سياسة إدارة هويات الدخول والصلاحيات

تم الاعتماد بمجلس إدارة جمعية التنمية الأسرية بمنطقة الباحة مَعين والمعتمد لدى المركز الوطني لتنمية القطاع الغير ربحي بخطاب تشكيل المجلس رقم NBM 015268 في تاريخ: ٢٠٢٣/١٢/١٤م والمعاد تشكيله بخطاب رقم EBM 018943 بتاريخ: ٢٠٢٤/٠٩/٢٤م حتى تاريخ:٢٠٢٧/١٢/١٤م

المملكة العربية السعودية
جمعية التنمية الأسرية بمنطقة الباحة (معين)
مسجلة بوزارة الموارد البشرية والتنمية الاجتماعية
برقم ٣٩٠
تحت اشراف مركز التنمية الاجتماعية بالباحة

تم التحديث والاعتماد بمحضر مجلس الإدارة رقم:٠٢ - ٢٠٢٤م بتاريخ: ٢٠٢٤/٠٦/١٢م، وبقرار اداري رقم:٢٠٢٤-٩٤ بتاريخ:٢٠٢٤/٠٦/٢٥م

باركود الاطلاع على الاعتمادات والتعديلات

المقدمة

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة هويات الدخول والصلاحيات على الأصول المعلوماتية والتقنية الخاصة بجمعية التنمية الأسرية بمنطقة الباحة (معين) لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية، وذلك من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-٢-١ من الضوابط الأساسية للأمن السيبراني (ECC-١:٢٠١٨) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بجمعية التنمية الأسرية بمنطقة الباحة (معين)، وتنطبق على جميع العاملين في جمعية التنمية الأسرية بمنطقة الباحة (معين).

الأدوار والمسؤوليات

١. راعي ومالك وثيقة السياسة: مسؤول تقنية المعلومات.
٢. مراجعة السياسة وتحديثها: مسؤول تقنية المعلومات.
٣. تنفيذ السياسة وتطبيقها: مسؤول تقنية المعلومات ومسؤول الموارد البشرية.

الالتزام بالسياسة

١. يجب على مسؤول تقنية المعلومات ضمان التزام جمعية التنمية الأسرية بمنطقة الباحة (معين) بهذه السياسة دورياً.
٢. يجب على كافة العاملين في جمعية التنمية الأسرية بمنطقة الباحة (معين) الالتزام بهذه السياسة.
٣. قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جمعية التنمية الأسرية بمنطقة الباحة (معين).

بنود السياسة

١- إدارة هويات الدخول والصلاحيات (Identity and Access Management)

١-١ إدارة الصلاحيات

١-١-١ توثيق واعتماد إجراء لإدارة الوصول يوضح آلية منح صلاحيات الوصول للأصول المعلوماتية والتقنية وتعديلها وإلغائها في جمعية التنمية الأسرية بمنطقة الباحة (معين)، ومراقبة هذه الآلية والتأكد من تطبيقها.

١-١-٢ إنشاء هويات المستخدمين (User Identities) وفقاً للمتطلبات التشريعية والتنظيمية الخاصة بجمعية التنمية الأسرية بمنطقة الباحة (معين).

١-١-٣ التحقق من هوية المستخدم (Authentication) والتحقق من صحتها قبل منح المستخدم صلاحية الوصول إلى الأصول المعلوماتية والتقنية.

١-١-٤ توثيق واعتماد مصفوفة (Matrix) لإدارة تصاريح وصلاحيات المستخدمين (Authorization) بناءً على مبادئ التحكم بالدخول والصلاحيات التالية:

١-١-٤-١ مبدأ الحاجة إلى المعرفة والاستخدام (**Need-to-Know and Need-to-Use**).

١-١-٤-٢ مبدأ فصل المهام (**Segregation of Duties**).

١-١-٤-٣ مبدأ الحد الأدنى من الصلاحيات والامتيازات (**Least Privilege**).

١-١-٤-٤ تطبيق ضوابط التحقّق والصلاحيات على جميع الأصول التقنية والمعلوماتية في جمعية التنمية الأسرية بمنطقة الباحة (معين) من خلال نظام مركزي آلي للتحكّم في الوصول، مثل بروتوكول النفاذ إلى الدليل البسيط (**Lightweight Directory Access Protocol "LDAP**").

