ونقل المعلومات المتعلقة بالأمن بين الدار للتعليم والأطراف أو الوكالات الخارجية، وأن يكون ذلك وفقًا للسلطة القانونية للوكالات.

3-4 يجب أن يكون هذا التعاون في مصلحة الدار للتعليم ويجب ألا يؤدي إلى انتهاك لهذه السياسة، بما في ذلك النقل غير المصرح به للمعلومات السرية / المصنفة إلى منظمات خارجية غير مصرح لها.

4-4 يجب معالجة اتفاقيات الأطراف الخارجية ومتطلبات الوصول وفقًا لضوابط إدارة خدمات الأطراف الثالثة المحددة في هذه السياسة.

5-4 لن تقوم الدار للتعليم بإسناد أي أنشطة تتعلق بوظائف معالجة المعلومات أو البيانات أو خدمات النظام إلى طرف ثالث إلا بعد الحصول على الموافقة اللازمة. في هذه الحالات، يتم توقيع اتفاقيات مستوى خدمة رسمية بين الأطراف لضمان الالتزام بهذه السياسة، كما يخضع أداء الطرف الثالث لمراجعة دورية.

5- إدارة الأصول

1-5 يجب أن يكون تحديد وتصنيف وصيانة والتخلص من أصول معلومات الدار للتعليم آمنًا، مما يضمن حصر الأصول المتعلقة بنظام المعلومات وتعيين مالك لها.

2-5 تصنيف الأصول

1-2-5 يعد تصنيف ومعالجة والتعامل مع أصول نظام معلومات الدار للتعليم أمرًا أساسيًا لحماية المعلومات الحيوية والحساسة. ويجب أن تأخذ إدارة الأصول في الاعتبار احتياجات السرية والسلامة والتوافر (CIA) لجميع أصول نظام المعلومات لضمان التنفيذ والإدارة المناسبين للعمليات والضوابط الأمنية.

2-2-5 إرشادات تصنيف الأصول

- يجب على مالك المعلومات تصنيف أصول معلوماته بناءً على ثلاثة معايير مختلفة:

المعايير	الوصف
السرّية	مستوى السرية الذي سيُمنح لأصول نظام المعلومات، وبالتالي مستوى إمكانية الوصول إلى المعلومات التي يحتوي عليها أو يمثلها درجة السرية الممنوحة لأصول نظام المعلومات تحدد مدى إمكانية الوصول إلى بياناته.
النزاهة	تأثير التعديل غير المصرح به على أصل نظام معلومات أو فقدان أصل نظام المعلومات أو البيانات الواردة فيه. يُشير النص إلى التعديل غير المصرح به على أصل نظام المعلومات، أو فقدان هذا الأصل أو البيانات المرتبطة به.
حالة التوافر	تأثير عدم توفر أصل أنظمة المعلومات. تنقسم معايير التوافر أيضًا إلى عدم التوافر طويل الأجل وعدم التوافر قصير الأجل. تأثير غياب أنظمة المعلومات ينقسم إلى عدم توفر طويل أو قصير الأمد.

- تأخذ إرشادات تصنيف الأصول في الاعتبار ما يلي:
  - نوع الأصل (بيانات أو أنظمة معلومات)،
  - مدى أهمية الأصل،
  - قيمة أصل أنظمة المعلومات وحساسيته،
  - تأثير الانتهاك الأمني،
  - تحديد قواعد منح الوصول إلى أنظمة المعلومات، ونوعية الصلاحيات (قراءة، تعديل، حذف) لكل مستخدم.
- تصنف الأصول حسب معايير السرية والسلامة والتوافر عند الحاجة. (CIA)
- تحدد فئات التصنيف مستوى الحماية المطبق على أصل المعلومات.
- يجب أن يعكس التصنيف وضوابط الوصول إلى المعلومات متطلبات العمل في المشاركة أو التقييد، وتأثيرها على الأعمال.

3-5 تماشيًا مع سياسة المكتب النظيف والشاشة النظيفة لمجموعة الدار التقنية، يجب على المستخدمين التأكد مما يلي:

1-3-5 عدم ترك المستندات على المكتب بعد ساعات العمل.

2-3-5 إغلاق الأدراج الفردية التي تحتوي على مستندات قبل مغادرة المكتب في نهاية اليوم.

4-5 النسخ الاحتياطي والتخزين

1-4-5 يوضع إجراء رسمي للنسخ الاحتياطي للبيانات لضمان نسخ احتياطي آمن وتخزين للمعلومات للبيئة المحلية. ويجب حفظ النسخ الاحتياطية للبيانات الحيوية وتخزينها في بيئة آمنة أو غير متصلة بالإنترنت.

2-4-5 تُنسخ جميع أصول المعلومات والبيانات وقواعد البيانات والتكوينات والتطبيقات والخدمات والبرامج الأساسية للعمليات المستمرة للدار للتعليم احتياطيًا وتُختبر دوريًا وفقًا لجدول النسخ الاحتياطي للاسترداد والموثوقية.

3-4-5 يجب الاحتفاظ بنسخ احتياطية لجميع بيانات المقر الرئيسي للدار للتعليم بحيث تكون جميع أصول المعلومات وأنظمة المعلومات قابلة للاسترداد بالكامل. وكحد أدنى، سيُحتفظ بنسخ احتياطية لبيانات المقر الرئيسي للدار للتعليم لمدة 30 يومًا.

4-4-5 يتم حفظ النسخ الاحتياطية في مكان آمن ومنفصل عن شبكة المدرسة الرئيسية لضمان حماية البيانات من الفقدان أو الاختراق.

5-4-5 تأكد أن النظام والتطبيقات والبيانات المستعادة من النسخة الاحتياطية تعمل بشكل سليم.

