

بسم الله الرحمن الرحيم



المملكة العربية السعودية
جمعية المستقبل
لصناعة الكوادر البشرية
ترخيص : (1000832700)

سياسة الأمن السيبراني



الفصل الأول: الأحكام العامة

المادة الأولى: الهدف

تهدف هذه السياسة إلى حماية أصول الجمعية الرقمية ومعلوماتها وأنظمتها وشبكتها من الوصول أو الاستخدام أو التعديل أو الإفصاح أو الإلتلاف غير المصرح به، وضمان استمرارية الخدمات التقنية، ورفع مستوى الوعي بالأمن السيبراني، والاستجابة للحوادث ومعالجتها.

المادة الثانية: نطاق التطبيق

تطبق هذه السياسة على:
أعضاء مجلس الإدارة واللجان.
المسؤول التنفيذي والعاملين والمتدربين.
المتطوعين والمستشارين.
الموردين والشركاء والمنفذين الذين يصلون إلى أنظمة الجمعية.
جميع الأجهزة والشبكات والأنظمة والتطبيقات.
البريد الإلكتروني والحسابات والمنصات السحابية.
قواعد البيانات والنسخ الاحتياطية.
العمل عن بعد والأجهزة المحمولة.
المعلومات والبيانات الرقمية والورقية المرتبطة بالأنظمة.
أي خدمة تقنية تستضيف أو تعالج بيانات الجمعية.



المادة الثالثة: المرجعيات

تستند السياسة إلى:

اللائحة الأساسية للجمعية.

نظام الجمعيات والمؤسسات الأهلية ولائحته التنفيذية.

تعليمات المركز الوطني لتنمية القطاع غير الربحي.

الأنظمة والضوابط الوطنية ذات العلاقة بالأمن السيبراني.

نظام حماية البيانات الشخصية.

سياسة سرية المعلومات.

سياسة حماية البيانات والخصوصية.

سياسة استمرارية الأعمال والتعافي.

سياسة إدارة المخاطر.

سياسة إدارة الحوادث والأزمات.

سياسة إدارة العقود والاتفاقيات.

أي متطلبات نظامية أو تقنية واجبة التطبيق.

المادة الرابعة: التعريفات

الأمن السيبراني: حماية الشبكات والأنظمة والأجهزة والبرامج والبيانات من التهديدات والمخاطر الرقمية.

الأصل المعلوماتي: أي نظام أو جهاز أو برنامج أو قاعدة بيانات أو ملف أو خدمة تقنية.

المستخدم: الشخص الذي يملك صلاحية استخدام أصل معلوماتي.

الحساب: هوية رقمية تستخدم للوصول إلى نظام أو خدمة.



الصلاحيّة: مستوى الوصول أو الإجراء المسموح به للمستخدم.
الحادث السيبراني: واقعة تؤثر أو قد تؤثر في سرية المعلومات أو سلامتها أو توافرها.
الثغرة: ضعف في نظام أو إعداد أو إجراء يمكن استغلاله.
البرمجيات الخبيثة: برامج تهدف إلى الإضرار أو التجسس أو الوصول غير المصرح.
النسخ الاحتياطي: نسخة من البيانات أو الأنظمة تستخدم للاستعادة.
الطرف الخارجي: أي جهة خارج الجمعية تصل إلى أنظمتها أو بياناتها.

الفصل الثاني: مبادئ الأمن السيبراني

المادة الخامسة: المبادئ العامة

تلتزم الجمعية بالمبادئ الآتية:
حماية سرية المعلومات وسلامتها وتوافرها.
تطبيق مبدأ الحد الأدنى من الصلاحيات.
الوقاية قبل وقوع الحادث.
التحديث المستمر للأنظمة والضوابط.
توثيق جميع الصلاحيات والأحداث المهمة.
حماية البيانات خلال الجمع والحفظ والنقل والإتلاف.
فصل مهام الإدارة والتشغيل والمراجعة.
التوعية المستمرة للمستخدمين.
سرعة اكتشاف الحوادث والاستجابة لها.
اختبار النسخ الاحتياطية وخطط التعافي.