١-١-٤-٥ منع استخدام الحسابات المشتركة (**Generic User**) للوصول إلى الأصول المعلوماتية والتقنية الخاصة بجمعية التنمية الأسرية بمنطقة الباحة (معين).

١-١-٤-٦ ضبط إعدادات الأنظمة ليتم إغلاقها تلقائياً بعد فترة زمنية محدّدة (**Session Timeout**)، (يوصى ألا تتجاوز الفترة ١٥ دقيقة).

١-١-٤-٧ تعطيل حسابات المستخدمين غير المستخدمة خلال فترة زمنية محدّدة (يوصى ألا تتجاوز الفترة ٩٠ يوماً).

١-١-٤-٨ ضبط إعدادات جميع أنظمة إدارة الهويات والوصول لإرسال السجلات إلى نظام تسجيل ومراقبة مركزي وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني.

١-١-٤-٩ عدم منح المستخدمين صلاحيات الوصول أو التعامل المباشر مع قواعد البيانات للأنظمة الحساسة، حيث يكون ذلك من خلال التطبيقات فقط، ويستثنى من ذلك مشرفي قواعد البيانات (**Database Administrators**). [CSCC-٢-١-٧]

١-١-٤-١٠ توثيق واعتماد إجراءات واضحة للتعامل مع حسابات الخدمات (**Service Account**) والتأكد من إدارتها بشكل آمن ما بين التطبيقات والأنظمة، وتعطيل الدخول البشري التفاعلي (**Interactive Login**) من خلالها. (CSCC-٢-١-٧).

١-٢ منح حق الدخول:

١-٢-١ متطلبات حق الدخول لحسابات المستخدمين:

١-٢-١-١ منح صلاحية الدخول بناءً على طلب المستخدم من خلال نموذج أو عن طريق النظام المعتمد من قبل مديره المباشر ومالك النظام (System Owner) يُحدّد فيه اسم النظام ونوع الطلب والصلاحية ومدتها (في حال كانت صلاحية الدخول مؤقتة).

١-٢-١-٢ منح المستخدم حق الوصول إلى الأصول المعلوماتية والتقنية الخاصة بجمعية التنمية الأسرية بمنطقة الباحة (معين) بما يتوافق مع الأدوار والمسؤوليات الخاصة به.

١-٢-١-٣ إتباع آلية موحدة لإنشاء هويات المستخدمين بطريقة تتيح تتبع النشاطات التي يتم أداؤها باستخدام "هوية المستخدم" (User ID) وربطها مع المستخدم، مثل كتابة <الحرف الأول من الاسم الأول> نقطة <الاسم الأخير>، أو كتابة رقم الموظف المعرف مسبقاً لدى مسؤول الموارد البشرية.

١-٢-١-٤ تعطيل إمكانية تسجيل دخول المستخدم من أجهزة حاسبات متعدّدة في نفس الوقت (Concurrent Logins).

١-٢-٢ متطلبات حق الوصول للحسابات الهامة والحسّاسة

بالإضافة إلى الضوابط المذكورة في قسم متطلبات حق الوصول لحسابات المستخدمين، يجب أن تُطبَق الضوابط المُوضّحة أدناه على الحسابات ذات الصلاحيات الهامة والحسّاسة:

١-٢-١-١ تعيين حق وصول مستخدم فردي للمستخدمين الذين يطلبون الصلاحيات الهامة والحسّاسة (Administrator Privilege) ومنحهم هذا الحق بناءً على مهامهم الوظيفية، مع الأخذ بالاعتبار مبدأ فصل المهام.

١-٢-١-٢ يجب تفعيل سجل كلمة المرور (Password History) لتتبع عدد كلمات المرور التي تم تغييرها.

١-٢-١-٣ تغيير أسماء الحسابات الافتراضية، وخصوصاً الحسابات الحاصلة على صلاحيات هامة وحسّاسة مثل "الحساب الرئيسي" (Root) وحساب "مدير النظام" (Admin) وحساب "مُعرّف النظام الفريد" (Sys id).

١-٢-١-٤ منع استخدام الحسابات ذات الصلاحيات الهامة والحسّاسة في العمليات التشغيلية اليومية.