6- إدارة الهوية والوصول

1-6 يتم تنظيم الوصول إلى المعلومات ومرافق معالجة البيانات وفقًا لاحتياجات العمل ومتطلبات الأمان الخاصة بكل تطبيق بشكل مستقل.

2-6 يخضع استخدام النظام أو إساءة استخدامه غير المُصرَّح به للملاحقة الجنائية.

3-6 تُستخدم تطبيقات التعلم الخارجية المعتمدة فقط في بيئة المدرسة. يجب تنفيذ ضمانات، مثل آليات تسجيل الدخول الموحد، لضمان الوصول الآمن وحماية البيانات الحيوية.

4-6 سيتم مراقبة استخدام النظام وتسجيله.

5-6 إدارة وصول المستخدم

1-5-6 لا يكون تفعيل حسابات المستخدمين للمقاولين أو الاستشاريين أو العمال المؤقتين أو موظفي الموردين ساريًا إلا خلال الفترة التي يؤدي فيها هؤلاء الأفراد مهامًا أو خدمات للدار للتعليم بفاعلية.

2-5-6 يُسمح بالوصول إلى أصول معلومات العمل للأطراف الثالثة فقط في حال وجود اتفاقية تعاقدية واتفاقية عدم إفصاح داعمة.

3-5-6 يُحظر استخدام المعرفات العامة على أي نظام.

6-6 إدارة الامتيازات

1-6-6 يُحظر على المستخدمين تثبيت أي شيفرة أو برنامج أو تقنية تتحايل على آليات التحكم في الوصول المصرح بها الموجودة في أنظمة التشغيل أو أنظمة التطبيقات أو آليات التحكم في الوصول إلى نظام البنية التحتية.

7-6 يجب على المستخدمين التعاون في تعزيز أمن أنظمة معلومات الدار للتعليم، والحفاظ على سرية حساباتهم وكلمات المرور.

8-6 التحكم في الشبكة

1-8-6 يتم التحكم في الوصول إلى شبكة الدار للتعليم وحمايتها لضمان سرية وسلامة وتوافر أصول أنظمة المعلومات الخاصة بالدار للتعليم.

2-8-6 يتم منح الوصول إلى الشبكات وخدمات الشبكة بناءً على تصاريح محددة ومراقبة وفقًا لمتطلبات العمل والأمان، بالإضافة إلى قواعد التحكم في الوصول المحددة لكل شبكة.

7 يتعين على جميع المستخدمين الوصول إلى أنظمة معلومات وموارد المؤسسة حصريًا عبر المسار المحدد مسبقًا لشبكة الاتصال الخاصة الافتراضية (VPN). ولا يُسمح لأجهزة الكمبيوتر الشخصية بالوصول إلى أنظمة معلومات الدار للتعليم عبر شبكة خاصة افتراضية. (مثل، بريد الويب).

يتعين على جميع المستخدمين الوصول إلى أنظمة معلومات وموارد المؤسسة حصريًا عبر المسار المحدد مسبقًا لشبكة الاتصال الخاصة الافتراضية (VPN).

1-8-7 تتلقى الدار للتعليم على أوصافًا تفصيلية للسمات الأمنية لجميع الخدمات الخارجية المستخدمة (إن وجدت) من مزودي خدمات الشبكات الخارجية لتحديد سرية وسلامة وتوافر تطبيقات الأعمال ومستوى الضوابط (إن وجدت) التي تطلبها الدار للتعليم. ويجب تضمين وصف الضوابط الأمنية في اتفاقية الخدمة.

9-6 برامج الوصول عن بعد

1-9-6 ستحتوي البرامج على ضوابط مدمجة لضمان حماية وخصوصية محطات عمل المستخدمين.

10-6 DevSecOps (عمليات التطوير والأمان)

6-10-1 يجب أن يُطلب من المطورين اتباع ممارسات الترميز الآمن عند تطوير البرامج. كما يجب أن تشمل هذه الممارسات استخدام معايير ترميز آمنة، وتجنب الثغرات الأمنية المعروفة، واختبار الشيفرة بحثًا عن الثغرات الأمنية.

6-10-2 يجب استخدام اختبار الأمن المؤتمت لفحص الشيفرة بحثًا عن الثغرات واختبار الامتثال للوائح الأمنية.

6-10-3 يجب استخدام التكامل المستمر والتسليم المستمر لأتمتة عملية تطوير البرامج ونشرها، بما في ذلك الفحوصات الأمنية في بيئة DevSecOps.

7- إدارة خدمات الجهات الخارجية

7-1 أمن المعلومات لعلاقات الموردين

7-1-1 حددت الدار للتعليم ونفذت إجراءات لمعالجة المخاطر الأمنية المرتبطة باستخدام المنتجات والخدمات التي يقدمها الموردون.

7-1-2 حددت الدار للتعليم ووثقت أنواع الموردين الذين يمكن أن يؤثروا على سرية وسلامة وتوافر معلومات الدار للتعليم.

7-1-3 بالنسبة لترتيبات الاستعانة بمصادر خارجية، تضمن الدار للتعليم الحفاظ على الأمن طوال عملية الخدمة.

7-1-4 تُقيّم الدار للتعليم وتدير مخاطر أمن المعلومات المرتبطة بما يلي:

- استخدام معلومات الدار للتعليم والأصول الأخرى المرتبطة بها.
- الثغرات الأمنية للمنتجات أو الخدمات التي يقدمها الموردون.

7-1-5 تراقب الدار للتعليم الامتثال لمتطلبات أمن المعلومات المعمول بها لكل نوع من الموردين.