حماية الأنظمة عند تصميمها أو شرائها.
عدم استخدام أدوات أو خدمات غير معتمدة.

المادة السادسة: أهداف الأمن السيبراني

تسعى الجمعية إلى:

- منع الوصول غير المصرح.
- تقليل أثر الهجمات والحوادث.
- حماية بيانات المستفيدين والمتبرعين والموظفين.
- ضمان توافر الأنظمة الحيوية.
- رفع موثوقية الخدمات الإلكترونية.
- حماية الحسابات والأجهزة والشبكات.
- دعم استمرارية الأعمال والتعافي.
- الالتزام بالمتطلبات النظامية والتعاقدية.

الفصل الثالث: الحوكمة والمسؤوليات

المادة السابعة: مسؤولية مجلس الإدارة

يتولى مجلس الإدارة:

- اعتماد سياسة الأمن السيبراني.
- متابعة المخاطر والحوادث الجوهرية.
- توفير الموارد المناسبة.



اعتماد خطط التعافي والاستجابة.
متابعة نتائج المراجعة والاختبارات.
مساءلة الإدارة عن القصور الجوهري.
اعتماد قبول المخاطر التقنية العالية عند الحاجة.

المادة الثامنة: مسؤولية المسؤول التنفيذي

يتولى المسؤول التنفيذي:
تطبيق السياسة.
تعيين مسؤول عن الأمن السيبراني أو تكليف جهة مختصة.
اعتماد الإجراءات التنفيذية.
متابعة الالتزام الإداري والتقني.
تفعيل خطة الاستجابة للحوادث.
رفع الحوادث الجوهرية إلى مجلس الإدارة.
توفير التدريب والموارد.
متابعة الموردين ومزودي الخدمات.

المادة التاسعة: مسؤول الأمن السيبراني وتقنية المعلومات

يتولى المسؤول المختص:
إدارة الأنظمة والشبكات والأجهزة.
تحديد الأصول التقنية وتصنيفها.



- إدارة المستخدمين والصلاحيات.
- تطبيق التحديثات والحماية.
- مراقبة الأنظمة والسجلات.
- إدارة النسخ الاحتياطية.
- معالجة الثغرات والحوادث.
- إعداد خطط التعافي.
- تنفيذ الاختبارات الأمنية.
- تقديم التقارير والتوصيات.
- تدريب المستخدمين.
- مراجعة أمن الموردين.

المادة العاشرة: الإدارات المالكة للبيانات والأنظمة

- تلتزم الإدارات بما يأتي:
- تحديد البيانات والأنظمة التي تديرها.
- اعتماد صلاحيات العاملين لديها.
- مراجعة دقة البيانات.
- الإبلاغ عن الحاجة إلى نظام أو خدمة جديدة.
- عدم مشاركة البيانات خارج القنوات المعتمدة.
- الالتزام بخطط النسخ والاستعادة.
- التعاون في التحقيق والاستجابة.



مراجعة المخاطر المرتبطة بعملياتها.

المادة الحادية عشرة: المستخدمون

يلتزم كل مستخدم بما يأتي:

- حماية اسم المستخدم وكلمة المرور.
- عدم مشاركة الحساب أو الصلاحية.
- استخدام الأجهزة والأنظمة لأغراض العمل.
- عدم تثبيت برامج غير معتمدة.
- عدم فتح الروابط أو المرفقات المشبوهة.
- قفل الجهاز عند تركه.
- الإبلاغ عن أي حادث أو رسالة مشبوهة.
- عدم نسخ البيانات إلى وسائط شخصية.
- الالتزام بتعليمات العمل عن بعد.
- إعادة الأجهزة والعهد عند انتهاء العلاقة.

الفصل الرابع: إدارة الأصول التقنية

المادة الثانية عشرة: سجل الأصول

تنشئ الجمعية سجلاً للأصول التقنية يتضمن:

اسم الأصل ونوعه.

