هذا المربع مخصّص لأغراض توجيهية. احذف جميع المربعات التوجيهية بعد تعبئة النموذج. يجب تحرير البنود الملوّنة باللون الأزرق بصورة مناسبة. والبنود الملونة باللون الأخضر هي أمثلة يجب حذفها. ويجب إزالة التظليل الملون بعد إجراء التعديلات.

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج معيار إدارة هويات الدخول والصلاحيات

استبدل <اسم الجهة> باسم الجهة في مجمل صفحات الوثيقة. وللقيام بذلك، اتبع الخطوات التالية:

- اضغط على مفتاحي "Ctrl" و"H" في الوقت نفسه.
- أضف "<اسم الجهة>" في مربع البحث عن النص.
- أدخل الاسم الكامل لجهتك في مربع "استبدال" النص.
- اضغط على "المزيد" وتأكّد من اختيار "Match case".
- اضغط على "استبدل الكل".
- أغلق مربع الحوار.

اختر التصنيف

التاريخ: اضغط هنا لإضافة تاريخ

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

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 <اسم الجهة> 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.

اختر التصنيف

الإصدار <١,٠>

اعتماد الوثيقة

الدور	المسمى الوظيفي	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل المسمى الوظيفي>	<أدخل الاسم الكامل للموظف>	اضغط هنا لإضافة تاريخ	<أدخل التوقيع>

نسخ الوثيقة

النسخة	التاريخ	عُدِّلَ بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة تاريخ	<أدخل الاسم الكامل للموظف>	<أدخل وصف التعديل>

جدول المراجعة

معدل المراجعة	التاريخ لأخر مراجعة	تاريخ المراجعة القادمة
مره واحدة كل سنة	اضغط هنا لإضافة تاريخ	اضغط هنا لإضافة تاريخ

اختر التصنيف

الإصدار <١,٠>

قائمة المحتويات

اختر التصنيف

الإصدار <١,٠>

الغرض

الغرض من هذا المعيار هو تحديد متطلبات الأمن السيبراني التفصيلية لإدارة هويات الدخول والصلاحيات لأنظمة وبيانات ومعلومات <اسم الجهة> وذلك لتقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية بغرض تحقيق الأهداف الرئيسية للحماية وهي: سرية المعلومات، وسلامة أنظمة المعلومات، وتوافرها.

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

نطاق العمل

يغطي هذا المعيار جميع الأصول المعلوماتية والتقنية (مثل أجهزة المستخدمين، الأجهزة المحمولة والخوادم) الخاصة ب<اسم الجهة> وينطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

المعايير

١	هوية المستخدم (User identity)
الهدف	إدارة هوية المستخدم باستخدام أنظمة تقنية المعلومات في <اسم الجهة>.
المخاطر المحتملة	قد يؤدي عدم وجود هوية مستخدم فريدة إلى عدم القدرة على مساءلة المستخدم عند الحاجة وعدم القدرة على تتبع أنشطته وضعف التحكم في حقوق وامتيازات الوصول.
الإجراءات المطلوبة	
١-١	على <اسم الجهة> تعيين مسؤول لتحديد عملية إصدار هوية مستخدم فريدة لجميع موظفي <اسم الجهة> والحفاظ عليها وتغييرها وفقًا للتوجيهات الناتجة عن متطلبات الأعمال و/أو المتطلبات القانونية.
١-٢	تطبيق آلية لإصدار هوية مستخدم لجميع الموظفين لاستخدامها مع أنظمة تقنية المعلومات الخاصة ب<اسم الجهة>.
١-٣	تحديد الحد الأدنى من متطلبات هوية المستخدم لتزويد هويات المستخدمين بسمات مناسبة ومتسقة.
١-٤	تحديد معيار كلمة مرور آمن باتباع الحد الأدنى من المتطلبات (انظر المعيار رقم ٣-٥).

