٢- سياسة إدارة هويات الدخول والصلاحيات

المسؤول عنها	الاتصال المؤسسي
رمز السياسة	تقنية.س.٢
الحالة	معتمدة

-الاعتماد

الحمدالله والصلاة والسلام على رسول الله وبعد:

فقد اطلع أعضاء الجمعية العمومية بجمعية مكافحة السرطان الخيرية بالأحساء (تفاؤل) في اجتماعهم العادي يوم الثلاثاء بتاريخ ١٤٤١/٥/٣هـ الموافق ٢٠٢٠/١/٢٨م على سياسة معيار الامتثال والالتزام وقرروا اعتمادها والعمل بموجبها ونشرها على الموقع الإلكتروني للجمعية وفق الصيغة المرفقة بالاعتماد.

رئيس مجلس الإدارة

محمد بن عبد العزيز العفالق

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة هويات الدخول والصلاحيات على الأصول المعلوماتية والتقنية الخاصة بـجمعية مكافحة السرطان (تفاؤل) 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-٢٠١٨:١) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بجمعية مكافحة السرطان (تفاؤل) ، وتنطبق على جميع العاملين في جمعية مكافحة السرطان (تفاؤل) .

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 مكافحة السرطان (تفاؤل) ، ومراقبة هذه الآلية والتأكد من تطبيقها.

١-١-٢ إنشاء هويات المستخدمين (USER IDENTITIES)وفقاً للمتطلبات التشريعية والتنظيمية الخاصة بجمعية مكافحة السرطان (تفاؤل) .

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

١-١-٤ توثيق واعتماد مصفوفة (MATRIX)الإدارة تصاريح وصالحيات المستخدمين (AUTHORIZATION) بناءً على مبادئ التحكم بالدخول والصالحيات التالية:

١-١-٤-١ مبدأ الحاجة الى 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 الصالحيات والامتيازات (LEAST PRIVILEGE)

١-١-٤-٤ تطبيق ضوابط التحقّق والصالحيات على جميع الأصول التقنية والمعلوماتية في جمعية مكافحة السرطان (تفاؤل) 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 بـجمعية مكافحة السرطان (تفاؤل)

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 ٢ 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-2-2-1-7)

١-١-٤-١ توثيق واعتماد إجراءات واضحة للتعامل مع حسابات الخدمات (ACCOUNT SERVICE)والتأكد من إدارتها بشكل آمن ما بين التطبيقات والأنظمة، وتعطيل الدخول البشري التفاعلي (INTERACTIV LOGIN) من خلالها (CSCC-2-2-1-7)

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 او 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 الى الأصول المعلوماتية والتقنية الخاصة بـجمعية مكافحة السرطان (تفاؤل) بما يتوافق مع الأدوار والمسؤوليات الخاصة به.

١-٢-١-٣ اتباع آلية موحدة لإنشاء هويات المستخدمين بطريقة تتيح تتبع النشاطات التي يتم أداوها باستخدام " هوية المستخدم" (USER ID) وربطها مع المستخدم، مثل كتابة <الحرف الأول من الاسم الأول> نقطة <الاسم الأخير>، او 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 المهمة والحساسة

بالإضافة الى الضوابط المذكورة في قسم متطلبات حق الوصول لحسابات المستخدمين، يجب أن تطبَق الضوابط الموضحة أدناه على الحسابات ذات الصلاحيات المهمة والحساسة:

١-٢-٢-١ تعيين حق وصول مستخدم فردي للمستخدمين الذين يطلبون الصلاحيات المهمة والحساسة

(PRIVILEGE ADMINISTRATOR)

١-٢-٢-٢ يجب تفعيل سجل كلمة المرور (PASSWORD HISTORY) لتتبع عدد كلمات المرور التي تم تغييرها

١-٢-٢-٣ تغيير أسماء الحسابات الافتراضية، وخصوصاً الحسابات الحاصلة على صلاحيات مهمة وحسّاسة مثل "الحساب الرئيسي" (ROOT) وحساب "مدير النظام" (ADMIN) وحساب "مُعرّف النظام الفريد" (SYS ID).

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

١-٢-٢-٥ التحقّق من حسابات المستخدمين ذات الصالحيات 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 (TIME-ONE PASSWORD)
- الملازمة صفة أو سمة حيوية متعلقة بالمستخدم نفسه فقط "مثل بصمة الإصبع.