الرقم أو المعرف.





المالك أو الإدارة المسؤولة.

الموقع.

المستخدم.

مستوى الحساسية.

نظام التشغيل أو الإصدار.

تاريخ الشراء أو التفعيل.

حالة الدعم والصيانة.

تاريخ الإيقاف أو الإتلاف.

المادة الثالثة عشرة: تصنيف الأصول

تصنف الأصول وفق أهميتها إلى:

أصول حرجة.

أصول عالية الأهمية.

أصول تشغيلية.

أصول منخفضة الحساسية.

ويحدد مستوى الحماية والنسخ الاحتياطي والاستعادة بحسب التصنيف.

المادة الرابعة عشرة: الأجهزة

تلتزم الجمعية بما يأتي:



استخدام أجهزة معتمدة.

تثبيت برامج حماية مناسبة.

تطبيق التحديثات.

تشفير الأجهزة التي تحتوي بيانات حساسة عند الحاجة.

منع استخدام أجهزة شخصية للوصول إلى البيانات الحساسة إلا بضابط معتمد.

تسجيل الأجهزة المسلمة للعاملين.

مسح البيانات عند إعادة الاستخدام أو الإتلاف.

الإبلاغ عن الفقد أو السرقة فوراً.

المادة الخامسة عشرة: الوسائط القابلة للإزالة

لا تستخدم وحدات التخزين المحمولة إلا عند الحاجة وبموافقة مناسبة، ويجب:

فحصها أمنياً.

تشفير البيانات الحساسة.

منع استخدامها على أجهزة غير موثوقة.

حفظ سجل التسليم والاستلام.

إتلافها بطريقة آمنة عند انتهاء الحاجة.

الفصل الخامس: إدارة الهوية والصلاحيات

المادة السادسة عشرة: إنشاء الحسابات

لا ينشأ حساب مستخدم إلا بناء على طلب معتمد، ويتضمن:





اسم المستخدم ووظيفته.

الإدارة.

النظام المطلوب.

مستوى الصلاحية.

مدة الصلاحية.

موافقة مالك النظام.

تاريخ الإنشاء والمراجع.

المادة السابعة عشرة: مبدأ الحد الأدنى من الصلاحية

تمنح الصلاحية التي يحتاجها المستخدم لأداء مهمته فقط، ولا تمنح صلاحيات إدارية أو مالية أو تقنية واسعة إلا عند الضرورة وبموافقة صاحب الصلاحية.

المادة الثامنة عشرة: مراجعة الصلاحيات

تراجع الصلاحيات دورياً وعند:

تغيير الوظيفة.

النقل بين الإدارات.

انتهاء المشروع.

الإجازة أو الإيقاف.

انتهاء العقد أو التطوع.

وقوع حادث أو مخالفة.



تغيير النظام أو مستوى المخاطر.

المادة التاسعة عشرة: الحسابات ذات الصلاحيات العالية

تخضع الحسابات الإدارية أو الحساسة إلى:

موافقة إضافية.

مصادقة متعددة العوامل عند الإمكان.

تسجيل العمليات.

عدم استخدامها في العمل اليومي.

مراجعة دورية.

تغيير بيانات الوصول عند تغيير المسؤول.

منع مشاركتها بين الأشخاص.

المادة العشرون: إلغاء الصلاحيات

تلغى الحسابات والصلاحيات فور انتهاء الحاجة أو العلاقة، ويجب:

تعطيل الحساب.

إلغاء الوصول عن بعد.

استرداد الأجهزة والبطاقات.

تغيير كلمات المرور ذات العلاقة.

مراجعة العمليات الأخيرة عند الحاجة.

توثيق الإلغاء.



الفصل السادس: كلمات المرور والمصادقة

المادة الحادية والعشرون: ضوابط كلمات المرور

يجب أن تكون كلمات المرور:

قوية وغير قابلة للتخمين.

