إطار أمن المعلومات لشبكات المدارس

وزارة الاتصالات وتكنولوجيا المعلومات

إشارة الوثيقة
ISGSN2012-10-01-Ver 1.0

قائمة المحتويات

تعريفات

في تطبيق هذه الإرشادات، يكون للمصطلحات والتعابير التالية المعاني المحددة لكل منها، ما لم يقتض السياق خلاف ذلك:

- **فيروسات الكمبيوتر**: هجمات باستخدام رمز فيروسي ينسخ نفسه عن طريق تعديل البرامج الأخرى، وينتشر في عدة برامج أو في ملفات البيانات أو أجهزة النظام أو خلال عدة أجهزة ضمن شبكة، وقد ينتج عنه تدمير للبيانات أو ضعف أداء النظام.
- **المعلومات**: كافة المعلومات المحفوظة لدى المدرسة أو الخاضعة لسيطرتها، سواءً كانت في صورة إلكترونية أو صورة مسجلة أخرى، وتشمل المعلومات الإدارية والمالية والشخصية ومعلومات الطلاب، ومعلومات عن الجهات التي تتعامل أو تتواصل مع المدرسة.
- **توفر المعلومات**: القدرة على الوصول إلى المعلومات أو المصادر في موقع معين.
- **سرية المعلومات**: ضمان اقتصار الوصول إلى المعلومات على الأشخاص المخولين فقط وحمايتها على مدى دورة حياتها.
- **سلامة المعلومات**: دقة ومطابقة وموثوقية محتوى المعلومات.
- **إساءة الاستخدام**: استخدام أصول المعلومات لأغراض أخرى بخلاف الأغراض المصرح بها من قبل المستخدمين الداخليين أو الخارجيين.
- **الاختراق**: هجمات يقوم بها أشخاص غير مخولين أو أنظمة غير مخولة قد ينتج عنها انقطاع الخدمة أو زيادات ملحوظة في تكاليف التعامل مع الحوادث.
- **البيانات الشخصية**: معلومات خاصة أو شخصية أو سرية، سواءً كانت في صورة إلكترونية أو مكتوبة، عن طلاب أو أسر أو موظفين معروفين أو أحد أفراد الجمهور أو أي أشخاص آخرين.
- **معلومات شخصية**: معلومات مسجلة عن شخص معروف.
- **الأمن**: القدرة على حماية سلامة وتوفر وسرية المعلومات التي تحتفظ بها المدرسة وحماية أصول الشبكة من الاستخدام أو التعديل غير المرخص ومن الضرر أو التدمير العارض أو المقصود. ويشمل الأمن أمن مرافق الشبكة وتخزين البيانات خارج الموقع؛ والخدمات المتعلقة بالحوسبة والاتصالات والتطبيقات، وكذلك التطبيقات المتعلقة بالإنترنت والربط.

١ – التكليف القانوني

تنص المادة رقم (14)من المرسوم بقانون رقم 16 لسنة 2014 المبينة لاختصاصات وزارة الاتصالات وتكنولوجيا المعلومات(ويشار إليها فيما بعد باسم" الوزارة)"، على أن الوزارة تختص بالإشراف على قطاع الاتصالات وتكنولوجيا المعلومات وتطويره بما يتفق مع متطلبات التنمية الوطنية، وإيجاد بيئة تنظيمية مناسبة للمنافسة العادلة، ودعم وتنمية وتحفيز هذا القطاع وتشجيع الاستثمار فيه، وتأمين ورفع كفاءة البنية التحتية التكنولوجية والمعلوماتية، وتطوير الجيل التالي منها، وتوعية المجتمع بأهمية تكنولوجيا المعلومات والاتصالات واستخدامها بطرق آمنة لتحسين حياة الفرد والارتقاء بالمجتمع، وصولا إلى بناء مجتمع المعرفة القائم على الاقتصاد الرقمي، وتنفيذ والإشراف على برامج الحكومة الإلكترونية.

