

جمعية البر الخيرية بتبليث

تحت إشراف وزارة الموارد البشرية
والتنمية الاجتماعية برقم 245



“

سياسة إدارة هويات الدخول والصلاحيات

”

2021م

4-1-1 توثيق واعتماد مصفوفة (Matrix) لإدارة تصاريح وصلاحيات المستخدمين (Authorization) بناءً على مبادئ التحكم بالدخول والصلاحيات التالية:

1-4-1-1 مبدأ الحاجة إلى المعرفة والاستخدام (Need-to-Know and Need-to-Use).

2-4-1-1 مبدأ فصل المهام (Segregation of Duties).

3-4-1-1 مبدأ الحد الأدنى من الصلاحيات والامتيازات (Least Privilege).

4-4-1-1 تطبيق ضوابط التحقق والصلاحيات على جميع الأصول التقنية والمعلوماتية في جمعية البر الخيرية بتثليث من خلال نظام مركزي آلي للتحكم في الوصول، مثل بروتوكول النفاذ إلى الدليل البسيط ("Lightweight Directory Access Protocol" LDAP).

5-4-1-1 منع استخدام الحسابات المشتركة (Generic User) للوصول إلى الأصول المعلوماتية والتقنية الخاصة بجمعية البر الخيرية بتثليث .

6-4-1-1 ضبط إعدادات الأنظمة ليتم إغلاقها تلقائياً بعد فترة زمنية محدّدة (Session Timeout)، (يوصى ألا تتجاوز الفترة 15 دقيقة).

7-4-1-1 تعطيل حسابات المستخدمين غير المستخدمة خلال فترة زمنية محدّدة (يوصى ألا تتجاوز الفترة 90 يوماً).

8-4-1-1 ضبط إعدادات جميع أنظمة إدارة الهويات والوصول لإرسال السجلات إلى نظام تسجيل ومراقبة مركزي وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني.

9-4-1-1 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 (CSCC-2-2-1-7). [Database Administrators].

10-4-1-1 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-2-2-1-7)

2-1 منح حق الدخول













































































































































































































































































































- 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").

6-2-2-1 يجب أن يتطلب الوصول إلى الأنظمة الحساسة والأنظمة المستخدمة لإدارة الأنظمة الحساسة ومتابعتها استخدام التحقق من الهوية متعدد العناصر (MFA) لجميع المستخدمين.

3-2-1 الدخول عن بُعد إلى شبكات جمعية البر الخيرية بتثليث .

1-3-2-1 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).

2-3-2-1 حفظ سجلات الأحداث المتعلقة بجميع جلسات الدخول عن بُعد الخاصة ومراقبتها حسب حساسية الأصول المعلوماتية والتقنية.

3-1 إلغاء وتغيير حق الوصول

3-2-1 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 البر الخيرية بتثليث . ويقوم مسؤول تقنية المعلومات بإيقاف أو تعديل صلاحيات الدخول الخاصة بالمستخدم بناءً على مهامه الوظيفية الجديدة.

4-2-1 في حال تم إيقاف صلاحيات المستخدم، يمنع حذف سجلات الأحداث الخاصة بالمستخدم ويتم حفظها وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني.












































































































































































































































































































حسابات الخدمات (Service Account)	حسابات المستخدمين ذات الصلاحيات الهامة والحساسة (Privileged Users)	جميع المستخدمين (All Users)	ضوابط كلمات المرور
8 أحرف أو أرقام أو رموز	12 حرفاً أو رقماً أو رمزاً	8 أحرف أو أرقام أو رموز	الحد الأدنى لعدد أحرف كلمة المرور
تذكر 5 كلمات مرور	تذكر 5 كلمات مرور	تذكر 5 كلمات مرور	سجل كلمة المرور
45 يوماً	45 يوماً	180 يوماً	الحد الأعلى لعمر كلمة المرور
مُفعّل	مُفعّل	مُفعّل	مدى تعقيد كلمة المرور
r?M4d5V=	R@rS%7qY#b!u	D_dyW5\$_	مثال على تعقيد كلمة المرور
30 دقيقة أو حتى يقوم النظام بفك الإغلاق	30 دقيقة أو حتى يقوم النظام بفك الإغلاق	30 دقيقة أو حتى يقوم النظام بفك الإغلاق	مدة إغلاق الحساب
لا توجد محاولات	5 محاولات غير صحيحة لتسجيل الدخول	5 محاولات غير صحيحة لتسجيل الدخول	حد إغلاق الحساب
لا يوجد	30 دقيقة (يقوم المدير بفك إغلاق الحساب المغلق يدوياً)	30 دقيقة (يقوم المدير بفك إغلاق الحساب المغلق يدوياً)	إعادة ضبط عداد إغلاق الحساب بعد مرور فترة معينة
غير مُفعّل	مُفعّل	مُفعّل على الدخول عن بعد فقط	استخدام التحقق متعدد العناصر

2-3 معايير كلمات المرور

- | | |
|---------|---|
| 1-2-3 | يجب أن تتضمن كلمة المرور (8) أحرف على الأقل. |
| 2-2-3 | يجب أن تكون كلمة المرور معقدة (Complex Password) وتتضمن ثلاثة رموز من الرموز التالية على الأقل: |
| 1-2-2-3 | أحرف كبيرة (Upper Case Letters). |
| 2-2-2-3 | أحرف صغيرة (Lower Case Letters). |
| 3-2-2-3 | أرقام (1235). |
| 4-2-2-3 | رموز خاصة (@/!/*#). |
| 3-2-3 | يجب إشعار المستخدمين قبل انتهاء صلاحية كلمة المرور لتذكيرهم بتغيير كلمة المرور قبل انتهاء الصلاحية |
| 4-2-3 | يجب ضبط إعدادات كافة الأصول المعلوماتية والتقنية لطلب تغيير كلمة المرور المؤقتة عند تسجيل المستخدم لأول مرة. |
| 5-2-3 | يجب تغيير جميع كلمات المرور الافتراضية لجميع الأصول المعلوماتية والتقنية قبل تثبيتها في بيئة الإنتاج. |
| 6-2-3 | يجب تغيير كلمات مرور السلاسل النصية (Community String) الافتراضية (مثل: «Public» و«Private» و الخاصة ببروتوكول إدارة الشبكة البسيط (SNMP)، ويجب أن تكون مختلفة عن كلمات المرور المستخدمة لتسجيل الدخول التقنية المعنية. |

