سياسة إدارة هويات الدخول والصلاحيات

مقيّد

التاريخ:	02/11/2025
الإصدار:	٢,٠
المرجع:	الهيئة الوطنية للأمن السيبراني

إخلاء المسؤولية

طُور هذا النموذج عن طريق الهيئة الوطنية للأمن السيبراني كمثال توضيحي يمكن استخدامه كدليل ومرجع للجهات. يجب أن يتم تعديل هذا النموذج ومواءمته مع أعمال جامعة نجران والمتطلبات التشريعية والتنظيمية ذات العلاقة. كما يجب أن يُعتمد هذا النموذج من قبل رئيس الجهة أو من يقوم/تقوم بتفويضه. وتخلي الهيئة مسؤوليتها من استخدام هذا النموذج كما هو، وتؤكد على أن هذا النموذج ما هو إلا مثال توضيحي.

`

قائمة المحتويات

`

الغرض

الغرض من هذه السياسة هو تحديد متطلبات الأمن السيبراني المتعلقة بإدارة هويات الدخول والصلاحيات على الأصول المعلوماتية والتقنية الخاصة بـجامعة نجران وذلك لحمايتها من المخاطر السيبرانية ومن التهديدات الداخلية والخارجية لـجامعة نجران ، من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تمت موائمة هذه السياسة مع الضوابط والمعايير الصادرة من الهيئة الوطنية للأمن السيبراني والمتطلبات التنظيمية والتشريعية ذات العلاقة.

نطاق العمل

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بجامعة نجران ، وتنطبق على جميع العاملين (الموظفين والمتعاقدين) في جامعة نجران .

بنود السياسة

١- البنود العامة

١-١ يجب توثيق واعتماد إجراء لإدارة الوصول يوضح آلية منح صلاحيات الوصول للأصول المعلوماتية والتقنية وتعديلها وإلغائها في جامعة نجران ، ومراقبة هذه الآلية والتأكد من تطبيقها.

١-٢ يجب إنشاء هويات المستخدمين (User Identities) وفقًا للمتطلبات التشريعية والتنظيمية الخاصة بجامعة نجران .

١-٣ يجب التحقق من هوية المستخدم (Authentication) باستخدام اسم مستخدم وكلمة مرور والتحقق من صحتها قبل منح المستخدم صلاحية الوصول إلى الأصول المعلوماتية والتقنية الخاصة بجامعة نجران .

١-٤ يجب التأكد من المحافظة على سرية هوية المستخدم والحسابات والصلاحيات، بما في ذلك الطلب من المستخدمين حفظ خصوصيتها (للعاملين، والأطراف الخارجية، والمستخدمين).

١-٥ يجب توثيق واعتماد ومراجعة مصفوفة (Matrix) لإدارة تصاريح وصلاحيات المستخدمين (Authorization) بناءً على مبادئ التحكم بالدخول والصلاحيات التالية:

- مبدأ الحاجة إلى المعرفة والاستخدام (Need-to-Know and Need-to-Use).
- مبدأ فصل المهام (Segregation of Duties).
- مبدأ الحد الأدنى من الصلاحيات والامتيازات (Least Privilege).

١-٦ يجب تطبيق ضوابط التحقّق من الهويات والصلاحيات على جميع الأصول التقنية والمعلوماتية في جامعة نجران من خلال نظام مركزي آلي للتحكّم في الوصول، مثل "خدمات النطاقات-الدليل النشط (Domain services -Active Director).

`

١-٧ يجب منع استخدام الحسابات المشتركة (Generic User) للوصول إلى الأصول المعلوماتية والتقنية الخاصة بجامعة نجران .

١-٨ يجب التأكد من الإدارة الآمنة للجلسات (Secure Session Management)، وتشمل موثوقية الجلسات (Authenticity)، وإقفالها (Lockout)، وإنهاء مهلتها (Timeout).

١-٩ يجب ضبط إعدادات الأنظمة وجلسات الاتصال ليتم إنهائها تلقائيًا بعد فترة زمنية محدّدة (Session Timeout) وفقًا لمعيار إدارة هويات الدخول والصلاحيات المعتمد لدى جامعة نجران .