وتنص المادة(9/12) من المرسوم بقانون رقم 27 لسنة 2014 باعتماد الهيكل التنظيمي للوزارة، على اختصاص الوزارة بصياغة التشريعات والسياسات والمعايير المتعلقة بنظم تكنولوجيا المعلومات، والمعاملات الإلكترونية، وخدمات الحكومة الإلكترونية، لإحداث التحول التكنولوجي في الجهات الحكومية في دولة قطر.

٢– مقدمة

المدارس حول العالم قد تكون عرضة للاختراق والهجمات الإلكترونية، مما يعرض بيانات الطلاب والموظفين والإدارة للخطر. ويعد هذا الأمر مقلقاً للغاية بالنظر إلى أن حفظ البيانات الشخصية والسرية عن الطلاب والآباء والموظفين على أجهزة الكمبيوتر الخاصة بالمدرسة، وأجهزة الكمبيوتر الشخصية المحمولة وأجهزة الكمبيوتر المنزلية وبطاقات الذاكرة USB وغيرها من الوسائط قد أصبح ممارسة شائعة في المدارس في الوقت الحالي. وتتحمل المدارس واجب حماية البيانات الشخصية للموظفين والطلاب التي يتم تخزينها ونقلها إلكترونياً. وقد وضعت هذه الإرشادات لمساعدة المدارس على إحكام ممارساتها وإجراءاتها لضمان أمن تلك البيانات.

ومن بين أمثلة البيانات السرية التي يمكن الكشف عنها السجلات المالية وبيانات كشوف الرواتب والملفات الطبية للطلاب ونتائج الامتحانات وخطوط سير الحافلات.. الخ

ويتمثل المبدأ الرئيس لهذا الدليل في وجوب قيام المدارس بكل شيء ضمن صلاحيتها لضمان سلامة وأمن أي مادة ذات طبيعة شخصية أو حساسة عن طريق حماية سريتها وسلامتها وتوفرها.

لماذا أمن المعلومات

١- ضمان سرية المعلومات.
٢- ضمان دقة المعلومات.
٣- ضمان توفر البيانات.
٤- تحسين الإنتاجية عن طريق ضمان وقت عمل الشبكة وسرعة التعافي من حالات الاختراق الأمني.

٣– النطاق والتطبيق

تلخص وثيقة موجهات أمن المعلومات الماثلة ما هو منتظر من كافة الموظفين في المدرسة في سياق واجباتهم فيما يتعلق بأمن المعلومات وأجهزة الكمبيوتر.

وتهدف هذه الإرشادات إلى حماية ما يلي:

- الموظفين والطلاب والآباء والزائرين.
- الأصول، بما في ذلك أصول المعلومات.

- السجلات المدرسية (الإدارية والمالية والصحية... الخ)
- صورة المدرسة والسمعة العامة.

وذلك عن طريق تقليل مخاطر:

- الفقدان أو التلف العرضي للأصول.
- التعديل أو الإفصاح غير المرخص أو غير المقصود للمعلومات الشخصية أو السرية أو أي شكل آخر من أشكال إساءة الاستخدام.
- اختراق المعلومات أو أي تصرفات مقصودة وضارة تحدث بسبب غياب الوعي بنتائجها.

بتحقيق الأهداف التالية:

- **الوقاية** : كلما كانت السياسات الوقائية أفضل، انخفضت احتمالية نجاح الهجمة.
- **الكشف**: يجب أن تكون أنشطة الكشف مستمرة، وأن تصبح جزءً من سياسات وإجراءات أمن المعلومات.
- **الاستجابة**: استراتيجيات وأساليب التعامل مع أي هجوم أو فقدان، وخطة للاستجابة واسترداد التشغيل وإبطال مفعول التهديد.

وتنطبق هذه الإرشادات على ما يلي:

- كافة الخدمات في المدرسة.
- كافة الموظفين والطلاب في المدرسة.
- أي طرف آخر يعمل في المدرسة أو في مباني المدرسة.