7-2 معالجة الأمن ضمن اتفاقيات الموردين

7-2-1 يجب أن يجب أن تتوافق جميع الاتفاقيات مع الأطراف الثالثة بشأن الوصول إلى أنظمة معلومات الدار للتعليم مع سياسة أمن المعلومات والإجراءات والمعايير والمبادئ التوجيهية ومدونات الممارسة الخاصة بالدار للتعليم. بالإضافة إلى ذلك، سيكون الامتثال لسياسة أمن المعلومات والإجراءات والمبادئ التوجيهية الخاصة بالدار للتعليم هو الأساس لمنح وإلغاء وصول الأطراف الثالثة إلى البنية التحتية لأنظمة معلومات الدار للتعليم.

7-2-2 يتم ضمان جميع متطلبات الأمن والتدقيق ذات الصلة في الاتفاقيات مع الأطراف الثالثة.

7-2-3 يُنظر في تضمين الشروط التالية في الاتفاقيات لتلبية متطلبات أمن المعلومات المحددة:

- المتطلبات القانونية والنظامية والتنظيمية والتعاقدية، بما في ذلك حماية البيانات، والتعامل مع المعلومات الشخصية المحددة للهوية، وحقوق الملكية الفكرية، وحقوق الطبع والنشر.
- التزام كل طرف تعاقدي بتنفيذ مجموعة متفق عليها من الضوابط.
- قواعد الاستخدام المقبول للمعلومات والأصول الأخرى المرتبطة بها.
- التعويضات والإصلاحات عند إخفاق المقاول في تلبية المتطلبات.
- متطلبات وإجراءات إدارة الحوادث.
- الأحكام ذات الصلة بالتعاقد من الباطن.
- الحق في تدقيق عمليات المورد وضوابطه المتعلقة بالاتفاقية.
- التزام المورد بتقديم تقرير دوري عن فعالية الضوابط والاتفاقية.

- تصحيح القضايا المذكورة في التقرير فوراً.
- توافر الخدمات

4-2-7 يجب معالجة المسؤوليات والإجراءات القانونية المتعلقة بخرق أمن المعلومات في شروط وأحكام جميع الاتفاقيات مع الأطراف الثالثة.

5-2-7 تلتزم الدار بحقوق النشر وتراخيص البرامج عند مشاركة المعلومات خارجياً.

6-2-7 يُشترط توقيع الاتفاقيات الرسمية مثل اتفاقية عدم الإفصاح قبل مشاركة أي معلومات حساسة مع جهات خارجية.

7-2-7 يجب تنفيذ وإدارة الضوابط الأمنية وتعريفات الخدمة ومستويات التسليم المدرجة في اتفاقيات تقديم خدمات الطرف الثالث من قبل الدار للتعليم والأطراف الثالثة.

8-2-7 يجب أن توضح الاتفاقيات مع الأطراف الخارجية نوع ومستوى الخدمة المطلوبة لضمان استمرارية الأعمال عند الحاجة إلى توافر عالٍ.

9-2-7 الشروط والأحكام

- يجب أن تنص الاتفاقيات مع المقاولين والأطراف الثالثة الأخرى بوضوح على مسؤولياتهم تجاه أمن المعلومات.
- يجب اعتماد وتوثيق ومراجعة الاتفاقيات الخاصة بالسرية وعدم الإفصاح بصورة دورية بما يتناسب مع احتياجات المؤسسة التعليمية لضمان حماية المعلومات، ويُشترط توقيع جميع الموظفين وكافة الأطراف ذات الصلة على هذه الاتفاقيات.

3-7 سلسلة توريد تقنية المعلومات والاتصالات

1-3-7 لإدارة مخاطر سلسلة التوريد والتخفيف منها، تضمن الدار للتعليم ما يلي:

- تلبية المنتجات والخدمات الرقمية والتقنية المكتسبة لعمليات الأعمال لمتطلبات الأمن المحددة في جميع مراحل سلسلة التوريد، بما في ذلك مؤسسة الشراء والموردون وأي مقاولين من الباطن معنيين.
- يجري التحقق لضمان استمرار المنتجات والخدمات الرقمية والتقنية في تلبية متطلبات الأمن المحددة دون أي ميزات غير متوقعة أو غير مرغوب فيها.
- يتعين أن تكون العناصر الأساسية قابلة للتتبع إلى مصدرها الأصلي ضمن سلسلة التوريد. كما ينبغي وضع إجراءات واضحة لتبادل المعلومات بين الدار للتعليم وموردِيها فيما يتعلق بمخاطر أو اختراقات أو مشكلات قد تؤثر على سلامة سلسلة توريد الخدمات الرقمية والتقنية.

4-7 إمكانية وصول الأطراف الثالثة

1-4-7 يجب أن يكون وصول الطرف الثالث إلى البنية التحتية لأنظمة معلومات الدار للتعليم مصرحًا به رسميًا ويخضع لاتفاقية رسمية بين الدار للتعليم والطرف الثالث المعني. ومع ذلك، ستُقيِّم الدار للتعليم المخاطر المرتبطة بمشاركة الأنظمة والمعلومات والأصول عبر تقييم رسمي للمخاطر مع مراعاة المعايير التالية:

- نوع ومستوى الوصول الذي سيُمنح للطرف الثالث.
- تصنيف المخاطر (القيمة والحساسية) لأصل (أصول) المعلومات الذي يُمنح الوصول إليه.
- الغرض من الوصول.
- معلومات أساسية تتعلق بالطرف الثالث.
- علاقة الطرف الثالث بالدار للتعليم.

- فعالية الضوابط التي يجب تنفيذها لتنظيم ومراقبة وصول الطرف الثالث.

7-4-2 قبل منح الوصول إلى أي معلومات، ستقدم الدار للتعليم إيجازًا لجميع مستخدمي الطرف الثالث حول أدوار ومسؤوليات أمن المعلومات من خلال توقيع اتفاقية الحوسبة المسؤولة.

7-4-3 لن يُسمح بالاتصالات المخصصة وغير المراقبة على مدار الساعة طوال أيام الأسبوع من قبل أطراف ثالثة بأنظمة الإنتاج.