مختلفة بين الأنظمة المهمة.

غير مستخدمة في حسابات شخصية.

غير مكتوبة في أماكن مكشوفة.

غير مشتركة مع أي شخص.

محدثة عند الاشتباه بتسريبها.

محفوظة في أداة معتمدة عند الحاجة.

المادة الثانية والعشرون: المصادقة متعددة العوامل

تطبق المصادقة متعددة العوامل على:

الحسابات الإدارية.

البريد الإلكتروني.

الأنظمة المالية.

الأنظمة التي تحتوي بيانات حساسة.

الوصول عن بعد.

الخدمات السحابية المهمة.





المادة الثالثة والعشرون: الحسابات المشتركة

يحظر إنشاء حسابات مشتركة إلا عند الضرورة التقنية، ويجب عند استخدامها:
اعتماد سبب الاستثناء.
تحديد المسؤولين.
تسجيل العمليات.
تغيير كلمة المرور دورياً.
إلغاؤها عند انتهاء الحاجة.

الفصل السابع: حماية الشبكات والأنظمة

المادة الرابعة والعشرون: الشبكات

تطبق الجمعية ضوابط مناسبة، منها:
حماية الشبكة اللاسلكية.
تغيير الإعدادات الافتراضية.
فصل شبكة الضيوف عن شبكة العمل.
تقييد الوصول إلى الأنظمة الداخلية.
تحديث أجهزة الشبكة.
مراقبة الاتصالات غير المعتادة.
منع استخدام أجهزة غير موثوقة.

المادة الخامسة والعشرون: التحديثات





تطبق التحديثات الأمنية والتقنية في الوقت المناسب، ويجب:

حصر الأنظمة والإصدارات.

اختبار التحديثات المهمة.

إعطاء الأولوية للشغرات الحرجة.

توثيق التحديثات.

معالجة الأنظمة غير المدعومة.

اعتماد استثناءات مؤقتة عند تعذر التحديث.

المادة السادسة والعشرون: مكافحة البرمجيات الخبيثة

تستخدم الجمعية وسائل حماية مناسبة، وتمنع:

تثبيت برامج غير مرخصة.

تعطيل برامج الحماية.

فتح ملفات مشبوهة.

استخدام برمجيات مقرصنة.

تشغيل وسائط غير مفحوصة.

تجاوز ضوابط التحميل والتنزيل.

الفصل الثامن: البريد والتصيد والاستخدام المقبول

المادة السابعة والعشرون: البريد الإلكتروني

يلتزم المستخدم:



باستخدام البريد الرسمي في أعمال الجمعية.

بالتحقق من المرسل والروابط والمرفقات.

بعدم إرسال بيانات حساسة دون حماية.

بعدم إعادة توجيه الرسائل المهنية إلى بريد شخصي.

بالإبلاغ عن الرسائل المشبوهة.

بعدم استخدام البريد لانتحال صفة الجمعية.

المادة الثامنة والعشرون: التصيد والهندسة الاجتماعية

عند الاشتباه في رسالة أو اتصال:

لا يفتح المستخدم الرابط أو المرفق.

لا يرسل كلمة مرور أو رمز تحقق.

يتحقق من الطلب عبر قناة مستقلة.

يبلغ تقنية المعلومات.

يحفظ الرسالة كدليل.

يغير كلمة المرور إذا أدخل بياناته.

المادة التاسعة والعشرون: الاستخدام المقبول

يجوز استخدام أصول الجمعية في الأعمال المرتبطة بالعمل، ويحظر:

تنزيل أو نشر محتوى غير مشروع.

استخدام الأنظمة لأغراض شخصية مؤثرة.



محاولة تجاوز الضوابط.

فحص أو مهاجمة أنظمة دون تصريح.

تعيين العملات أو تشغيل خدمات غير معتمدة.

مشاركة حسابات أو برامج غير مرخصة.

تخزين محتوى مخالف أو مسيء.