١-٥	أن تتضمن عملية إصدار هويات مستخدم لجميع الموظفين الحد الأدنى من المتطلبات التالية: أ) مصفوفة أدوار ومسؤوليات يحدد من يمكنهم تقديم طلبات إصدار هوية المستخدم وتفويضها ب) كيفية تقديم طلب الحصول على هوية مستخدم جديدة ج) من يمكنهم طلب هوية مستخدم جديدة (مثل الموارد البشرية) د) الأشخاص الذين يمكنهم إنشاء هوية مستخدم ومنح حقوق الدخول ه) الأشخاص الذين يمكنهم تفويض الطلبات (مثل: المدير المباشر) و) كيفية ربط حقوق الدخول بمستخدم معين (مثل: بناءً على الدور أو الموقع) ز) استخدام نماذج هويات المستخدم لإنشاء بطاقة الهوية ح) كيفية إصدار هوية المستخدم وكلمة المرور ط) كيفية تعطيل هوية المستخدم ي) الحد الأقصى للوقت الذي يمكن أن يستغرقه طلب إنشاء أو تعطيل هوية مستخدم ك) الحد الأقصى للوقت الذي يجب فيه إلغاء جميع صلاحيات الدخول المرتبطة بهوية المستخدم، إذا لزم الأمر ل) الحد الأقصى للوقت بعد ذلك، والذي يجب حذف هوية المستخدم فيه م) كيفية تسجيل إصدار هوية المستخدم وحمايتها
١-٦	إصدار هوية مستخدم لجميع الموظفين لاستخدامها مع أنظمة تقنية المعلومات لدى <اسم الجهة>. وألّا تكون هذه المُعرفات عامة أو مشتركة.
١-٧	تنفيذ عملية تضمن إمكانية تدقيق جميع التغييرات وتسجيلها، مع الاحتفاظ بالسجلات لمدة ١٢ شهرًا على الأقل.
٢	التحقق من صلاحيات المستخدم (User authorization)
الهدف	حصول المستخدمين على تصريح باستخدام أنظمة تقنية المعلومات الخاصة بـ <اسم الجهة> (بما في ذلك أنظمة الحوسبة السحابية).
المخاطر المحتملة	قد يؤدي عدم حصول المستخدمين على تصريح إلى الوصول إلى الأنظمة أو البيانات والمعلومات التي لا تتناسب مع وظيفة المستخدم أو دوره أو مستواه الوظيفي أو تصريحه الأمني.
الإجراءات المطلوبة	
٢-١	تعيين مالك للعملية (Process owner) لتحديد عملية تفويض المستخدمين قبل منحهم امتيازات الدخول إلى أنظمة تقنية المعلومات الخاصة ب<اسم الجهة>.

٢-٢	تحديد وتوثيق عملية تفويض المستخدمين التي يجب أن تتضمن ما يلي كحد أدنى: أ) آلية التصريح بالوصول إلى الأنظمة والمعلومات والبيانات للمستخدم وتحديد المسؤولين المتفق عليهم لاعتماد التصريح (الأدوار) ب) ربط امتيازات الوصول بمستخدمين محددين (مثل: استخدام معرفات فريدة كمعرفات المستخدمين) ج) تحديد وتعيين المستخدمين الذين لديهم إمكانية وصول افتراضية د) موافقة المسؤولين على صلاحيات الوصول الافتراضي للأدوار الأساسية (مراقبة الوصول القائمة على مصفوفة الأدوار والمسؤوليات) ه) تعيين صلاحيات الوصول بناءً على "مبدأ الحاجة إلى المعرفة" و"الحاجة إلى الاستخدام" و"الحد الأدنى من الصلاحيات والامتيازات" (أي "لا شيء" إذا لم يكن الوصول مطلوبًا ومصرحًا به) والفصل بين المهام (انظر المعيار ٤) إلى الأنظمة المختلفة بما في ذلك على سبيل المثال لا الحصر الخوادم وقواعد البيانات وتطبيقات الويب الخارجية وأنظمة التسجيل و) ضمان عدم إصدار معرفات زائدة (مثل: هويات المستخدمين) للاستخدام ز) التحقق من قدرة وصول المستخدم في حالة الظروف الاستثنائية (على سبيل المثال، عندما لا تتوفر آليات التحكم في الوصول أو تكون غير عملية أو آمنة أو حيث لا تتوفر الوظائف الفنية)
٣-٢	الحصول على موافقة المسؤولين ذوي العلاقة وتطبيقها على جميع المستخدمين.
٤-٢	الاحتفاظ بملف أو قاعدة بيانات تحتوي على تفاصيل جميع المستخدمين المصرح لهم من قبل الأفراد المصرح لهم.
٥-٢	يجب حماية الملف أو قاعدة البيانات التي تحتوي على تفاصيل جميع المستخدمين المصرح لهم من الوصول غير المصرح به والتغيير غير المصرح به والإفصاح غير المصرح به باتباع الضوابط المنطقية والمادية.
٦-٢	تحديد آلية مراجعة امتيازات الوصول للمستخدمين المصرح لهم: أ) للتأكد من الإبقاء على امتيازات وصول مناسبة ب) للتحقق من حذف التصاريح الزائدة وحقوق الوصول المرتبطة بها (مثل الأفراد الذين قاموا بتغيير أدوارهم أو تركوا الجهة) ج) بشكل منتظم (أي مرة واحدة سنويًا على الأقل) د) بشكل أكثر تكرارًا للمستخدمين الذين لديهم امتيازات وصول خاصة / مرتفعة، أو عند استخدام بيانات مصنفة على أنها سرية وأعلى (أي كل ستة أشهر) ه) بشكل أكثر تكرارًا فيما يتعلق بوصول المستخدم إلى الأنظمة الحساسة (أي كل ثلاثة أشهر)

