وزارة التربية والتعليم	إجراء جودة
رقم الوثيقة: QP- 14 إصدار : 1/3	موافقة معالي الوزير:
	إعتماد مدير إدارة مركز الملكة رانيا العبدالله لتكنولوجيا التعليم والمعلومات:
التاريخ : 2025/2/10 صفحة : 4/1	إعتماد رئيس وحدة الرقابة الداخلية :
العنوان: ضبط البيانات الإلكترونية	إعتماد ممثل الجودة :

1 – الهـدف

1/1 يهدف هذا الإجراء إلى توضيح الطريقة المستخدمة في ضبط البيانات الإلكترونية، وتحديد الأشخاص المخولين بالدخول إلى البرامج، بما في ذلك إدارة كلمات المرور (Passwords) ، ونظام حفظ واستعادة البيانات (Backup System)باستخدام وسائط التخزين الحديثة مثل الأقراص الصلبة الخارجية أو الخدمات السحابية الآمنة، ومواكبة التطورات الحديثة في وزارة التربية والتعليم، بما يشمل تطبيق أفضل ممارسات الأمن السيبراني، والتخزين السحابي، وإدارة الأجهزة المحمولة (MDM) ، واستخدام تقنيات الذكاء الاصطناعي لتحليل المخاطر الأمنية.

2 – نطاق العمل

2/1 يطبق هذا الإجراء على جميع بيانات الإلكترونية الموجودة على جميع الأجهزة المتصلة بشبكة الوزارة، سواء كانت أجهزة طرفية، حواسيب مكتبية، أجهزة محمولة، أو خوادم سحابية والمؤثرة على جودة الخدمة المقدمة من قبل وزارة التربية والتعليم، بما في ذلك البرمجيات وقواعد البيانات والتطبيقات الإلكترونية المستخدمة.

3 – تعريفات

3/1 البيانات الإلكترونية: جميع الملفات والبرمجيات وقواعد البيانات المخزنة على أجهزة الحاسوب أو الخوادم السحابية أو الأنظمة المركزية.

3/2 كلمة المرور(Password) : سلسلة من الأحرف والأرقام والرموز تستخدم للتحقق من هوية المستخدم قبل السماح له بالوصول إلى النظام.

3/3 النسخ الاحتياطي(Backup) : عملية نسخ البيانات الإلكترونية المهمة وتخزينها في موقع آمن لضمان استرجاعها في حالة الفقدان أو التلف.

3/4 إدارة الأجهزة المحمولة(MDM) : نظام يتيح التحكم في الأجهزة المتصلة بشبكة الوزارة لضمان الأمان ومنع الوصول غير المصرح به.

3/5 الذكاء الاصطناعي الأمني :استخدام أنظمة تحليل السلوك لرصد أي محاولات دخول غير مشروعة أو سلوكيات مشبوهة وحسب الأوقات الغير مصرح بها.

3/6 المصادقة متعددة العوامل Multi-Factor Authentication (MFA) : هي تقنية أمان تتطلب من المستخدمين تقديم أكثر من عامل تحقق للوصول إلى الحسابات أو الأنظمة، مثل كلمة المرور (شيء تعرفه)

ورمز تحقق يُرسل إلى الهاتف (شيء تمتلكه) أو بصمة الإصبع (شيء يخصك)، مما يعزز الحماية ضد الاختراقات.

3/7 المصادقة الثنائية (Two-Factor Authentication – 2FA): هي طريقة أمان تُضيف طبقة حماية إضافية عند تسجيل الدخول، حيث تتطلب من المستخدم إثبات هويته باستخدام **عاملين مختلفين**، مثل كلمة المرور وهاتفه المحمول.

3/8 Active Directory (AD): خدمة من مايكروسوفت لإدارة الهوية والوصول داخل شبكة المؤسسة، تشمل المصادقة وإدارة المستخدمين والصلاحيات.

3/9 LDAP (Lightweight Directory Access Protocol): بروتوكول يستخدم للوصول إلى خدمات الدليل (Directory Services) وإدارة بيانات المستخدمين والموارد عبر الشبكة.

3/10 FreeIPA: حل مفتوح المصدر لإدارة الهوية والسياسات والأمان في بيئات Linux، يتضمن إدارة كلمات المرور والمصادقة باستخدام Kerberos.

3/11 حلول إدارة الأجهزة المحمولة (MDM – Mobile Device Management): هي تقنيات وبرمجيات تُستخدم لإدارة وتأمين الأجهزة المحمولة (مثل الهواتف الذكية والأجهزة اللوحية) في بيئات العمل.

3/21 التحكم في الوصول بناءً على الدور(RBAC - Role-Based Access Control) : تحديد الصلاحيات بناءً على دور المستخدم (مثل مدير، موظف، أو موظف دعم فني)، بحيث يتم منح الوصول فقط إلى البيانات أو العمليات التي يحتاجها المستخدم لأداء وظيفته.

4 – المسؤوليات

4/1 يتولى قسم الأمن السيبراني في إدارة مركز الملكة رانيا العبدالله لتكنولوجيا التعليم والمعلومات تحديد الأجهزة التي تحتاج إلى ضبط بكلمة مرور وفقًا لطبيعة العمل ومتطلبات الأمان.

4/2 يتولى رئيس كل قسم في مركز الوزارة ومديريات التربية والتعليم مسؤولية الإشراف على ضبط وحفظ جميع البرمجيات المؤثرة على جودة الخدمة.