تقدم هذه الوثيقة المعلومات الضرورية التي تمكن الموظفين وغيرهم من النهوض بمسؤوليتهم العامة لحماية معلومات وأصول المدرسة. ويمكن للمدارس ان تقوم بتعديل هذه الوثيقة لتعكس ظروفها الخاصة حتى يتسنى لها إصدار ونشر وثيقة أمن المعلومات الخاصة بها.

٤– بنود الإرشادات

الغرض من هذه الإرشادات هو المحافظة على سلامة البيانات واستمرار العمل بسلاسة. وتتألف موجهات الأمن من عدة قواعد وسلوكيات، مثل سياسة كلمة المرور التي تطلب من المستخدمين استخدام كلمات مرور لا يسهل تخمينها أو اختراقها، وقواعد الجدران النارية التي تسمح بمرور بيانات معينة إلى الشبكة وخارجها.

٤-١ أمن الموظفين

٤-١-١ يتعين أن تتضمن إجراءات تعيين كافة الموظفين وتعريفهم بالمنظمة فهم وتوضيح المسؤولية العامة عن أمن المعلومات.

٤-١-٢ يتعين أن يخضع المتعاقدين والمستشارين والمدربين الخارجيين والمعلمين المؤقتين / الإدارات المؤقتة وغيرهم من العاملين في مباني المدرسة أو من يتم منحهم حق الوصول إلى أنظمة المدرسة لعمليات الفحص وللاتفاقيات الملائمة للخدمات التي يتم تقديمها.

٤-١-٣ يتعين أن يوقع العاملين والطلاب والمتطوعين والآباء وأي أشخاص آخرين لا يرتبطون بعقد عمل وتم منحهم حق الوصول إلى أنظمة الكمبيوتر المدرسية، بما في ذلك الوصول عن بُعد، على اتفاقيات أمن وسرية معلومات.

٤-١-٤ يتعين عدم تزويد الموظفين العاملين بشكل مؤقت في المدرسة بحسابات دخول للأنظمة تتيح لهم الوصول إلى بيانات حساسة. بالإضافة إلى ذلك، يجب معاملة السجلات الورقية بنفس الحذر، وأن تقتصر المشاركة على القدر المطلوب من البيانات اللازم لأدائهم وظائفهم بفاعلية.

٤-١-٥ يتعين إعداد سجل بالأجهزة والبطاقات الذكية... الخ التي تصدر للموظفين الجدد وأي شخص آخر مذكور في الفقرات ٤-١-٣ و٤-١-٤.

٤-١-٦ يتعين رد كافة ممتلكات المدرسة أو تحديد المسئولية عنها عند انتهاء علاقة العمل. كما يتعين إلغاء حسابات البريد الإلكتروني وشبكة المدرسة والمكتبة وغير ذلك من حسابات الوصول إلى الأنظمة. ويجب تغيير كلمات المرور التي تحمي البيانات الحساسة.

٤-٢ أمن المعلومات

٤-٢-١ تعد المعلومات أحد الأصول الهامة في المدرسة، ويجب ألا ينظر إليها كأحد المصادر الشائعة التي يمكن تبادلها بحرية.

٤-٢-٢ يتعين على المدارس وضع وتنفيذ برنامج توعية بأمن المعلومات لضمان دراية كافة الموظفين المطلعين على البيانات أو المتعاملين بها بمسؤولياتهم بشأن أمن المعلومات.

٤-٢-٣ يتعين حماية كافة المعلومات، سواءً كانت قابلة للكشف أم لا، من الفقدان أو التلف العرضي أو المقصود. كما يجب حماية المعلومات الشخصية والسرية من الوصول والإفصاح غير المرخص وغير المقصود.

٤-٢-٤ يجب أن تخضع كل مجموعة بيانات شخصية يتم تداولها بشكل منتظم مع جهة خارجية لاتفاقية مشاركة معلومات.