٢-٧	إنهاء جلسة المستخدم تلقائيًا بعد استيفاء الشروط المحددة، مثل انتهاء وقت الجلسة على أنظمة مختلفة بما في ذلك على سبيل المثال لا الحصر قواعد البيانات وتطبيقات الويب الخارجية ومراكز عمل المستخدمين.
٢-٨	إنشاء سجل مركزي يحتوي على تفاصيل جميع المستخدمين المصرح لهم (الحالية والسابقة)، والتي يحتفظ بها الأفراد المصرح لهم.
٢-٩	حماية السجل المركزي من الوصول والتغيير والإفصاح غير المصرح به باتباع الضوابط المنطقية والمادية.
٣	التحقق من هوية المستخدم (User authentication)
الهدف	تطبيق عملية التحقق الآمن من هوية المستخدم على أنظمة تقنية المعلومات الخاصة بـ <اسم الجهة>
المخاطر المحتملة	قد يؤدي عدم التحقق من هوية المستخدم إلى تمكين المستخدمين من انتحال شخصية مستخدمين آخرين، أو تجاوز حقوق وأنظمة الوصول أو البيانات والمعلومات غير المناسبة للمسمى الوظيفي للمستخدم أو دوره أو مستواه الوظيفي أو تصريحه الأمني.
الإجراءات المطلوبة	
٣-١	فرض عملية التحقق من هوية المستخدم عند الوصول إلى أنظمة تقنية المعلومات الخاصة بـ <اسم الجهة> (بما في ذلك على سبيل المثال لا الحصر الحوسبة السحابية وقواعد البيانات وأجهزة الشبكة وأجهزة الشبكة اللاسلكية) من خلال طلب استخدام معرف فريد وعامل (عوامل) داعمة (على سبيل المثال كلمات المرور/ العبارات أو الرموز المميزة أو كلمات المرور لمرة واحدة).
٣-٢	إعداد آليات التحقق من هوية المستخدم بحيث يتم: أ) إدخال جميع معلومات تسجيل الدخول قبل التحقق منها ب) تعتيم كلمات المرور ومعلومات تسجيل الدخول الأخرى أثناء عملية الإدخال ج) يقتصر عدد محاولات تسجيل الدخول غير الناجحة على ثلاث محاولات غير صحيحة، بعدها يتم إغلاق المستخدم مؤقتًا، مما يجبر على إعادة ضبط معلومات التحقق من هوية المستخدم (وليس هوية المستخدم) د) تخزين جميع معلومات التحقق من هوية المستخدم ومعالجتها بطريقة آمنة (مثل: باستخدام التشفير) ه) تسجيل جميع محاولات تسجيل الدخول وتخزينها بطريقة آمنة
٣-٣	تطبيق الاستخدام الآمن لمعلومات التحقق من هوية المستخدم (المستخدم وكلمات المرور وعوامل التحقق الأخرى)

٣-٤	مراجعة سجلات الوصول مرة واحدة على الأقل كل ستة أشهر لمحاولات تسجيل الدخول المتعددة باستخدام نفس هوية المستخدم، وكذلك لهوية المستخدم ذاتها المستخدمة من بوابات مختلفة (إمكانية تسجيل دخول المستخدم من أجهزة حاسبات متعدّدة في نفس الوقت)
٣-٥	أن يطبق معيار كلمة المرور لمراكز عمل المستخدمين الحد الأدنى من القواعد التالية: أ) ألّا يقل طول كلمة المرور عن ٨ عناصر ب) أن تتضمن كلمات المرور واحدًا على الأقل مما يلي: الحروف الصغيرة (a-z) والحروف الكبيرة (A-Z) والأرقام (٠-٩) والرموز الخاصة (مثل: £$*) ج) تغيير كلمات المرور بشكل منتظم، كل ٩٠ يومًا على الأقل، عند الاستخدام (غير مطلوب في حال تطبيق عملية التحقق من هوية المستخدم متعددة العوامل) د) لا يجوز تكرار كلمات المرور التي استخدمت خلال المرات الـ ١٢ الأخيرة ه) ألّا تتبع كلمات المرور التي يتم إنتاجها تلقائيًا نمطًا ثابتًا
٣-٦	تغيير جميع أسماء المستخدمين وكلمات المرور الافتراضية للأنظمة الجديدة قبل استخدامها في بيئة الإنتاج.
٣-٧	تعطيل أو إعادة تسمية الحسابات الافتراضية أو غير التفاعلية أو غير اللازمة على الأنظمة المختلفة بما في ذلك على سبيل المثال لا الحصر الخوادم وقواعد البيانات وتطبيقات الويب الخارجية وأنظمة التسجيل وأجهزة الشبكة وأجهزة الشبكة اللاسلكية ومراكز عمل المستخدمين أو إعادة تسميتها.
٣-٨	تنفيذ إجراءات التحقق متعددة العوامل المعتمدة للمستخدمين في الحالات التالية: أ) الوصول إلى النطاق ب) الأنظمة الحساسة أو الأنظمة المستخدمة في إدارة الأنظمة الحساسة ج) الخوادم الحساسة د) المستخدمين ذوي الامتيازات والصلاحيات (بما في ذلك مستخدمي الحوسبة السحابية ذو الصلاحيات) ه) تطبيقات الويب و) قواعد البيانات ز) أجهزة الشبكة ح) أجهزة الشبكة اللاسلكية ط) أنظمة التسجيل
٤	مبدأ فصل المهام (Segregation of duties)