١-١٠ يجب ضبط إعدادات الأنظمة وجلسات الاتصال ليتم إغلاقها مؤقتًا بعد عدد معين من محاولات الوصول الخاطئة وفقًا لمعيار إدارة هويات الدخول والصلاحيات المعتمد لدى جامعة نجران .

١-١١ يجب تعطيل حسابات المستخدمين غير المستخدمة خلال فترة زمنية محدّدة وفقًا لمعيار إدارة هويات الدخول والصلاحيات المعتمد لدى جامعة نجران .

١-١٢ يجب ضبط إعدادات جميع أنظمة إدارة الهويات والوصول لإرسال السجلات إلى نظام تسجيل ومراقبة مركزي وفقًا لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني.

١-١٣ يجب 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) على أن يتم تطبيق إجراءات تمنع إطلاع المشرفين على البيانات المصنفة والحساسة، وفقا لسياسة أمن قواعد البيانات المعتمدة لدى جامعة نجران .

١-١٤ يجب 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 ومراجعتها دورياً.

١-١٥ يجب إدارة صلاحيات المستخدمين للعمل عن بعد بناءً على احتياجات العمل، مع مراعاة حساسية الأنظمة ومستوى الصلاحيات، ونوعية الأجهزة المستخدمة من قبل الموظفين للعمل عن بعد وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-١٦ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات حماية إدارة هويات الدخول والصلاحيات.

٢- منح صلاحية الدخول

٢-١ متطلبات صلاحية الدخول لحسابات المستخدمين

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

٢-١-٢ يجب منح المستخدم صلاحية الوصول إلى الأصول المعلوماتية والتقنية الخاصة بجامعة نجران بما يتوافق مع الأدوار والمسؤوليات الخاصة به مع أخذ الموافقات اللازمة.

`

٢-١-٣ يجب اتباع آلية موحدة لإنشاء هويات المستخدمين بطريقة تتيح 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 مسبقًا لدى إدارة الموارد البشرية.

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

٢-١-٥ يجب تحديد عدد محاولات تسجيل الدخول غير الناجحة المسموح بها إلى النظام لتفادي هجمات تخمين كلمات المرور وفقًا لمعيار إدارة هويات الدخول والصلاحيات المعتمد لدى جامعة نجران .

٢-٢ متطلبات صلاحية الوصول للحسابات الهامة والحسّاسة

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

٢-٢-١ يجب تعيين صلاحيات مديري النظام بناءً على مهامهم الوظيفية، مع الأخذ بالاعتبار مبدأ فصل المهام.

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

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

٢-٢-٤ يجب منع استخدام الحسابات ذات الصلاحيات الهامة والحسّاسة في العمليات التشغيلية اليومية ومنعها من الوصول للإنترنت.

٢-٢-٥ يجب 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 عنصرين مستقلة على الأقل من آليات التحقق من الهوية على الأقل وفقًا لمعيار إدارة هويات الدخول والصلاحيات المعتمد لدى جامعة نجران .

٢-٢-٦ يجب استخدام التقنيات الخاصة بحفظ وإدارة الصلاحيات الهامة والحسّاسة (Privilege Access Management Solution).

٢-٢-٧ يجب أن يتطلب الوصول إلى الأنظمة الحساسة والأنظمة المستخدمة لإدارة الأنظمة الحساسة ومتابعتها استخدام آلية التحقق من الهوية متعدد العناصر (MFA) لجميع العاملين.

٢-٣ الدخول عن بُعد إلى شبكات جامعة نجران

٢-٣-١ يجب منح صلاحية الدخول عن بعد للأصول المعلوماتية والتقنية بعد الحصول على إذن مسبق من إدارة الأمن السيبراني وتقييد الدخول باستخدام التحقق من الهوية متعدد العناصر (MFA) عبر قنوات آمنة ومعتمدة في جامعة نجران .

`

٢-٣-٢ يجب حفظ سجلات الأحداث المتعلقة بجميع جلسات الدخول عن بُعد الخاصة ومراقبة الأنشطة المتعلقة بها بشكل مستمر حسب حساسية الأصول المعلوماتية والتقنية.