7-4-4 تضمن الدار للتعليم أن البيانات الحساسة المرسلة إلى الأطراف الثالثة عبر قنوات الاتصال مثل الإنترنت، وروابط الشبكة الواسعة، وروابط الإكسترانت محمية بشكل كافٍ من الاعتراض والتلاعب.

7-4-5 وحيثما يلزم تبادل كميات كبيرة من البيانات، في شكل نسخ احتياطية كاملة للنظام أو تفريغ قواعد البيانات، مع أطراف ثالثة؛ ستكون هناك حاجة إلى موافقات إضافية. يجب على الأطراف الثالثة وضع ضوابط أمنية كافية لحماية هذه البيانات.

7-5 مراقبة ومراجعة وإدارة تغيير خدمات الموردين

7-5-1 يمكن أخذ المعايير التالية في الاعتبار لمراقبة ومراجعة الخدمات والتقارير والسجلات المقدمة من أطراف خارجية:

- الأداء مقابل مستويات الخدمة وإعداد التقارير بعد الأحداث الكبرى.
- عدم الامتثال والقضايا، على سبيل المثال، لاتفاقية مستوى الخدمة أو الخروقات الأمنية.
- مؤشرات فرص تحسين الخدمة.

7-5-2 عند الحاجة، ستجري الدار للتعليم عمليات تدقيق/مراجعة لخدمات الطرف الثالث.

7-5-3 ستراقب الدار للتعليم التغييرات في خدمات الموردين بما في ذلك:

- التغييرات والتحسينات على الشبكات.
- استخدام تقنيات جديدة.
- اعتماد منتجات جديدة أو إصدارات أو تحديثات.
- أدوات وبيئات تطوير جديدة.
- تغييرات في الموقع المادي لمرافق الخدمة.
- التعاقد من الباطن مع مورد آخر.

7-5-4 سيتم تعديل الاتفاقيات الحالية بما يلزم الموردين بالامتثال لسياسة أمن المعلومات والضوابط.

8- إدارة حوادث وتهديدات أمن المعلومات

8-1 ستُوثق خطة الاستجابة للحوادث وتُحدَّث بانتظام لتوجيه الاستجابة لحوادث الأمن الإلكتروني.

8-2 يجب على المدارس اتباع إجراءات إدارة الحوادث المحددة من قبل الدار للتعليم وتشمل الإبلاغ الداخلي للمدرسة أثناء وقوع حادث، وفريق أمن المعلومات وإدارة المخاطر في مجموعة الدار، وإخطار دائرة التعليم والمعرفة.

8-2-1 يجب أن يقتصر التواصل بشأن حوادث الأمن الإلكتروني على أصحاب المصلحة الداخليين المعنيين، ودائرة التعليم والمعرفة، ومقدمي الخدمات المشاركين مباشرة. يُحظر على المدارس إبلاغ أي أطراف خارجية أخرى بمثل هذه الحوادث.

8-2-2 يجب أن تمتثل جميع الإجراءات المتخذة استجابة لحادث أمن إلكتروني للقوانين والسياسات المعمول بها في دولة الإمارات العربية المتحدة، بما في ذلك تلك التي وضعتها هيئة أبوظبي الرقمية والمرسوم بقانون اتحادي رقم (34) لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية.

8-3 يجب على أولياء الأمور مراقبة استخدام الطلاب للأجهزة الرقمية خارج مباني المدرسة وساعات الدوام المدرسي لضمان سلوك رقمي

آمن ومناسب.

4-8 إدارة التهديدات

1-4-8 طبقت الدار للتعليم آليات كشف تهديدات عبر شبكة المقر الرئيسي والمدارس لرصد عن الأجهزة المخترقة أو المصابة والاستجابة للحوادث وفق سياسات إدارة الحوادث.

2-4-8 يشمل إجراء إدارة التهديدات ما يلي:

- استخدام المصادر الداخلية، مثل التحكم في الوصول، وسجلات التطبيقات والبنية التحتية، وأنظمة كشف التسلل، وأنظمة منع التسلل، وأدوات الأمان، ومراقبة معلومات وأحداث الأمان.
- استخدام مصادر خارجية موثوقة وذات صلة، مثل منتديات الأمان، والموردين، ومنظمات الأمان، وخدمات الإشعارات المتخصصة.
- تحديد منهجية لتحليل معلومات التهديدات بشكل دوري.
- التفاصيل ذات الصلة بالتهديدات المُحدَّدة أو المُجمَّعة، مثل طريقة العمل والجهات الفاعلة والدافع ونوع التهديدات.
- مدى صلة المعلومات الاستخباراتية المستخلصة وقابليتها للتنفيذ للمتابعة (على سبيل المثال، مركز عمليات الأمان، وإدارة المخاطر).

3-4-8 تُجمع معلومات حول التهديدات الحالية أو الناشئة وتُحلل من أجل:

- دعم اتخاذ قرارات فعّالة لحماية دار التعليم من التهديدات
- تُقلِّل من تأثير هذه التهديدات.

4-4-8 يُضمن أن تكون المعلومات الاستخباراتية عن التهديدات:

- ذات صلة (أي مرتبطة بحماية الدار للتعليم).
- ثاقبة (أي تزويد الشركة بفهم دقيق ومفصل لمشهد التهديدات).
- قابلة للتنفيذ (أي يمكن للدار للتعليم التصرف بناءً على المعلومات بسرعة وفعالية).

5-4-8 معلومات استباقية عن التهديدات:

- يجب على المستخدمين الاشتراك لدى مزودي المعلومات الاستخباراتية عن التهديدات للبقاء على اطلاع على الحوادث والتهديدات المتعلقة بأمن المعلومات.
- يجب الاحتفاظ بالمعلومات الاستباقية حول التهديدات وترتيبها في قاعدة بيانات مرنة مناسبة لصياغة ملاحظات العمل والبيانات الوصفية للمؤشرات مثل قاعدة المعرفة.
- يجب تحديث أنظمة منع وكشف التسلل بمعلومات استباقية عن التهديدات ويجب التأكد من قدرة هذه الأنظمة على كشف التهديدات والتعامل معها بفعالية.