الهدف	تطبيق فصل المهام ومنع المستخدمين من حقوق الوصول التي تمنحهم حقوق وصول مفرطة من دون قصد.
المخاطر المحتملة	عدم تطبيق مبدأ فصل المهام للمستخدمين قد يسمح بإجراء معاملات احتيالية أو خاطئة أو تتجاوز المستوى الوظيفي للمستخدم أو صلاحياته.
الإجراءات المطلوبة	
١-٤	تحديد أنواع الأنشطة التي تتطلب فصل المهام وحقوق الوصول.
٢-٤	تتضمن قائمة الأنشطة (على سبيل المثال لا الحصر) ما يلي، حيث قد يكون للمستخدمين مجموعة واحدة فقط من الحقوق من أي قائمة: أ) مهام إدارة تطبيقات الأعمال والأنظمة والشبكات ب) مهام المسؤولين عن تصميم وتطوير واختبار تطبيقات وأنظمة وشبكات الأعمال ج) تصميم الضوابط وتنفيذها وضمانها د) تصميم ومراجعة وتشغيل الكود والإعدادات ه) الوصول إلى بيئات التطوير والاختبار وقبول المستخدم والإنتاج (يجب عدم توفير بيانات الإنتاج في البيئات غير الإنتاجية) و) البدء (أو التغيير) والموافقة على الوظائف الحيوية أو الحساسة (مثل: المدفوعات والتسعير) ز) طلب حقوق الوصول والموافقة عليها وتوفيرها ح) بدء واعتماد وتنفيذ التغييرات على أنظمة تقنية المعلومات
٣-٤	توثيق ترتيبات ومعايير وإجراءات التحكم في الوصول. ويجب أن تراعي هذه الترتيبات والمعايير والإجراءات ما يلي: أ) متطلبات الأمن السيبراني وتصنيفات البيانات والاتفاقيات مع مسؤولي التطبيقات والمتطلبات التي حددها مسؤولو النظام والالتزامات القانونية والتنظيمية والتعاقدية ب) الحاجة إلى تحقيق المساءلة الفردية، وتطبيق ضوابط إضافية على المستخدمين ذوي امتيازات وصلاحيات الوصول الخاصة، وفصل المهام
٤-٤	مراجعة الأنشطة التي تتطلب فصل المهام وترتيبات التحكم في الوصول: أ) مرة واحدة سنويًا على الأقل لجميع المستخدمين ب) كل ثلاثة أشهر على الأقل للمستخدمين ذو الصلاحيات العالية
٥-٤	إلغاء حقوق الوصول التي تبين أنها تنتهك مبدأ فصل المهام أو معايير التحكم في الوصول على الفور.

اختر التصنيف

الإصدار <١,٠>

٦-٤	إجراء مراجعة لتحديد كيفية انتهاك مبدأ الفصل بين المهام.
٧-٤	تحديث مبدأ الفصل بين المهام عند الحاجة وتطبيقه لتعكس التغييرات المحددة في المراجعة.
٥	إدارة الوصول (Access management)
الهدف	إدارة امتيازات الوصول للمستخدمين الافتراضيين لأنظمة <اسم الجهة>.
المخاطر المحتملة	قد تسمح امتيازات وصلاحيات الوصول الممنوحة بشكل سيء للمستخدمين بإجراء معاملات غير مصرح بها أو إدخال أو تغيير البيانات والمعلومات، أو تغيير تشغيل النظام على نحو لا يتناسب مع وظيفة المستخدم أو دوره أو مستواه الوظيفي أو تصريحه الأمني.
الإجراءات المطلوبة	
١-٥	تعيين مسؤول عن العملية لتولي مسؤولية عملية توفير الوصول الافتراضي للمستخدم.
٢-٥	تحديد وتوثيق عملية توفير الوصول إلى النظام لتحديد كيفية طلب امتيازات وصلاحيات الوصول إلى التطبيق والموافقة عليها وتوفيرها وصيانتها.
٣-٥	تتضمن العملية المتطلبات التالية كحد أدنى: أ) طريقة تقديم طلب الوصول إلى النظام (أو تغيير هذا الوصول) ب) من يمكنه طلب الوصول إلى النظام للمستخدم (مثل: المستخدم، المدير المباشر، غير ذلك) ج) من يمكنه تفويض الوصول إلى النظام (مثل: مسؤول تطبيق الأعمال) د) الأشخاص الذين يمكنهم إنشاء هوية مستخدم ومنح حقوق الوصول ه) كيف ترتبط حقوق الوصول بمستخدم النظام (أي بناءً على الدور) و) كيفية الوصول إلى النظام ز) كيفية إصدار الوصول إلى النظام ح) كيف يمكن إلغاء الوصول إلى النظام ط) الحد الأقصى للوقت الذي يمكن أن يستغرقه طلب إنشاء أو تغيير أو إلغاء الوصول إلى النظام ي) كيفية تسجيل وحماية مشكلة الوصول إلى النظام
٤-٥	مراجعة امتيازات وصلاحيات الوصول إلى النظام مرة واحدة سنويًا على الأقل لضمان توافقها مع الأدوار والمسؤوليات الوظيفية للمستخدم.