الأدوار والمسؤوليات

1. راعي ومالك وثيقة السياسة: مسؤول تقنية المعلومات.
2. مراجعة السياسة وتحديثها: مسؤول تقنية المعلومات.
3. تنفيذ السياسة وتطبيقها: مسؤول تقنية المعلومات ومسؤول الموارد البشرية .

الالتزام بالسياسة

1. يجب على مسؤول تقنية المعلومات ضمان التزام جمعية البر الخيرية بتثليث بهذه السياسة دورياً.
2. يجب على كافة العاملين في جمعية البر الخيرية بتثليث الالتزام بهذه السياسة.
3. قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جمعية البر الخيرية بتثليث .

١

٢

٣

٤

٥

٦

٧

٨

٩

١٠

١١

١٢

١٣

١٤

١٥

١٦

١٧

١٨

١٩

٢٠

٢١

٢٢

٢٣

٢٤

٢٥

٢٦

٢٧

٢٨

٢٩

٣٠

٣١

٣٢

٣٣

٣٤

٣٥

٣٦

٣٧

٣٨

٣٩

٤٠

٤١

٤٢

٤٣

٤٤

٤٥

٤٦

٤٧

٤٨

٤٩

٥٠

٥١

٥٢

٥٣

٥٤

٥٥

٥٦

٥٧

٥٨

٥٩

٦٠

٦١

٦٢

٦٣

٦٤

٦٥

٦٦

٦٧

٦٨

٦٩

٧٠

٧١

٧٢

٧٣

٧٤

٧٥

٧٦

٧٧

٧٨

٧٩

٨٠

٨١

٨٢

٨٣

٨٤

٨٥

٨٦

٨٧

٨٨

٨٩

٩٠

٩١

٩٢

٩٣

٩٤

٩٥

٩٦

٩٧

٩٨

٩٩

١٠٠

١٠١

١٠٢

١٠٣

١٠٤

١٠٥

١٠٦

١٠٧

١٠٨

١٠٩

١١٠

١١١

١١٢

١١٣

١١٤

١١٥

١١٦

١١٧

١١٨

١١٩

١٢٠

١٢١

١٢٢

١٢٣

١٢٤

١٢٥

١٢٦

١٢٧

١٢٨

١٢٩

١٣٠

١٣١

١٣٢

١٣٣

١٣٤

١٣٥

١٣٦

١٣٧

١٣٨

١٣٩

١٤٠

١٤١

١٤٢

١٤٣

١٤٤

١٤٥

١٤٦

١٤٧

١٤٨

١٤٩

١٥٠

١٥١

١٥٢

١٥٣

١٥٤

١٥٥

١٥٦

١٥٧

١٥٨

١٥٩

١٦٠

١٦١

١٦٢

١٦٣

١٦٤

١٦٥

١٦٦

١٦٧

١٦٨

١٦٩

١٧٠

١٧١

١٧٢

١٧٣

١٧٤

١٧٥

١٧٦

١٧٧

١٧٨

١٧٩

١٨٠

١٨١

١٨٢

١٨٣

١٨٤

١٨٥

١٨٦

١٨٧

١٨٨

١٨٩

١٩٠

١٩١

١٩٢

١٩٣

١٩٤

١٩٥

١٩٦

١٩٧

١٩٨

١٩٩

٢٠٠

٢٠١

٢٠٢

٢٠٣

٢٠٤

٢٠٥

٢٠٦

٢٠٧

٢٠٨

٢٠٩

٢١٠

٢١١

٢١٢

٢١٣

٢١٤

٢١٥

٢١٦

٢١٧

٢١٨

٢١٩

٢٢٠

٢٢١

٢٢٢

٢٢٣

٢٢٤

٢٢٥

٢٢٦

٢٢٧

٢٢٨

٢٢٩

٢٣٠

٢٣١

٢٣٢

٢٣٣

٢٣٤

٢٣٥

٢٣٦

٢٣٧

٢٣٨

٢٣٩

٢٤٠

٢٤١

٢٤٢

٢٤٣

٢٤٤

٢٤٥

٢٤٦

٢٤٧

٢٤٨

٢٤٩

٢٥٠

٢٥١

٢٥٢

٢٥٣

٢٥٤

٢٥٥

٢٥٦

٢٥٧

٢٥٨

٢٥٩

٢٦٠

٢٦١

٢٦٢

٢٦٣

٢٦٤

٢٦٥

٢٦٦

٢٦٧

٢٦٨

٢٦٩

٢٧٠

٢٧١

٢٧٢

٢٧٣

٢٧٤

٢٧٥

٢٧٦

٢٧٧

٢٧٨

٢٧٩

٢٨٠

٢٨١

٢٨٢

٢٨٣

٢٨٤

٢٨٥

٢٨٦

٢٨٧

٢٨٨

٢٨٩

٢٩٠

٢٩١

٢٩٢

المحتويات

الصفحة	الموضوع
2	الأهداف
2	نطاق العمل وقابلية التطبيق
2	بنود السياسة
10	الأدوار والمسؤوليات
10	الالتزام بالسياسة