9- إدارة التعافي من الكوارث

1-9 طورت الدار للتعليم خطة للتعافي من الكوارث لإدارة التعافي من الكوارث.

10- أمن الموارد البشرية

10-1 ستُقدم تدريبات توعية بأمن المعلومات لجميع مستخدمي الطرف الثالث لضمان أن يكون المستخدمون:

10-1-1 على درايةٍ كافية بأدوارهم ومسؤولياتهم الأمنية.

10-1-2 مزودين بإرشادات تحدد هذه التوقعات الأمنية.

10-1-3 لديهم الحافز للوفاء بسياسات أمن المؤسسة.

10-1-4 مدعومين ومثقفين لممارسة مستوى من الوعي الأمني.

10-1-5 لديهم التزام بشروط وأحكام التوظيف والسياسات الأمنية.

10-2 التوعية بأمن المعلومات والتثقيف والتدريب

10-2-1 يتم توعية كل موظف وطالب عن أمن المعلومات والوعي الأمني من خلال مواد توعية منتظمة، ومنشورات بريد إلكتروني، ومنشورات على الإنترانت (الشبكة الداخلية)، وما إلى ذلك.

10-2-2 سيغطي التدريب ما يلي:

- تأكيد التزام الإدارة بأمن المعلومات في جميع أنحاء الشركة.
- أفضل الممارسات لتأمين أو حماية المعلومات التابعة للدار للتعليم والأطراف الخارجية.
- سياسة أمن المعلومات وإجراءاتها.
- سجلات التدريب / كشوف الحضور موقعة من المتدربين.
- يجب أخذ ملاحظات التدريب، وتحسين فعالية التدريب باستمرار بناءً على الملاحظات.

10-3 الإدارة التأديبية

10-3-1 ستُتخذ إجراءات تأديبية ضد أي خرق لسياسة وممارسات أمن المعلومات الخاصة بالدار للتعليم.

10-3-2 ستكون شدة الإجراء التأديبي المتخذ متناسبة طرديًا مع خطورة المخالفة المرتكبة.

10-3-3 ستُتخذ الإجراءات بشكل عادل ومبرر على نحو مناسب. يهدف الإجراء التأديبي إلى أن يكون رادعًا لمستخدمي أنظمة معلومات الدار للتعليم.

10-3-4 سيتم التعامل مع خرق سياسة أمن المعلومات من قبل الغير، مثل مورد، عبر آليات يُتفَق عليها مع كلا الطرفين وتُذكر على وجه التحديد في العقد.

11- العمل عن بُعد

11-1 أنشأت الدار قناة اتصال آمنة للاتصال عن بُعد.

11-2 يجب على جميع أجهزة الكمبيوتر المتصلة بشبكات الدار للتعليم الداخلية عبر الشبكة الخاصة الافتراضية أو أي تقنية أخرى استخدام أحدث برامج مكافحة الفيروسات ذات المعايير المؤسسية، بما في ذلك أجهزة الكمبيوتر الشخصية.

11-3 لا يجوز الاستخدام سوى لعملاء الشبكة الخاصة الافتراضية المعتمدين من الدار للتعليم.

11-4 يجب على مديري المدارس المعنيين الحصول على موافقة أولياء الأمور لجميع التفاعلات الافتراضية المباشرة مع الزوار المدعوين، داخل الفصل أو خارجه. يجب أن تُعتمد جميع هذه التفاعلات رسميًا من قبل دائرة التعليم والمعرفة، بما يتماشى مع سياسات الأنشطة

اللاصفية وحماية الطلاب الخاصة بالدائرة.

12- الأمن المادي والبيئي

12-1 تعد الضوابط المادية والبيئية جزءًا لا يتجزأ من الوضع الأمني العام الذي تتبناه الدار للتعليم. يجب على كل مستخدم التأكد من تطبيق الضمانات الأمنية المادية التي تنفذها الدار للتعليم باستمرار وحماية الأصول من التلف أو سوء الاستخدام.

12-2 المناطق الآمنة

12-2-1 توضع أصول نظام المعلومات الحيوية لأعمال الدار للتعليم في مناطق آمنة مخصصة ويجرى حمايتها بحواجز أمنية مناسبة وضوابط دخول مادية.

12-2-2 تُحمى الأصول من الوصول المادي غير المصرح به والتلف. وتكون التدابير الوقائية متناسبة مع المخاطر والأهمية المحددة لهذه الأصول.

12-3 تنظيم دخول الأشخاص إلى منشآت التقنية والخدمات الرقمية

12-3-1 لا يجوز للمستخدمين الذين يصلون إلى مناطق محددة بوصول مقيد أو محدود القيام بذلك إلا إذا مُنحوا بطاقات وصول خاصة للمناطق المقيدة.

12-3-2 لا يُسمح إلا للموظفين المصرح لهم من الموردين أو المقاولين بالوصول إلى مرافق أنظمة معلومات الدار للتعليم (مناطق الوصول المحدود) ويجب عليهم التوقيع إما في سجل استقبال المبنى الرئيسي أو في سجلات مركز بيانات الدار للتعليم، كجزء من الرقابة الأمنية.

12-4 تأمين مكاتب وغرف ومرافق الخدمات الرقمية والتقنية

12-4-1 تحتوي جميع مراكز البيانات وغرف المعدات وخزائن الاتصالات على خطة إخلاء موثقة مدمجة في خطة التعافي من الكوارث.