4/3 يتولى رئيس القسم المعني مسؤولية توزيع وإدارة كلمات المرور للمستخدمين المصرح لهم فقط، مع ضرورة تحديثها دوريًا.

4/4 يتولى كل موظف يعمل على برمجيات معينة مسؤولية الحفاظ على سرية بياناتها وعدم مشاركتها مع أي شخص غير مخول.

4/5 يتولى قسم الأمن السيبراني في في إدارة مركز الملكة رانيا العبدالله لتكنولوجيا التعليم والمعلومات مسؤولية تفعيل أنظمة تحليل المخاطر والذكاء الاصطناعي لرصد محاولات الاختراق أو الأنشطة المشبوهة، واتخاذ الإجراءات التصحيحية الفورية.

4/6 يتولى قسم الأمن السيبراني و قسم أنظمة المعلومات الإدارية في إدارة مركز الملكة رانيا العبدالله لتكنولوجيا التعليم والمعلومات مسؤولية تعزيز مستوى الأمان باستخدام تقنيات مثل التحكم في الوصول بناءً على الدور **(RBAC - Role-Based Access Control)** والمصادقة متعددة العوامل **(Multi-Factor Authentication – MFA)** أو المصادقة الثنائية **(Two-Factor Authentication – 2FA)**

5 – العملية

5/1 يقوم قسم الأمن السيبراني في إدارة مركز الملكة رانيا العبدالله لتكنولوجيا التعليم والمعلومات بضبط بيانات الإلكترونية وصلاحيات الدخول كما يلي:

5/1/1 منح صلاحيات الدخول بناءً على مستوى المستخدم واحتياجات العمل، مع فرض سياسات أمان مشددة على الحسابات ذات الصلاحيات العالية.

5/1/2 التأكيد على عدم السماح لأي شخص بالاطلاع على بيانات البرمجيات أو تعديلها إلا إذا كان مخولًا بذلك، مع فرض قيود صارمة على الصلاحيات.

5/1/3 إلزام المستخدمين بتغيير كلمات المرور كل ثلاثة أشهر كحد أقصى من خلال إعداد سياسات كلمات المرور في النظام، مثل **Active Directory** أو **LDAP** أو **FreeIPA**، مع فرض معايير أمان صارمة (مثل استخدام 12 حرفًا على الأقل، ومزيج من الأحرف الكبيرة والصغيرة والأرقام والرموز).

5/1/4 تسجيل جميع محاولات الدخول الناجحة والفاشلة إلى الأنظمة لمراجعتها في حالة الاشتباه بأي نشاط غير طبيعي.

5/1/5 استخدام حلول إدارة الأجهزة المحمولة **(MDM)** لضمان أمان الأجهزة المتصلة بشبكة الوزارة.

5/2 حفظ البيانات والنسخ الاحتياطي

5/2/1 يقوم موظفو القسم المعنيون بعملية النسخ الاحتياطي للبيانات يوميًا أو أسبوعيًا أو شهريًا وفق أهمية البيانات، باستخدام تقنيات النسخ الاحتياطي التلقائي إلى خوادم داخلية أو سحابية معتمدة.

5/2/2 يقوم رؤساء الأقسام بالتأكد من تنفيذ عمليات النسخ الاحتياطي بانتظام، وتوثيقها في سجل حفظ البيانات (QF14-1) ، وتقديم تقرير دوري عن حالة النسخ الاحتياطية.

5/2/3 يقوم رؤساء الأقسام بتخزين النسخ الاحتياطية في مواقع آمنة ومحكمة الحماية، مع التأكد من تشفير البيانات للحفاظ على سريتها.

5/2/4 يقوم قسم الأمن السيبراني وقسم أنظمة المعلومات الإدارية في إدارة مركز الملكة رانيا العبدالله لتكنولوجيا التعليم والمعلومات بفرض قيود صارمة على الوصول إلى بيانات البرمجيات، مثل التحكم في الوصول بناة على الدور الوظيفي(RBAC) ، واستخدام التوثيق متعدد العوامل(MFA) ، وفرض سياسات قوية لكلمات المرور ما ورد في بند المسؤولية.

5/2/5 يقوم كل موظف بتشغيل برامج الحماية من الفيروسات وإجراء فحوصات دورية للتأكد من سلامة البيانات والأنظمة.

6 - الوثائق المتعلقة

#	اسم السجل	رقم السجل	مدة الحفظ
1/6	سجل حفظ البيانات	QF14-01	سنة

- مؤشرات القياس:

- عدد محاولات الدخول الفاشلة المسجلة وتحليلها لاتخاذ الإجراءات اللازمة.
- نسبة تنفيذ عمليات النسخ الاحتياطي وفق الجدول الزمني المحدد.
- نسبة الأجهزة التي يتم تحديث برامج الحماية من الفيروسات عليها بانتظام.
- عدد محاولات الاختراق التي تم رصدها عبر أنظمة الذكاء الاصطناعي وإحباطها.

- المخاطر:

- تسريب أو فقدان البيانات نتيجة الإهمال أو الهجمات الإلكترونية.
- فشل النسخ الاحتياطي أو عدم القدرة على استرجاع البيانات عند الحاجة.
- انتشار الفيروسات أو البرمجيات الخبيثة بسبب عدم تشغيل برامج الحماية بانتظام.
- عدم فعالية أنظمة الحماية المتوفرة.
- عدم إلتزام الموظفين بمعايير الأمان .
- العبث والتخريب.