٢-٤ إلغاء وتغيير صلاحية الوصول

٢-٤-١ يجب على إدارة الموارد البشرية تبليغ إدارة تقنية المعلومات لاتخاذ الإجراء اللازم عند انتقال المستخدم أو تغيير مهامه أو إنهاء/انتهاء العلاقة الوظيفية بين المستخدم وجامعة نجران لتقوم إدارة تقنية المعلومات بإيقاف الحسابات والصلاحيات أو تعديلها بناءً على مهامه الوظيفية الجديدة مع ضرورة الأتمتة قدر الإمكان.

٢-٤-٢ في حال تم إيقاف صلاحيات المستخدم، يجب منع حذف سجلات الأحداث الخاصة بالمستخدم ويتم حفظها وفقًا لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني المعتمدة لدى جامعة نجران .

٢-٥ مراجعة هويات الدخول والصلاحيات

٢-٥-١ يجب مراجعة هويات الدخول (User IDs) الخاصة بالأصول المعلوماتية والتقنية واستخداماتها سنويًا، ومراجعة هويات الدخول على الأنظمة الحساسة واستخداماتها مرة واحدة كل ثلاثة أشهر على الأقل.

٢-٥-٢ يجب مراجعة صلاحيات المستخدمين (User Profile) الخاصة بالأصول المعلوماتية والتقنية واستخداماتها سنويًا، ومراجعة الصلاحيات الخاصة بالأنظمة الحساسة واستخداماتها كل ثلاث أشهر على الأقل.

٢-٦ إدارة كلمات المرور

٢-٦-١ يجب تطبيق سياسة آمنة لكلمة المرور ذات معايير عالية لجميع الحسابات داخل جامعة نجران وذلك وفقًا لمعيار إدارة الهويات والصلاحيات المعتمد لدى جامعة نجران ووفقًا للسياسات والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٦-٢ يجب إشعار المستخدمين قبل انتهاء صلاحية كلمة المرور لتذكيرهم بتغيير كلمة المرور قبل انتهاء الصلاحية.

٢-٦-٣ يجب عدم استخدام كلمة مرور تم استخدامها من قبل.

٢-٦-٤ يجب ضبط إعدادات كافة الأصول المعلوماتية والتقنية لطلب تغيير كلمة المرور المؤقتة عند تسجيل المستخدم الدخول لأول مرة.

٢-٦-٥ يجب تغيير جميع كلمات المرور الافتراضية لجميع الأصول المعلوماتية والتقنية قبل تثبيتها في بيئة الإنتاج.

٢-٦-٦ 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.

`

٢-٧ حماية كلمات المرور

٢-٧-١ يجب تشفير جميع كلمات المرور للأصول المعلوماتية والتقنية الخاصة بجامعة نجران بصيغة غير قابلة للقراءة أثناء إدخالها ونقلها وتخزينها وذلك وفقًا لسياسة التشفير المعتمدة لدى جامعة نجران .

٢-٧-٢ يجب إخفاء (Mask) كلمة المرور عند إدخالها على الشاشة.

٢-٧-٣ يجب تعطيل خاصية "تذكّر كلمة المرور" (Remember Password) على الأنظمة والتطبيقات الخاصة بجامعة نجران .

٢-٧-٤ يجب منع استخدام الكلمات المعروفة (Dictionary) في كلمة المرور كما هي.

٢-٧-٥ يجب تسليم كلمة المرور الخاصة بالمستخدم بطريقة آمنة وموثوقة من خلال إجراءات محددة ومعتمدة.

٢-٧-٦ 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 من خلال طرق محددة ومعتمدة على سبيل المثال لا الحصر: تفعيل وتحديث الأسئلة الأمنية.

٢-٧-٧ 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).

الأدوار والمسؤوليات

١- **مالك السياسة:** رئيس الأمن السيبراني.

٢- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.

٣- **تنفيذ السياسة وتطبيقها:** عمادة التحول الرقمي ومصادر المعرفة، وإدارة الموارد البشرية، وإدارة الأمن السيبراني.

٤- **قياس الالتزام بالسياسة:** إدارة الأمن السيبراني.

التحديث والمراجعة

يجب على إدارة الأمن السيبراني مراجعة السياسة سنويًا على الأقل أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في جامعة نجران أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

`

الالتزام بالسياسة

١- يجب على إدارة الأمن السيبراني التأكد من التزام جامعة نجران بهذه السياسة دوريًا.

٢- يجب على كافة العاملين في جامعة نجران الالتزام بهذه السياسة.

٣- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة نجران .

`