13- أمن الأجهزة الطرفية

13-1 أمن الحوسبة المتنقلة

13-1-1 يُحظر نقل وتخزين بيانات الدار على أجهزة الحوسبة الشخصية مثل أجهزة الكمبيوتر المكتبية المنزلية أو أجهزة الكمبيوتر المحمولة.

13-1-2 يجب على المستخدمين التأكد من اتخاذ احتياطات إضافية أثناء التعامل مع المعلومات على أجهزة الكمبيوتر المحمولة وأجهزة آيباد في الأماكن العامة وضمان ما يلي:

- يُحظر ترك الأجهزة قيد التشغيل وغير مقفلة ودون مراقبة.
- يجب على المستخدمين الحذر من المتلصصين على الشاشات.
- يُحظر ترك الأجهزة دون مراقبة أثناء السفر أو نقلها في الأمتعة المسجلة.

13-1-3 يجب على المستخدمين التأكد من أن جميع أجهزة الكمبيوتر المحمولة وأجهزة الآيباد وأجهزة الكمبيوتر المحمولة الأخرى مؤمنة ماديًا.

13-1-4 يجب الإبلاغ فورًا عن أي أجهزة مفقودة أو مسروقة إلى الدار للتعليم عبر الرابط sd@aldareducation.com.

13-1-5 توجد منصات اتصال وتعاون آمنة لحماية المعلومات التعليمية الحساسة التي تُشارَك بين الطلاب والموظفين.

13-2 "أحضر جهازك الخاص" واستخدام الأجهزة الشخصية

13-2-1 يجب أن تمتثل الأجهزة الشخصية المستخدمة للوصول إلى أنظمة الدار للتعليم للحد الأدنى من متطلبات الأمان، بما في ذلك برامج مكافحة الفيروسات المحدثة، والتكوينات الآمنة، ومواصفات الأجهزة المعتمدة.

14- إدارة كلمات المرور

14-1 تعد كلمات المرور جانبًا لا يتجزأ من أمن الكمبيوتر. فهي خط الدفاع الأول لحماية حسابات المستخدمين. وقد يؤدي اختيار كلمة مرور ضعيفة إلى اختراق شبكة الشركة وأنظمتها وتطبيقاتها بالكامل. وعلى هذا النحو، يتحمل جميع مستخدمي أنظمة معلومات الدار للتعليم مسؤولية اتخاذ الخطوات المناسبة، كما هو موضح أدناه، لاختيار وتأمين كلمات المرور الخاصة بهم.

14-2 المعيار الأدنى لحماية كلمة المرور

14-3-1 يجب على المستخدمين دائمًا الحفاظ على سرية كلمات مرور الوصول إلى نظام الدار للتعليم.

14-3-2 يُحظر مشاركة كلمات المرور تحت أي ظرف من الظروف. ويجب أن يمتلك كل مستخدم حسابًا فرديًا لضمان المساءلة وعدم إنكار المعاملات.

14-3-3 يجب على المستخدمين التأكد من أن كلمات المرور غير قابلة للتخمين، أي عدم استخدام كلمات قاموس بسيطة فقط، أو أسماء، أو تسلسلات بسيطة من الأرقام أو الحروف على لوحة المفاتيح. يجب ألا تستند كلمات المرور إلى معلومات شخصية أو أسماء أفراد العائلة أو الأصدقاء أو الأقارب أو الزملاء، وما إلى ذلك.

14-3-4 يجب على المستخدمين التأكد من عدم استخدام كلمات مرور لأنظمة الدار للتعليم تكون مطابقة لكلمات المرور المستخدمة في حسابات الإنترنت الشخصية مثل Hotmail وYahoo mail وGmail ومواقع الشبكات الاجتماعية.

14-3-5 يجب على جميع المستخدمين التأكد من عدم طباعة كلمات المرور أو تدوينها أو تخزينها في مناطق مرئية أو يسهل الوصول إليها.

14-3 إعادة تعيين كلمة المرور

14-3-1 ستدير المدرسة إعادة تعيين كلمة المرور للطلاب بطريقة آمنة، مع إبلاغ التفاصيل مباشرة إلى أولياء الأمور حسب الاقتضاء.

15- إدارة مكافحة الفيروسات

15-1 تضمن الدار للتعليم تثبيت وتفعيل برامج حماية نقاط النهاية الموحدة على كل جهاز بما في ذلك الأجهزة التي تديرها المدرسة. ويتم تفعيل جدران الحماية من الجيل التالي وأنظمة كشف ومنع التطفل على مستوى الشبكة. كما يجب أن يوفر هذا النظام الحماية ضد الفيروسات، وبرامج التجسس، والشيفرات المتنقلة، ومحاولات التسلل.

15-2 يجب فحص جميع الملفات أو البيانات الواردة من مصادر خارجية، بغض النظر عن وسائط التخزين، بحثًا عن الفيروسات قبل استخدامها.

16- تسجيل النظام

16-1 الاحتفاظ بالسجلات وحمايتها

16-1-1 تُنشأ جميع سجلات التدقيق التي تسجل الاستثناءات والأحداث الأخرى ذات الصلة بالأمن للأنظمة الحيوية، ويُحتفظ بها لمدة متفق عليها للمساعدة في التحقيقات والمراقبة المستقبلية.

16-1-2 يجب الاحتفاظ بجميع السجلات والمدونات على النظام. في حالة وجود قيود على السعة، يجب أرشفة السجلات وتخزينها عبر طرق قابلة للاسترجاع. يُحظر حذف السجلات دون التحقق من متطلبات الاحتفاظ بها من قطاع الأعمال، والتدقيق الداخلي، وإدارة الأمن الرقمي والمخاطر.