٤-٢-٥ يجب أن تحتفظ المدرسة بسجل مركزي لكافة اتفاقيات مشاركة البيانات وضمان معرفة الموظفين المعنيين بوجود مثل تلك الاتفاقيات ومدة سريانها ونطاقها.

٤-٢-٦ يجب أن يقتصر غرض واستخدامات جمع البيانات الشخصية على الحصول على معلومات وثيقة الصلة بالغرض. كما يجب الكشف عن تلك المعلومات بموافقة الشخص أو ولي الأمر المعني. ويجب ألا تستخدم تلك البيانات لأي غرض آخر، ما لم يحدد خلاف ذلك. كما يجب أن يقتصر الكشف عن البيانات الشخصية على الأشخاص الذين لهم الحق في الاطلاع على تلك البيانات. ويجب عدم الوصول إلى البيانات الشخصية أو الاطلاع عليها إلا بسبب مشروع.

٤-٢-٧ يجب أن يقتصر تخزين البيانات الشخصية على أقراص الشبكة المؤمّنة أو أجهزة الكمبيوتر المكتبية والمحمولة الآمنة أو في نظام آمن على شبكة الإنترنت أو برنامج تعلم، وهو ما يتطلب التأكد من هوية المستخدم (اسم المستخدم وكلمة المرور) للوصول إلى البيانات.

٤-٢-٨ يجب أخذ نسخ احتياطية من كافة البيانات الشخصية المخزنة إلكترونيا بصورة نظامية كجزء من الإدارة العادية للشبكة. ويعد التخزين الآمن لتلك النسخ الاحتياطية ضرورياً، كما يتعين إجراء اختبارات بشكل دوري.

٤-٢-٩ يجب على المدارس الاحتفاظ بسجل آمن لكافة كلمات المرور المستخدمة لتشفير البيانات الحساسة بحيث يمكن استرداد تلك البيانات وتغييرها عند ترك أحد الموظفين للعمل.

٤-٢-١٠ يجب أن يتوفر لدى المدرسة طريقة آمنة لإعادة ضبط كلمات المرور.

٤-٢-١١ يجب تشفير البيانات الشخصية أو أي بيانات سرية أخرى يتم نقلها إلى جهاز محمول، كما يجب حذفها قبل تقديم الجهاز إلى شخص آخر وفقاً لسياسة تأمين المعلومات الوطنية في قطر.

٤-٢-١٢ وفقاً لأصول التهيئة والإعداد، يعتبر البريد الإلكتروني والفاكس وسائط غير آمنة لنقل المعلومات الشخصية والسرية، ويجب تجنبهما عند وجود بديل. ويعتبر المرسل مسؤولاً دائماً عن ضمان إخطار المرسل إليه المعني بأي رسالة فاكس سرية قبل إرسالها.

٤-٢-١٣ في الظروف الاستثنائية التي تقتضي تداول بيانات شخصية عبر البريد الإلكتروني، يجب إرسال البيانات بأقصى درجة تأمين ممكنة، على سبيل المثال عن طريق تشفير ملف البيانات المرفق باستخدام كلمة مرور قوية يتم تقاسمها شفهياً.

٤-٢-١٤ يجب التخلص من الوثائق التي تحتوي على معلومات شخصية أو سرية بإتلافها. كما يجب عدم إعادة تدوير الأوراق التي تحتوي على بيانات شخصية أو استخدامها كمخلفات.

٤-٢-١٥ يجب تخزين الوثائق والوسائط وأجهزة الكمبيوتر التي لا حاجة لها والأجهزة المشابهة المعدة للتخلص منها بأمان لحين إزالتها للتخلص منها. كما يجب التخلص من كافة أجهزة الاتصالات وتكنولوجيا المعلومات وفقاً لسياسة تأمين المعلومات الوطنية في قطر.