٥-٥	على مسؤول النظام إجراء مراجعة مرة واحدة سنويًا على الأقل لضمان الوصول إلى النظام وأن يكون النشاط مناسبًا وساريًا، على سبيل المثال: استخراج البيانات من النظام. ويمكن استخدام بيانات السجل التي تم جمعها في هذه المراجعة.
٦-٥	مراجعة امتيازات وصلاحيات الوصول إلى نظام المستخدم للتأكد من أنها لا تنتهك أي قواعد للفصل بين المهام التي تحددها الجهة.
٧-٥	ضبط إعدادات الوصول إلى جميع أنظمة المستخدمين وفقًا لمبدأ الحد الأدنى من الصلاحيات والامتيازات.
٨-٥	تعطيل حسابات مستخدمي التطبيقات غير النشطة بعد ٣٠ يومًا من عدم النشاط المستمر، بعد الحصول على ملاحظات إدارة شؤون الموارد البشرية فيما يتعلق بأسباب عدم النشاط.
٩-٥	اقتصار الوصول إلى الأنظمة على المنطقة الإدارية أو الشبكة المحلية الافتراضية الإدارية فقط.
١٠-٥	يجب تنفيذ عملية (JML) لإدارة دورة حياة هوية المستخدم والسماح بالتصاريح اللازمة للأنظمة: أ) يجب منح حق الوصول تلقائيًا بناءً على تصاريح الوصول المعتمدة مسبقًا للموظفين الجدد بناءً على الأدوار الوظيفية ب) يجب مراجعة الوصول وتعديله وفقًا لذلك عند نقل الموظفين ج) يجب تعطيل الوصول إلى الأنظمة عند إنهاء خدمات الموظفين
٦	إدارة وصول المستخدمين ذوي الصلاحيات والامتيازات (Privileged user access management)
الهدف	إدارة وصول للمستخدمين ذوي الصلاحيات والامتيازات إلى أنظمة تقنية المعلومات الخاصة بـ <اسم الجهة>.
المخاطر المحتملة	قد يؤدي الافتقار إلى إدارة المستخدمين ذوي الصلاحيات إلى السماح للمستخدمين بالوصول إلى البيانات والمعلومات بطريقة غير ملائمة لوظيفة المستخدم أو دوره أو مستواه الوظيفي أو تصريحه الأمني. وقد يسمح ذلك للمستخدمين أيضًا بتغيير أو تعديل أو حذف البيانات والمعلومات، أو إجراء تغييرات على التطبيقات أو أنظمة التشغيل أو البرامج الأخرى التي يمكن أن تتداخل مع التشغيل العادي أو تعطله.
الإجراءات المطلوبة	