17- استخدامات البرمجيات

17-1 يُحظر على المستخدمين نسخ أي برمجيات مرخصة أو وثائق ذات صلة لاستخدامها سواء على شبكة الدار للتعليم أو في أي مكان آخر، ما لم يُصرح بذلك صراحةً بموجب اتفاقية مع المرخِّص. قد يُعرِّض النسخ غير المصرح به للبرمجيات المستخدمين و/أو الدار للتعليم لعقوبات مدنية وجنائية.

17-2 يُحظر على المستخدمين إعطاء البرمجيات للغير، بما في ذلك العملاء، والمقاولون، والأصدقاء، والأقارب، أو للاستخدام الشخصي للموظفين، وما إلى ذلك. ويجب على مستخدمي الدار للتعليم استخدام البرمجيات على الشبكات المحلية أو على أجهزة متعددة فقط وفقًا لاتفاقيات الترخيص السارية.

17-3 يجب استخدام البرمجيات التي اعتمدتها إدارة الخدمات الرقمية والتقنية فقط.

17-4 تُعد أجهزة كمبيوتر الدار للتعليم من أصول الشركة ويجب الحفاظ عليها قانونية من حيث البرمجيات وخالية من الفيروسات.

17-5 يُحظر على المستخدمين إحضار برمجيات من المنزل وتحميلها على أجهزة كمبيوتر الدار للتعليم. كما يُحظر أخذ البرمجيات المملوكة للشركة إلى المنزل وتحميلها على جهاز كمبيوتر منزلي خاص بالمستخدم.

17-6 تحتفظ إدارة الخدمات الرقمية والتقنية بالحق في إجراء عمليات تدقيق دورية على أجهزة كمبيوتر الدار للتعليم، بما في ذلك أجهزة الكمبيوتر المحمولة، لضمان الامتثال لتراخيص البرمجيات.

18- التشفير

18-1 يُتخذ القرار بشأن متطلبات تشفير المعلومات مع مراعاة المعايير التالية:

18-1-1 مخاطر نقل المعلومات داخليًا وخارجيًا.

18-1-2 مخاطر تخزين المعلومات والتحكم في الوصول إليها.

18-1-3 حماية المعلومات الموجودة على الأجهزة الطرفية المحمولة للمستخدم أو وسائط التخزين والمنقولة عبر الشبكات إلى هذه الأجهزة أو وسائط التخزين.

18-2 يجب تشفير البيانات الحساسة سواء كانت في حالة سكون أو أثناء نقلها.

ج- التعريفات

المصطلح أو الاختصار	التعريف
دائرة التعليم والمعرفة (ADEK)	دائرة التعليم والمعرفة - أبوظبي.
الدار للتعليم أو الشركة	يشير إلى الدار للتعليم بما في ذلك جميع مدارس الدار للتعليم المُشغَّلة، والمدارس المُدارة، وأكاديمية الدار للتدريب.
أكاديمية الدار للتدريب	تشير إلى أكاديمية الدار للتدريب التي تديرها الدار للتعليم.
/	تعني "أو" وتُستخدم لربط البدائل.
التسليم المستمر (CD)	يشير إلى التسليم المستمر.
التكامل المستمر (CI)	يشير إلى التكامل المستمر.
السرية والسلامة والتوافر (CIA)	يشير إلى السرية والسلامة والتوافر.
كوبيت (COBIT)	يشير إلى كوبيت 2019 - أهداف التحكم في المعلومات وتقنيات المعلومات ذات الصلة.
الإدارة	وحدة تنظيمية في الشركة، تشكل جزءًا من قسم. تخضع الإدارة لمنصب رئيس أو أعلى، والذي يقدم تقاريره مباشرة إلى المدير التنفيذي للقسم.
القسم	وحدة تنظيمية رأسية في الشركة، تقع تحت قيادة مدير تنفيذي يتبع مباشرة للرئيس التنفيذي، وقد يكون لها إدارات تابعة.
DNS	نظام أسماء النطاقات.
الخدمات الرقمية والتقنية (DTS)	إدارة الخدمات الرقمية والتقنية في الدار للتعليم.
الموظف	يشمل الموظفين المؤقتين والدائمين والعاملين بدوام كامل وجزئي.
المدير الإداري التنفيذي / EM	فرد يشغل منصب رئيس أو مدير أو أي لقب آخر في منصب قيادي بقسم، ويتبع مباشرة للرئيس التنفيذي.
الهيكل	نوع متخصص من السياسات يحتوي على هيكل منطقي يُصمم لتنظيم وثائق أخرى في خطة أو تسلسل هرمي أو هيكل.
الوثيقة الحاكمة	أي وثيقة ترسي القواعد أو المبادئ أو الإرشادات التي يجب أن تتماشى معها السياسة/إطار العمل.
المقر الرئيسي	يشير إلى المقر الرئيسي للدار للتعليم.
IDS	أنظمة كشف الاحتيال.
الوثيقة	وثيقة لتقديم التوجيه، أو فرض الالتزامات، أو تحديد المسؤوليات، أو تفويض السلطات، مثل إطار العمل، والسياسة، وإجراءات التشغيل القياسية، وما إلى ذلك.