٤-٢-١٦ عند العمل على بيانات شخصية وسرية يجب وضع شاشات الكمبيوتر ولوحات المفاتيح بحيث لا يمكن رؤيتها من خارج منطقة العمل.

٤-٢-١٧ في حالة وجود شبكة إدارية/ شبكة مناهج مشتركة، يجب أن يكون لدى المدرسة إجراءات واضحة جداً ومفهومة يتبعها كافة الموظفين لضمان حماية الشبكة.

٤-٢-١٨ يجب أن يتم العمل من المنزل بنفس مستوى الأمن للعمل من المكتب. كما يجب أن يكون كافة الموظفين العاملين خارج موقع المدرسة أو في المنزل على دراية بالمخاطر الإضافية والمؤثرة لما يلي:

أ- تسريب المعلومات عن طريق النظر إليها أو سماعها مصادفة.

ب- فرصة القرصنة عن طريق البلوتوث والشبكات المفتوحة Wi-Fi.

ج- ترك إمكانية الوصول إلى البيانات المدرسية الحساسة متاحة على أنظمة الكمبيوتر المنزلية.

٤-٢-١٩ يجب اتخاذ نفس الاحتياطات عند الوصول إلى بيانات سرية على شبكة الإنترنت في المنزل، ويجب عدم نسخ تلك البيانات على جهاز الكمبيوتر.

٤-٢-٢٠ يعتبر أي شخص يقوم بنقل بيانات شخصية من مصادر المدرسة إلى جهاز الكمبيوتر الشخصي الخاص به أو أي بطاقة ذاكرة مسؤول شخصياً عن أمن واختراق تلك البيانات وعن أي تبعات قانونية.

٤-٢-٢١ عندما يتاح لأي موظف الدخول على أحد أجهزة الكمبيوتر المحمولة الخاصة بالمدرسة للاستخدام الشخصي، يجب إعداد الجهاز بحسابي مستخدمين مختلفين أحدهما للمدرسة والآخر للاستخدام الشخصي.

٤-٢-٢٢ يجب أن يكون الموظفون على دراية بمخاطر البيانات من الفيروسات وبرامج التجسس الناتجة عن عمليات تنزيل البيانات الشخصية، واتخاذ الاحتياطات الصارمة لمنع أو إزالة تلك التهديدات. ويجب أن تكون هذه الموضوعات مشمولة في سياسة الاستخدام المقبول بالمدرسة لاستخدام الموظفين للأجهزة الإلكترونية.

٤-٢-٢٣ إذا أتيح لأي عضو من الموظفين العلم بأي حادث يمكن أن يعرض أمن البيانات للخطر، فيجب عليه أن يبلغ عنه إدارة المدرسة. وتشمل مثل تلك الحوادث على سبيل المثال لا الحصر ما يلي:

أ- الوصول غير المرخص أو محاولة الوصول إلى أنظمة الكمبيوتر.

ب- الوصول غير المرخص للبيانات الشخصية بأي وسيلة.

ج- فقدان البيانات الشخصية أو الكشف عنها بشكل عارض.

٤-٣ أمن الأجهزة

٤-٣-١ يجب أن يكون لكل مستخدم على شبكة المدرسة وأجهزة الكمبيوتر المستقلة اسم المستخدم وكلمة المرور الخاص به، بالإضافة إلى مجموعة من الحقوق المناسبة لعمله.

٤-٣-٢ يجب أن يخضع الوصول إلى كافة تطبيقات أجهزة الكمبيوتر التي تتضمن بيانات شخصية للرقابة والحماية بكلمات مرور آمنة.

٤-٣-٣ يجب عدم منح أي طرف أو مورّد أو فني خارجي أو مكتب أو جهة أخرى حق الوصول إلى الأنظمة أو البيانات أو الأجهزة أو الشبكات، سواءً داخل المدرسة أو عن بعد، ما لم تكن هناك اتفاقية ملائمة للوصول لضمان تفهم تلك الجهات لمسؤولياتهم.