الفصل التاسع: حماية البيانات والنسخ الاحتياطية

المادة الثلاثون: حماية البيانات

تطبق الجمعية سياسة حماية البيانات والخصوصية، ويجب:

تصنيف البيانات.

تقليل جمعها.

تقييد الوصول.

تشفير البيانات الحساسة عند الحاجة.

مراقبة المشاركة.

حذفها أو إخفاء هويتها عند انتهاء الغرض.

تسجيل الحوادث والإفصاحات.

المادة الحادية والثلاثون: النسخ الاحتياطية

تعد نسخ احتياطية للبيانات والأنظمة الحيوية، ويحدد لكل نظام:

دورية النسخ.





موقع الحفظ.

مدة الاحتفاظ.

مستوى التشفير.

المسؤول عن التنفيذ.

آلية اختبار الاستعادة.

الإجراء عند فشل النسخ.

المادة الثانية والثلاثون: اختبار الاستعادة

تختبر النسخ الاحتياطية بصورة دورية للتأكد من:

إمكانية استعادة البيانات.

سلامة الملفات.

تحقيق وقت الاستعادة المستهدف.

اكتمال البيانات.

قدرة الفريق على تنفيذ الإجراء.

توثيق النتائج والإجراءات التصحيحية.

الفصل العاشر: إدارة الحوادث السيبرانية

المادة الثالثة والثلاثون: الإبلاغ عن الحادث

يبلغ المستخدم فوراً عن:

فقد أو سرقة جهاز.



رسالة أو رابط مشبوه.

تسرب كلمة مرور.

وصول غير مصرح.

توقف أو سلوك غير طبيعي للنظام.

تشفير أو فقد ملفات.

تسرب أو إرسال بيانات إلى جهة خاطئة.

ظهور برمجية أو ملف مشبوه.

أي حادث قد يؤثر في أمن المعلومات.

المادة الرابعة والثلاثون: تصنيف الحوادث

تصنف الحوادث إلى:

منخفضة: أثر محدود ويمكن احتواؤه بسرعة.

متوسطة: تؤثر في مستخدم أو نظام محدود.

عالية: تؤثر في بيانات أو خدمات مهمة.

حرجة: تؤثر في أنظمة حيوية أو بيانات حساسة أو عدد كبير من أصحاب البيانات أو استمرارية الجمعية.

المادة الخامسة والثلاثون: الاستجابة للحادث

تتضمن الاستجابة:

تسجيل الحادث.

احتواء الضرر.



عزل الأصل المتأثر.

حفظ الأدلة والسجلات.

تحليل النطاق والسبب.

استعادة الخدمة بأمان.

إبلاغ المسؤولين والجهات المختصة عند الحاجة.

إشعار أصحاب البيانات عند وجوبه.

معالجة الثغرة.

إعداد تقرير ما بعد الحادث.

المادة السادسة والثلاثون: حظر العبث بالأدلة

يحظر على المستخدم حذف الملفات أو إعادة تهيئة الجهاز أو تغيير الإعدادات أو محاولة معالجة الحادث دون توجيه، إذا كان ذلك قد يؤدي إلى فقد الأدلة أو صعوبة التحقيق.

الفصل الحادي عشر: أمن التطبيقات والخدمات السحابية

المادة السابعة والثلاثون: شراء أو تطوير نظام

قبل شراء أو تطوير نظام جديد، تراجع الجمعية:

الغرض والاحتياج.

البيانات التي سيعالجها.

صلاحيات الوصول.

متطلبات الخصوصية.



أمن المورد.

النسخ الاحتياطية.

التكامل مع الأنظمة.

خطة الاستمرارية والخروج.

موقع تخزين البيانات.

الاختبارات الأمنية.

المادة الثامنة والثلاثون: الخدمات السحابية

لا تستخدم خدمة سحابية إلا بعد:

اعتمادها من الجهة المختصة.

مراجعة شروط الخدمة والخصوصية.

تقييم موقع معالجة البيانات.

تحديد الحسابات والصلاحيات.