٦-١	تطبيق التقنيات الخاصة بحفظ وإدارة الصلاحيات المهمة والحسّاسة (PAM) لتمكين الوصول المؤقت القائم على الجلسة إلى أنظمة مختلفة، بما في ذلك على سبيل المثال لا الحصر الخوادم وقواعد البيانات وأنظمة التسجيل.
٦-٢	تعيين مسؤول عن العملية لتحديد عملية إصدار حسابات الوصول ذات الصلاحيات المهمة والحساسة وتوفيرها.
٦-٣	تتضمن العملية المتطلبات التالية كحد أدنى: أ) كيفية تقديم طلب الوصول ذي الصلاحيات المهمة والحساسة، أو كيفية إدخال تغييرات على هذا الوصول ب) مَن يمكنه طلب هوية مستخدم ذي صلاحيات ج) مَن يمكنه الموافقة على طلب مستخدم ذو صلاحيات وامتيازات د) من يمكنه تفويض منح الوصول ذي الصلاحيات ه) مَن يمكنه إنشاء هوية مستخدم ذي صلاحيات ومنح حقوق الوصول و) كيفية ربط حقوق الوصول بمستخدم ذي صلاحيات عالية (مثل: بناءً على الدور) ز) كيفية إصدار الصلاحيات المهمة والحساسة ح) كيفية إلغاء الصلاحيات المهمة والحساسة ط) الوقت الأقصى لمنح أو تغيير أو إلغاء الصلاحيات المهمة والحساسة ي) كيفية تسجيل وحماية الصلاحيات المهمة والحساسة ك) وتيرة الصلاحيات المهمة والحساسة وإعادة اعتماد الحساب
٦-٤	توثيق وتنفيذ معيار تسمية منفصل ونظام مستخدم لجميع المستخدمين ذوي الصلاحيات المهمة والحساسة.
٦-٥	تحديد نموذج لهويات المستخدمين ذوي الامتيازات والصلاحيات المهمة لتعيين سمات مناسبة باستمرار للمستخدمين ذوي الامتيازات والصلاحيات المهمة.
٦-٦	تعيين هوية مستخدم ذي امتيازات وصلاحيات مهمة منفصلة لكل مستخدم ذي امتيازات وصلاحيات محددة بحيث يكون متميزًا عن هوية المستخدم العادية للموظفين.
٦-٧	تطبق كلمات المرور التي يستخدمها المستخدمون ذوو الصلاحيات المهمة والحساسة للوصول إلى الأنظمة المختلفة، بما في ذلك على سبيل المثال لا الحصر الخوادم وقواعد البيانات وتطبيقات الويب الخارجية وأنظمة التسجيل، القواعد التالية كحد أدنى: أ) ألّا يقل طول كلمة المرور عن ١٠ عناصر

	ب) أن تتضمن كلمات المرور عنصراً واحدًا على الأقل من كل مما يلي: الحروف الصغيرة (a-z) والحروف الكبيرة (A-Z) والأرقام (٠-٩) والرموز الخاصة (مثل: £$*) ج) تغيير كلمات المرور بشكل منتظم - كل ٣٠ يومًا على الأقل د) لا يجوز تكرار كلمات المرور التي أُستخدمت خلال المرات الـ١٢ الأخيرة ه) عدم استخدام كلمات المرور بناءً على البيانات الشخصية للمستخدم ذي الصلاحيات والامتيازات، مثل تاريخ الميلاد.
٦-٨	تحديد الأنشطة والمهام التي تتطلب الصلاحيات المهمة والحساسة.
٦-٩	تنفيذ أنشطة ومهام الصلاحيات المهمة والحساسة باستخدام هويات مستخدمين ذوي صلاحيات مهمة وحساسة محددة.
٦-١٠	يجب على المستخدمين ذوي الصلاحيات المهمة والحساسة استخدام هوية المستخدم الخاص بهم للقيام بالمهام ذات الصلاحيات والامتيازات المهمة والحساسة.
٦-١١	يجب تسجيل الحسابات ذات الصلاحيات المهمة والحساسة في نظام إدارة الصلاحيات المهمة والحساسة.
٦-١٢	يجب أن يقتصر وصول المستخدمين ذوي الصلاحيات والامتيازات على الأفراد المحددين والذي يحتاجون إليه لأداء دورهم الوظيفي (مثل: مشرفي قواعد البيانات وموظفي الشؤون المالية وموظفي الموارد البشرية).
٦-١٣	يجب تسجيل استخدام الحسابات ذات الصلاحيات المهمة والحساسة. تسجل السجلات ما يلي كحد أدنى: أ) بيانات اعتماد المستخدم المستخدمة ب) وقت تسجيل الدخول ج) مصدر بروتوكول الإنترنت IP (حيث تم تسجيل الدخول) د) الأنشطة المُنفّذة ه) وقت تسجيل الخروج
٦-١٤	تخزين بيانات سجل حسابات المستخدمين ذوي الصلاحيات المهمة والحساسة في مكان آمن، على أن يقتصر الوصول إليها على الموظفين المصرح لهم، باستخدام ضوابط الوصول المادية والمنطقية.