٤-٣-٤ تحدد كلمات المرور الخاصة بالمستخدمين من الموظفين، مثل كلمات المرور التي تستخدم للدخول على الشبكة أو أنظمة المدرسة، نظاماً تتبعياً للمساءلة، ويجب:

أ- عدم تسجيلها أو اطلاع أي شخص آخر عليها مع أي شخص آخر أو حفظها على جهاز الكمبيوتر.
ب- أن تكون كلمات مرور قوية (تتكون من عدد كبير من الحروف او الارقام او الرموز).
ج- ألا تتألف من كلمات معجمية أو أسماء شخصية أو كلمات مرتبطة بالمستخدمين.
د- أن يتم تغييرها بشكل دوري.
هـ- أن لا تكون مختلفة بصورة بسيطة عن كلمات المرور السابقة.

٤-٣-٥ يجب أن يحرص الموظفون على التأكد من حماية أجهزة الاتصالات وتكنولوجيا المعلومات ضد السرقة. كما يجب تأمين كافة الأجهزة تأميناً مادياً عند الإمكان. كما يجب الحرص بدرجة مماثلة على حماية الأجهزة التي يتم استخدامها خارج المدرسة أو في المنزل.

٤-٣-٦ يجب أن يكون لدى المدارس إجراءات لضمان أخذ نسخ احتياطية من كافة أجهزة الكمبيوتر المكتبية والمحمولة، بما في ذلك الأجهزة غير المرتبطة بشبكة المدرسة، وكذلك ضمان تثبيت برامج حديثة لمكافحة الفيروسات وبرامج التجسس والتحديثات الأمنية.

٤-٣-٧ يجب عدم فتح رسائل البريد الإلكتروني التي يكون من الواضح أنها رسائل غير مرغوبة أو الرسائل التي تحتوي على مرفقات غير مطلوبة أو غير متوقعة لتجنب مخاطر إصابة الأجهزة بالفيروسات.

٤-٣-٨ يجب أن يتم تثبيت البرامج على أجهزة المدرسة وفقاً لسياسة المدرسة فقط (والتي تتناول موضوعات مثل ترخيص البرامج و البرامج ذات المصادر المفتوحة للعامة open source والاستخدام في المنزل والسجلات والجرد... الخ).

٤-٣-٩ يجب أن يتم تركيب أو ربط الأجهزة (مثل محولات البلوتوث و شبكات Wi-Fi والأجهزة المحمولة الشخصية) بشبكة المدرسة وفقاً لسياسة المدرسة نظراً لمخاطر القرصنة والإصابة بالفيروسات.

٤-٣-١٠ يجب طلب المشورة الفنية على الفور في حالة الاشتباه في وجود فيروس.

٥- المراجع

دراسات من معهد SANS

http://www.sans.org/reading_room/whitepapers/bestprac/securing-network-k-12-public-School-environment_1292

سياسة السلامة الإلكترونية في المدارس – كيركليس Kirklees

www.**kirklees**safeguardingchildren.co.uk

دليل شركة YHGfL لوضع سياسة سلامة إلكترونية

https://public.rgfl.org/esafety/Shared%20Documents/YHGfL_Guidance_for_Creating_a_School_eSafety_Policy.pdf

مدارس مقاطعة براورد العامة

موجهات أمن معلومات المقاطعة

http://www.broward.k12.fl.us/Ets_Web/tpp/policies.htm

سياسة أمن المعلومات بوزارة التربية في أركنساس Arkansas

www.arkedu.state.ar.us/commemos/attachments/IT_**Security_Policies**.doc

وزارة التربية في المسيسيبي Mississippi

http://www.mde.k12.ms.us/docs/management-information-systems-library/enterprise_k12networksecuritypolicy.pdf?sfvrsn=2

سياسة تأمين المعلومات الوطنية (القطرية)

http://www.ictqatar.qa/en/documents/document/national-information-assurance-policy