١-٢-١-٥ التحقّق من حسابات المستخدمين ذات الصلاحيات الهامة والحسّاسة على الأصول التقنية والمعلوماتية من خلال آلية التحقّق من الهوية متعدد العناصر (Multi-Factor Authentication "MFA") باستخدام طريقتين على الأقل من الطرق التالية:

- المعرفة (شيء يعرفه المستخدم "مثل كلمة المرور").
- الحيازة (شيء يملكه المستخدم فقط "مثل برنامج أو جهاز توليد أرقام عشوائية أو الرسائل القصيرة المؤقتة لتسجيل الدخول"، ويطلق عليها ("**One-Time-Password**").
- الملازمة (صفة أو سمة حيوية متعلقة بالمستخدم نفسه فقط "مثل بصمة الإصبع").

١-٢-١-٦ يجب أن يتطلب الوصول إلى الأنظمة الحساسة والأنظمة المستخدمة لإدارة الأنظمة الحساسة ومتابعتها استخدام التحقق من الهوية متعدد العناصر (MFA) لجميع المستخدمين.

١-٢-٣ الدخول عن بُعد إلى شبكات جمعية التنمية الأسرية بمنطقة الباحة (معين).

١-٣-٢-١ منح صلاحية الدخول عن بعد للأصول المعلوماتية والتقنية بعد الحصول على إذن مسبق من مسؤول تقنية المعلومات وتقييد الدخول باستخدام التحقق من الهوية متعدد العناصر (MFA).

١-٣-٢-٢ حفظ سجلات الأحداث المتعلقة بجميع جلسات الدخول عن بُعد الخاصة ومراقبتها حسب حساسية الأصول المعلوماتية والتقنية.

١-٣ إلغاء وتغيير حق الوصول

١-٣-١ يجب على مسؤول الموارد البشرية تبليغ مسؤول تقنية المعلومات لاتخاذ الإجراء اللازم عند انتقال المستخدم أو تغيير مهامه أو إنهاء/انتهاء العلاقة الوظيفية بين المستخدم وجمعية التنمية الأسرية بمنطقة الباحة (معين). ويقوم مسؤول تقنية المعلومات بإيقاف أو تعديل صلاحيات الدخول الخاصة بالمستخدم بناءً على مهامه الوظيفية الجديدة.

١-٣-٢ في حال تم إيقاف صلاحيات المستخدم، يمنع حذف سجلات الأحداث الخاصة بالمستخدم ويتم حفظها وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني.

٢- مراجعة هويات الدخول والصلاحيات

٢-١ مراجعة هويات الدخول (User IDs) والتحقق من صلاحية الوصول إلى الأصول المعلوماتية والتقنية وفقاً للمهام الوظيفية للمستخدم بناءً على مبادئ التحكم بالدخول والصلاحيات دورياً، ومراجعة هويات الدخول على الأنظمة الحساسة مرة واحدة كل ثلاثة أشهر على الأقل.

٢-٢ مراجعة الصلاحيات الخاصة (User Profile) بالأصول المعلوماتية والتقنية بناءً على مبادئ التحكم بالدخول والصلاحيات دورياً، ومراجعة الصلاحيات الخاصة بالأنظمة الحساسة مرة واحدة سنوياً على الأقل.

٢-٣ يجب تسجيل وتوثيق جميع محاولات الوصول الفاشلة والناجحة ومراجعتها دورياً.

٣- إدارة كلمات المرور

٣-١ تطبيق سياسة آمنة لكلمة المرور ذات معايير عالية لجميع الحسابات داخل جمعية التنمية الأسرية بمنطقة الباحة (معين)، ويتضمّن الجدول أدناه أمثلة على ضوابط كلمات المرور لكل مستخدم:

ضوابط كلمات المرور	جميع المستخدمين (All Users)	حسابات المستخدمين ذات الصلاحيات الهامة والحسّاسة (Privileged Users)	حسابات الخدمات (Service Account)
الحدّ الأدنى لعدد أحرف كلمة المرور	٨ أحرف أو أرقام أو رموز	١٢ حرفاً أو رقماً أو رمزاً	٨ أحرف أو أرقام أو رموز
سجل كلمة المرور	تذكّر ٥ كلمات مرور	تذكّر ٥ كلمات مرور	تذكّر ٥ كلمات مرور
الحد الأعلى لعمر كلمة المرور	١٨٠ يوماً	٤٥ يوماً	٤٥ يوماً
مدى تعقيد كلمة المرور	مُفعّل	مُفعّل	مُفعّل
مثال على تعقيد كلمة المرور	D_dyW٥$_	R@rS%YqY#b!u	r?M٤d٥V=
مدة إغلاق الحساب	٣٠ دقيقة أو حتى يقوم النظام بفك الإغلاق	٣٠ دقيقة أو حتى يقوم النظام بفك الإغلاق	٣٠ دقيقة أو حتى يقوم النظام بفك الإغلاق
حد إغلاق الحساب	٥ محاولات غير صحيحة لتسجيل الدخول	٥ محاولات غير صحيحة لتسجيل الدخول	لا توجد محاولات
إعادة ضبط عداد إغلاق الحساب بعد مرور فترة معينة	٣٠ دقيقة (يقوم المدير بفك إغلاق الحساب المغلق يدوياً)	٣٠ دقيقة (يقوم المدير بفك إغلاق الحساب المغلق يدوياً)	لا يوجد
استخدام التحقق متعدد العناصر	مُفعل على الدخول عن بعد فقط	مُفعل	غير مُفعل