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

١-٢-٣ الدخول عن بُعد إلى شبكات جمعية مكافحة السرطان (تفاؤل).

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

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

١-٣ إلغاء وتغيير حق الوصول:

١-٢-٣ يجب على مسؤول الموارد البشرية تبليغ مسؤول تقنية المعلومات الاتخاذ الإجراء اللازم عند انتقال المستخدم أو تغيير مهامه أو إنهاء/انتهاء العالقة الوظيفية بين المستخدم وجمعية مكافحة السرطان (تفاؤل) . ويقوم مسؤول تقنية المعلومات بإيقاف أو تعديل صلاحيات الدخول الخاصة بالمستخدم بناءً على مهامه الوظيفية الجديدة.

١-٢-٤ في حال تم إيقاف صالحيات 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 والصالحيات دورياً، ومراجعة هويات الدخول على الأنظمة الحساسة مرة واحدة كل ثالثة أشهر على الأقل.

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

٣-٢ 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 مكافحة السرطان (تفاؤل) ، ويتضمّن الجدول أدناه أمثلة على ضوابط كلمات المرور لكل مستخدم:

ضوابط كلمات المرور	جميع المستخدمين (ALL USERS)	حسابات المستخدمين ذات الصلاحيات المهمة والحسّاسة (PRIVILEGED USERS)	حسابات الخدمات (SERVICE ACCOUNT)
الحدّ الأدنى لعدد أحرف كلمة المرور	٨ احرف أو أرقام او رموز	١٢ حرفا أو أرقام او رمزا	٨ أحرف أو أرقام او رموز
سجل كلمة المرور	تذكر ٥كلمات مرور	تذكر ٥ كلمات مرور	تذكر ٥ كلمات
الحد الأعلى لعمر كلمة المرور	١٨٠ يوم	٤٥ يوم	٤٥ يوم

مدى تعقيد كلمة المرور	مفعَل	مفعل	مفعل
مثال على تعقيد كلمة المرور	D_DYW5$_	R@RS%7QY#B!U	=R?M4D5V
مدة إغلاق الحساب	٣٠دقيقة أو حتى يقوم النظام بفك الإغلاق	٣٠دقيقة أو حتى يقوم النظام بفك الإغلاق	٣٠دقيقة أو حتى يقوم النظام بفك الإغلاق
حد اغلاق 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	مفعل	غير مفعل

٣-٢معايير كلمات المرور

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

٣-٢-٢يجب أن تكون كلمة المرور معقّدة (COMPLEX PASSWORD)وتتضمّن ثلاثة رموز من الرموز التالية

على الأقل:

٣-٢-٢-١ أحرف كبيره (UPPER CASE LETTERS).

٣-٢-٢-٢ احرف صغيره (LOWER CASE LETTERS).

٣-٢-٢-٣ أرقام (١٢٣٥).

٣-٢-٢-٤ رموز خاصة (#%*@).

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.

١-٣-٣ يجب تشفير جميع كلمات المرور للأصول المعلوماتية والتقنية الخاصة بـجمعية مكافحة السرطان (تفاؤل) بصيغة غير قابلة للقراءة أثناء إدخالها ونقلها وتخزينها وذلك وفقاً لسياسة التشفير.

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

٣-٣-٣ يجب تعطيل خاصية "تذكّر كلمة المرور" (REMEMBER PASSWORD)على الأنظمة والتطبيقات الخاصة بـجمعية مكافحة السرطان (تفاؤل).

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

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

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

٧-٣-٣ يجب حماية كلمات المرور الخاصة بحسابات الخدمة والحسابات ذات الصلاحيات المهمة والحسّاسة وتخزينها بشكل آمن في موقع مناسب) داخل مغلف مختوم في خزنة أو استخدام التقنيات الخاصة بحفظ وإدارة الصلاحيات المهمة والحسّاسة (PRIVILEGE (SOLUTION ACCESS MANAGEMENT

٤ -متطلبات أخرى

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

٤-٢يحب 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.

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 مكافحة السرطان (تفاؤل) بهذه السياسة دورياً.

٢.يجب على كافة العاملين في جمعية مكافحة السرطان (تفاؤل) الالتزام بهذه السياسة.

٣ .قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جمعية مكافحة السرطان (تفاؤل).