٦-١٥	الاحتفاظ ببيانات سجل حسابات المستخدمين ذوي الصلاحيات المهمة والحساسة وفقًا لمعايير/إجراءات الاحتفاظ.
٦-١٦	مراجعة سجلات الوصول مرة واحدة شهريًا على الأقل للتحقق من استخدام بيانات اعتماد المستخدم ذي الصلاحيات المهمة والحساسة في المهام ذات الصلاحيات.
٦-١٧	يجب على الإدارة التنفيذية مراجعة صلاحيات الوصول كل ستة أشهر على الأقل لضمان ملاءمة حسابات المستخدمين والأنشطة ذات الصلاحيات المهمة والحساسة وصحتها وتأكيد أو تغيير أو إلغاء الصلاحيات المهمة والحساسة التي تم تعيينها. يمكن استخدام بيانات السجل التي تم جمعها في هذه المراجعة.
٦-١٨	يجب تقييد الوصول إلى قواعد البيانات بالمسؤولين عنها ومن خلال تقديم طلب بالوصول فقط (عندما يكون ذلك ممكنًا) وبناءً على مبدأ الحاجة للمعرفة والحاجة للاستخدام.
٧	إدارة الوصول إلى الحساب الفني (Technical account access management)
الهدف	إدارة الحسابات الآلية أو الفنية أو الخدمية (المعروفة جميعها باسم "الفنية") على أنظمة تقنية المعلومات الخاصة بـ <اسم الجهة>
المخاطر المحتملة	قد يؤدي عدم إدارة الحسابات الفنية إلى اختراق هذه الحسابات أو استخدامها بطريقة مماثلة لحسابات المستخدمين، مما يقلل من كفاءتها ويعرضها لتهديدات متزايدة.
الإجراءات المطلوبة	
٧-١	تعيين مسؤول عن عملية إدارة الحسابات الفنية لتحديد مكوناتها والنموذج اللازم لإصدار الحسابات الفنية وتقديمها.
٧-٢	إنشاء نموذج كأساس للحسابات الفنية لضمان اتساق تكوينها وسماتها.
٧-٣	تحديد آلية تسمية الحسابات الفنية. يضمن اصطلاح التسمية إمكانية تمييز الحسابات الفنية بسهولة عن حسابات المستخدمين والمستخدمين ذوي الصلاحيات المهمة.
٧-٤	يحتوي نموذج الحسابات الفنية على الإعدادات التالية: أ) أن تكون غير تفاعلية ب) أن تكون لديها كلمة مرور غير منتهية الصلاحية ج) لا تستطيع الوصول إلى أدوات الإنتاجية أو متصفحات الويب أو أدوات التواصل أو التعاون أو الإنترنت أو الخدمات الأخرى.

	د) أن يكون الوصول المطلوب منحه إلى الحساب منطويًا على الحد الأدنى من الصلاحيات والامتيازات/الحد الأدنى من القدرات لأداء المهام الموكلة إليه، على أن يتم ذلك بشكل صريح وتقييمه والموافقة عليه ه) تحديد وحدة الأعمال المسؤولة ومسؤول الحساب و) تعيين معرفات فريدة للحسابات الفنية وفقًا لاصطلاح التسمية
٧-٥	تخصيص حساب فني لشخص مسؤول يتولى مسؤولية ما يلي: أ) طلب إنشاء الهوية والحساب ب) تسجيل الحساب وكلمة المرور في نظام إدارة الصلاحيات المهمة والحساسة ج) طلب حقوق الوصول إلى الحساب د) مراجعة استخدام الحساب وتصحيح الوصول مرة واحدة سنويًا على الأقل ه) طلب إلغاء الحساب عند إزالة الأصل التقني من الشبكة
٧-٦	توثيق امتيازات الوصول المخصصة للحسابات الفنية.
٧-٧	الموافقة على صلاحيات وامتيازات الوصول المخصصة من قبل مدير مناسب وقد تخضع لضوابط إضافية.
٧-٨	تسجيل استخدام الحسابات الفنية.
٧-٩	تخزين بيانات سجل حسابات المستخدمين ذوي الصلاحيات المهمة والحساسة في مكان آمن، على أن يقتصر الوصول إليها على الموظفين المصرح لهم، باستخدام ضوابط الوصول المادية والمنطقية.
٧-١٠	الاحتفاظ ببيانات السجل الخاصة بالحسابات التقنية وفقًا لمعايير/إجراءات الاحتفاظ.
٧-١١	على وحدة الأعمال ومسؤول الحساب مراجعة الحسابات الفنية مرة واحدة سنويًا على الأقل للتأكد من أن نشاط الحساب الفني والوصول إليه (إعادة التصديق) مناسب وساري. يمكن استخدام بيانات السجل التي تم جمعها في هذه المراجعة.
٧-١٢	على وحدة الأعمال ومسؤول الحساب تأكيد الحسابات الفنية أو تغييرها أو إلغائها مرة واحدة سنويًا على الأقل. يمكن استخدام بيانات السجل التي تم جمعها في هذه المراجعة.
٧-١٣	أن يقتصر استخدام كلمات المرور الثابتة على المسؤولين المعنيين فقط عند الضرورة للأغراض غير التفاعلية، وكذلك لاستعادة الأنظمة المختلفة بما في ذلك على سبيل المثال لا الحصر أجهزة الشبكة وأجهزة الشبكة اللاسلكية التي تم فصلها عن الشبكة.