٣-٢ معايير كلمات المرور

٣-٢-١ يجب أن تتضمّن كلمة المرور (٨) أحرف على الأقل.

٣-٢-٢ يجب أن تكون كلمة المرور معقّدة (Complex Password) وتتضمّن ثلاثة رموز من الرموز التالية على الأقل:

٣-٢-٢-١ أحرف كبيرة (**Upper Case Letters**).

٣-٢-٢-٢ أحرف صغيرة (**Lower Case Letters**).

٣-٢-٢-٣ أرقام (١٢٣٥).

٣-٢-٢-٤ رموز خاصّة (@#%*).

٣-٢-٣ يجب إشعار المستخدمين قبل انتهاء صلاحية كلمة المرور لتذكيرهم بتغيير كلمة المرور قبل انتهاء الصلاحية.

٣-٢-٤ يجب ضبط إعدادات كافة الأصول المعلوماتية والتقنية لطلب تغيير كلمة المرور المؤقتة عند تسجيل المستخدم الدخول لأول مرة.

٣-٢-٥ يجب تغيير جميع كلمات المرور الافتراضية لجميع الأصول المعلوماتية والتقنية قبل تثبيتها في بيئة الإنتاج.

٣-٢-٦ يجب تغيير كلمات مرور السلاسل النصية (Community String) الافتراضية (مثل: «Public» و«Private» و«System») الخاصة ببروتوكول إدارة الشبكة البسيط (SNMP)، ويجب أن تكون مختلفة عن كلمات المرور المستخدمة لتسجيل الدخول في الأصول التقنية المعنية.

٣-٣ حماية كلمات المرور

٣-٣-١ يجب تشفير جميع كلمات المرور للأصول المعلوماتية والتقنية الخاصة بجمعية التنمية الأسرية بمنطقة الباحة (معين) بصيغة غير قابلة للقراءة أثناء إدخالها ونقلها وتخزينها وذلك وفقاً لسياسة التشفير.

٣-٣-٢ يجب إخفاء (Mask) كلمة المرور عند إدخالها على الشاشة.

٣-٣-٣ يجب تعطيل خاصية "تذكّر كلمة المرور" (Remember Password) على الأنظمة والتطبيقات الخاصة بجمعية التنمية الأسرية بمنطقة الباحة (معين).

٣-٣-٤ منع استخدام الكلمات المعروفة (Dictionary) في كلمة المرور كما هي.

٣-٣-٥ يجب تسليم كلمة المرور الخاصة بالمستخدم بطريقة آمنة وموثوقة.

٣-٣-٦ إذا طلب المستخدم إعادة تعيين كلمة المرور عن طريق الهاتف أو الإنترنت أو أي وسيلة أخرى، فلا بد من التحقّق من هوية المستخدم قبل إعادة تعيين كلمة المرور.

٣-٣-٧ يجب حماية كلمات المرور الخاصة بحسابات الخدمة والحسابات ذات الصلاحيات الهامة والحسّاسة وتخزينها بشكل آمن في موقع مناسب (داخل مغلف مختوم في خزنة) أو استخدام التقنيات الخاصة بحفظ وإدارة الصلاحيات الهامة والحسّاسة (Privilege Access Management Solution).

٤- متطلبات أخرى

٤-١ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لإدارة هويات الدخول والصلاحيات.

٤-٢ يجب مراجعة تطبيق متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات دورياً.

٤-٣ يجب مراجعة هذه السياسة سنوياً على الأقل، أو في حال حدوث تغييرات في المتطلبات التشريعية أو التنظيمية أو المعايير ذات العلاقة.