تفعيل المصادقة المناسبة.

تحديد النسخ الاحتياطية.

تنظيم إعادة البيانات أو إتلافها.

تضمين الالتزامات في العقد.

المادة التاسعة والثلاثون: إدارة التغيير

لا يطبق تغيير جوهري على الأنظمة دون:



طلب تغيير معتمد.

تقييم أثر ومخاطر.

اختبار قبل التنفيذ.

خطة تراجع.

تحديد موعد مناسب.

توثيق النتيجة.

إشعار المستخدمين المتأثرين.

الفصل الثاني عشر: أمن الأطراف الخارجية

المادة الأربعون: الموردون والمنفذون

تتحقق الجمعية من أمن المورد أو المنفذ قبل تمكينه من الأنظمة أو البيانات، ويجب أن يتضمن العقد:

السرية وحماية البيانات.

ضوابط الأمن السيبراني.

إدارة الصلاحيات.

الإبلاغ عن الحوادث.

حق التدقيق.

التعاقد من الباطن.

إعادة البيانات أو إتلافها.

المسؤولية والتعويض.

خطة الخروج.



مدد الاستجابة والتعافي.

المادة الحادية والأربعون: الوصول المؤقت

يكون وصول الطرف الخارجي:

محدد الغرض.

محدود المدة.

مقيدا بالحد الأدنى.

مراقبا ومسجلا.

معتمدا من مالك النظام.

ملغى فور انتهاء المهمة.

الفصل الثالث عشر: التوعية والاختبارات

المادة الثانية والأربعون: التدريب

تدرب الجمعية العاملين والمتطوعين على:

كلمات المرور والمصادقة.

التصيد والهندسة الاجتماعية.

حماية البيانات.

العمل عن بعد.

استخدام البريد.

الإبلاغ عن الحوادث.



استخدام الأجهزة والوسائط.

التعامل مع الموردين.

النسخ الاحتياطية.

الالتزامات بعد انتهاء العلاقة.

المادة الثالثة والأربعون: الاختبارات الأمنية

تجري الجمعية، بحسب المخاطر والإمكانات:

مراجعة الصلاحيات.

فحص الثغرات.

اختبار النسخ الاحتياطية.

اختبار الاستعادة.

اختبارات التصيد التوعوية.

مراجعة إعدادات الأنظمة.

اختبار خطة الاستجابة.

مراجعة أمن الموردين.

المادة الرابعة والأربعون: مراجعة النتائج

توثق نتائج الاختبارات والثغرات والملاحظات، وتحدد الأولوية والمسؤول والموعد، ولا تغلق الملاحظة

إلا بعد التحقق من المعالجة.



الفصل الرابع عشر: التقارير والرقابة

المادة الخامسة والأربعون: التقارير

يرفع مسؤول الأمن السيبراني تقارير دورية تتضمن:

حالة الأصول والأنظمة.

الحوادث والثغرات.

حالة التحديثات.

نتائج النسخ والاستعادة.

حالة الصلاحيات.

نتائج الاختبارات.

مستوى الوعي والتدريب.

مخاطر الموردين.

الإجراءات التصحيحية.

الاحتياجات والقرارات المطلوبة.

المادة السادسة والأربعون: مؤشرات الأداء

تشمل المؤشرات:

نسبة الأصول المسجلة.

نسبة الأنظمة المحدثة.

نسبة مراجعة الصلاحيات.

نسبة نجاح النسخ الاحتياطية.



زمن اكتشاف الحادث.

زمن احتواء الحادث.

عدد حوادث التصيد.

عدد الحوادث المتكررة.

نسبة العاملين المدربين.

نسبة إغلاق الثغرات الحرجة.

نسبة الموردين الذين خضعوا للتقييم الأمني.

نسبة نجاح اختبارات الاستعادة.

المادة السابعة والأربعون: المراجعة الداخلية

تراجع المراجعة الداخلية أو جهة مستقلة:

تطبيق السياسة.