المصطلح أو الاختصار	التعريف
IPS	نظام منع التسلل.
الآيزو	المنظمة الدولية للمعايير
المدارس المُدارة	تشير إلى مدارس أدنوك أو دائرة التعليم والمعرفة التي تديرها الدار للتعليم. تخضع مجالات المسؤوليات المحددة للاتفاقيات القانونية ذات الصلة المبرمة مع هذه الكيانات.
المدارس المُشغَّلة	تشير إلى المدارس المملوكة بالكامل والمُشغَّلة مباشرة من قبل الدار للتعليم.
PC	كمبيوتر شخصي
PII	المعلومات الشخصية المحددة للهوية.
دليل السياسات والإجراءات	وثيقة تحتوي على بيانات المبادئ، أو قواعد العمل، أو الضوابط الداخلية المصاغة والمتوافقة مع المتطلبات القانونية أو التنظيمية أو المؤسسية، والتي ستسترشد بها الدار للتعليم في إدارة شؤونها وتطوير إجراءاتها.
الإجراء/إجراء التشغيل القياسي (SOP)	وثيقة تصف الأنشطة اللازمة لتنفيذ سياسة ما، وتركز على المسؤوليات والمتطلبات اللازمة لإنجاز المهام والأنشطة والعمليات.
العملية	سلسلة من المهام التي يتعين القيام بها لإنجاز المهام التشغيلية، وتحقيق النتائج أو المخرجات المرجوة في نهاية المطاف، والمساهمة في التشغيل الناجح للمجموعة. تحدد العملية أيضًا مسؤوليات محددة ووثائق داعمة ضرورية لتنفيذها وصيانتها بالكامل.
SIEM	نظام مراقبة معلومات وأحداث الأمان
SLA	اتفاقية مستوى الخدمة
المستندات الداعمة	المستندات التي تدعم تنفيذ الوثائق. تشمل الوثائق الداعمة على سبيل المثال لا الحصر المبادئ التوجيهية، والنماذج، والقوالب، وإجراءات التشغيل القياسية، أو أي وثائق "غير خاضعة للرقابة" (مثل التي ينشئها النظام أو الخارجية).
المستخدم / المستخدم (المستخدمون) النهائيون	المستهلك أو المستخدم النهائي الأخير لمنتج أو نظام أو خدمة. هم أفراد يتفاعلون مباشرة مع تطبيق البرنامج النهائي أو الجهاز أو الخدمة الرقمية، مستخدمين ميزاتها ووظائفها لتلبية احتياجاتهم أو متطلباتهم الخاصة.
VPN	شبكة خاصة افتراضية
WAN	شبكة المنطقة الواسعة

د- الملحق

-1 شهادات الآيزو ذات الصلة

1-1 البند 5-3 الأدوار والمسؤوليات والسلطات التنظيمية

2-1 أ-5-2 أدوار ومسؤوليات أمن المعلومات

3-1 البند 5-1 القيادة والالتزام

4-1 البند 5-2 – السياسة

5-1 البند 6-1-2 تقييم مخاطر أمن المعلومات

6-1 البند 6-1-3 معالجة مخاطر أمن المعلومات

7-1 البند 9-1 المراقبة والقياس والتحليل والتقييم

8-1 أ-5-1 سياسات أمن المعلومات

9-1 أ-5-2 أدوار ومسؤوليات أمن المعلومات

10-1 أ-5-3 فصل الواجبات

11-1 أ-5-4 مسؤوليات الإدارة

12-1 أ-5-5 التواصل مع السلطات

13-1 أ-5-6 التواصل مع مجموعات المصالح الخاصة

14-1 أ-5-7 استخبارات التهديدات

15-1 أ-5-8 أمن المعلومات في إدارة المشاريع

16-1 أ-5-12 تصنيف المعلومات

17-1 أ-5-13 وسم المعلومات

18-1 أ-5-14 نقل المعلومات

19-1 أ-5-15 التحكم في الوصول إلى حركة المرور

20-1 أ-5-16 إدارة الهوية

21-1 أ-5-17 مصادقة المعلومات

22-1 أ-5-18 حق الوصول

23-1 أ-8-2 حقوق الوصول المتميز

24-1 أ-8-3 تقييد الوصول إلى المعلومات

25-1 أ-8-4 الوصول إلى شفرة المصدر

26-1 أ-8-5 المصادقة الآمنة

27-1 أ-8-18 استخدام البرامج المساعدة المتميزة

28-1 أ-5-19 سياسة أمن المعلومات لعلاقات الموردين

29-1 أ-5-20 معالجة الأمن ضمن اتفاقيات الموردين

30-1 أ-5-21 إدارة أمن المعلومات في سلسلة توريد تقنية المعلومات والاتصالات

31-1 أ-5-22 مراقبة ومراجعة وإدارة تغيير خدمات الموردين

32-1 أ-5-23 أمن المعلومات لاستخدام الخدمات السحابية

69-1 أ-7-13 صيانة المعدات

70-1 أ-7-14 التخلص الآمن من المعدات أو إعادة استخدامها

71-1 أ-8-1 الأجهزة الطرفية للمستخدم

72-1 أ-8-6 إدارة السعة

73-1 أ-8-7 الحماية من البرامج الضارة

74-1 أ-8-8 إدارة الثغرات التقنية

75-1 أ-8-9 إدارة التهيئة

76-1 أ-8-10 حذف المعلومات

77-1 أ-8-11 إخفاء البيانات

78-1 أ-8-12 منع تسرب البيانات

79-1 أ-8-13 النسخ الاحتياطي للمعلومات

80-1 أ-8-15 التسجيل

81-1 أ-8-16 مراقبة الأنشطة

82-1 أ-8-17 مزامنة الساعة

83-1 أ-8-19 تثبيت البرمجيات على الأنظمة التشغيلية

84-1 أ-8-20 ضوابط الشبكة

85-1 أ-8-21 أمن خدمات الشبكة

86-1 أ-8-22 الفصل في الشبكات

87-1 أ-8-23 تصفية الويب

88-1 أ-8-24 استخدام التشفير

89-1 أ-8-25 دورة حياة التطوير الآمن

90-1 أ-8-26 متطلبات أمن التطبيقات

91-1 أ-8-27 مبادئ هندسة ومعمارية النظم الآمنة

92-1 أ-8-28 الترميز الآمن

93-1 أ-8-29 اختبار الأمان في التطوير والقبول

94-1 أ-8-30 التطوير الخارجي

95-1 أ-8-31 فصل بيئات التطوير والاختبار والإنتاج

96-1 أ-8-32 إدارة التغيير

97-1 أ-8-33 معلومات الاختبار