٨	إدارة الوصول عن بُعد (Remote access management)
الهدف	توفير الوصول الآمن عن بُعد إلى شبكات <اسم الجهة>
المخاطر المحتملة	قد يؤدي الوصول غير الآمن عن بعد إلى الإفصاح عن أنظمة وبيانات ومعلومات <اسم الجهة> على الإنترنت وللمستخدمين غير المصرح لهم بالوصول للأنظمة والمعلومات والبيانات.
الإجراءات المطلوبة	
١-٨	تعيين مسؤول عن العملية لتحديد عملية الوصول عن بعد إلى شبكة <اسم الجهة> بالنسبة للموظفين والأطراف الخارجية المصرح لهم.
٢-٨	تحديد وتوثيق عملية الوصول عن بعد إلى شبكة <اسم الجهة>.
٣-٨	يجب أن تتضمن العملية المتطلبات التالية كحد أدنى: أ) أنواع الأجهزة المسموح باستخدامها للوصول عن بعد ب) كيفية تقديم طلب الوصول عن بعد (أو تغيير هذا الوصول) ج) تقييم مخاطر الوصول المطلوبة عن بعد د) مَن يمكنه طلب الوصول عن بعد (مثل: الموظفين، المدير المباشر) ه) مَن يمكنه الموافقة على منح حق الوصول عن بعد (مثل: المدير المباشر) و) كيفية ربط حقوق الوصول بمستخدم الوصول عن بعد ز) كيفية إصدار حساب الوصول عن بعد والبرامج المرتبطة به ح) كيفية إلغاء حق الوصول عن بعد ط) الحد الأقصى للوقت الذي يمكن أن يستغرقه طلب إنشاء أو تغيير أو إلغاء الوصول عن بعد ي) كيفية تسجيل وحماية حق الوصول عن بعد والبرامج ذات الصلة للمستخدمين المصرح لهم
٤-٨	مراجعة صلاحيات وامتيازات الوصول عن بعد مرة واحدة سنويًا على الأقل لضمان توافقها مع الأدوار والمسؤوليات الوظيفية للمستخدم.
٥-٨	إعداد جميع عمليات الوصول عن بعد وفقًا لمبدأ الحد الأدنى من الصلاحيات والامتيازات.
٦-٨	أن تتطلب جميع عمليات الوصول عن بعد إلى شبكة <اسم الجهة> تشفير البيانات أثناء نقلها واستخدام التحقق من الهوية متعدد العناصر.

٧-٨	تسجيل استخدام الوصول عن بعد من قبل جميع المستخدمين، ويجب الاحتفاظ ببيانات السجل هذه وفقًا لسياسة ومعيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني الخاصة بـ <اسم الجهة>.
٨-٨	على مسؤول العملية إجراء مراجعة مرة واحدة سنويًا على الأقل للتأكد من أن الوصول عن بعد والنشاط مناسبان وساريان. يمكن استخدام بيانات السجل التي تم جمعها في هذه المراجعة.
٩-٨	تعطيل جميع حسابات الوصول عن بعد غير النشطة كجزء من مراجعة الحساب غير المستخدمة.
١٠-٨	إعداد خدمة الوصول عن بعد بحيث: أ) يتم فصل جلسات الوصول عن بعد تلقائيًا بعد فترة عدم النشاط المحددة مسبقًا البالغة ٣٠ دقيقة ب) يكون لصلات الوصول عن بعد حد زمني مطلق للاتصال كما هو محدد من قبل <اسم الجهة> ج) تستخدم جلسات الوصول عن بعد الاتصال بالشبكة الافتراضية الخاصة المعتمدة (VPN) لدى <اسم الجهة> د) يصادق المستخدمون عن بعد على الشبكة باستخدام المصادقة الثنائية المعتمدة (مثل: باستخدام هوية المستخدم الخاص بهم ورمز الأجهزة أو البرامج) ه) يجب ربط رموز الأجهزة أو البرمجيات المستخدمة في المصادقة الثنائية بشكل فريد مع الاستخدام الفردي
١١-٨	على <اسم الجهة> تطبيق الضوابط التنظيمية والفنية لمنع الوصول عن بعد للأنظمة الحساسة من خارج المملكة العربية السعودية.
١٢-٨	تقييد والتحكم بعمليات الوصول المتزامنة عن بعد (مثل: نفس المستخدم، محطات متعددة).

الأدوار والمسؤوليات

١- **مالك المعيار:** <رئيس الإدارة المعنية بالأمن السيبراني>.

٢- **مراجعة المعيار وتحديثه:** <الإدارة المعنية بالأمن السيبراني>.

٣- **تنفيذ المعيار وتطبيقه:** <الإدارة المعنية بتقنية المعلومات>.

٤- **قياس الالتزام بالمعيار:** <الإدارة المعنية بالأمن السيبراني>.

التحديث والمراجعة

يجب على <الإدارة المعنية بالأمن السيبراني> مراجعة المعيار سنويًا على الأقل أو في حال حدوث تغييرات تقنية جوهرية في البنية التحتية أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في <اسم الجهة> أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بالمعيار

١- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذا المعيار دوريًا.

٢- يجب على جميع العاملين في <اسم الجهة> الالتزام بهذا المعيار.

٣- قد يعرض أي انتهاك لهذا المعيار صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في <اسم الجهة>.