صلاحيات الوصول.

سلامة السجلات.

النسخ الاحتياطية.

حوادث الأمن السيبراني.

عقود الموردين.

الالتزام بالتدريب والاختبارات.

الإجراءات التصحيحية.



الفصل الخامس عشر: المخالفات والأحكام الختامية

المادة الثامنة والأربعون: المخالفات

تعد من المخالفات:

مشاركة كلمات المرور.

استخدام حساب الغير.

تثبيت برامج غير معتمدة.

تعطيل الحماية أو التحديثات.

نقل البيانات إلى جهاز شخصي.

فتح أو تمرير رسائل مشبوهة دون إبلاغ.

إخفاء حادث أو ثغرة.

العبث بالأدلة.

منح طرف خارجي صلاحية دون اعتماد.

استخدام النظام لمصلحة شخصية أو نشاط غير مشروع.

عدم تسليم الأجهزة أو إلغاء الصلاحيات عند انتهاء العلاقة.

استخدام خدمة سحابية غير معتمدة.

المادة التاسعة والأربعون: الإجراءات التصحيحية

تتخذ الجمعية بحسب الحالة:

عزل النظام أو الحساب.

تغيير كلمات المرور.



سحب الصلاحيات.

استعادة البيانات.

فتح تحقيق.

إعادة التدريب.

تطبيق الجزاء الوظيفي أو التعاقد.

إبلاغ الجهات المختصة.

إصلاح الثغرة.

تحديث الأنظمة والسياسات.

متابعة الإغلاق وإعادة الاختبار.

المادة الخمسون: المراجعة والتعديل

تراجع السياسة سنوياً أو عند وقوع حادث جوهري أو تغير الأنظمة أو البنية التقنية أو المخاطر، ولا تعدل إلا بقرار من مجلس الإدارة.

المادة الحادية والخمسون: النفاذ

تسري هذه السياسة من تاريخ اعتمادها، ويلغى ما يتعارض معها من تعليمات سابقة، وتكون النسخة المحفوظة في سجل السياسات النسخة المرجعية المعتمدة.

النماذج والسجلات المرتبطة

سجل الأصول التقنية.

نموذج طلب إنشاء حساب.



نموذج طلب صلاحية.

سجل مراجعة الصلاحيات.

نموذج بلاغ حادث سيراني.

سجل الحوادث التقنية.

سجل التحديثات والثغرات.

سجل النسخ الاحتياطية.

نموذج اختبار الاستعادة.

نموذج تقييم أمن المورد.

نموذج اعتماد خدمة سحابية.

نموذج طلب تغيير تقني.

سجل التدريب والتوعية.

تقرير الأمن السيبراني الدوري.

نموذج إقرار استخدام الأنظمة.

نموذج بلاغ حادث سيراني

رقم الحادث:

تاريخ ووقت الاكتشاف:

اسم المبلغ وصفته:

الأصل أو النظام المتأثر:

نوع الحادث: تصيد / اختراق / فقد جهاز / تسرب بيانات / برمجية خبيثة / أخرى



وصف الحادث:

.....
.....

الإجراءات الفورية المتخذة:

.....

البيانات أو الخدمات المتأثرة:

.....

هل ما زال الحادث مستمرا؟ نعم / لا

هل توجد بيانات شخصية متأثرة؟ نعم / لا

هل تم عزل الجهاز أو الحساب؟ نعم / لا

الجهات التي تم إشعارها:

مستوى الحادث: منخفض / متوسط / عال / حرج

اسم مسؤول معالجة الحادث:

الإجراء التصحيحي:

تاريخ الإغلاق:

اعتماد مسؤول الأمن السيبراني:



سجل الاعتماد

اعتمد مجلس إدارة منظمة المستقبل لصناعة الكوادر البشرية هذه السياسة في اجتماعه الثاني المنعقد بتاريخ 1447/12/29هـ، الموافق 2026/06/15م، وقرر العمل بها من تاريخ اعتمادها.

