

سياسة الأمن السيبراني وإجراءات التعافي من الكوارث التقنية

الإصدار الثاني
٢٠٢٤ م / ١٤٤٦ هـ

معلومات السياسة أو الآلية

العنصر	البيان
العنوان	سياسة الأمن السيبراني وإجراءات التعافي من الكوارث التقنية
المسؤول عنها	إدارة التحول الرقمي
رمز السياسة	تقنية.س. ٠١
الإصدار	الثاني
تاريخ الإصدار	٢٠٢٦ م
معد السياسة	فريق عمل السياسات
مصدر الوثيقة	وثيقة تفاؤل
اعتماد السياسة	مجلس الإدارة في اجتماعه رقم (٢٥)

الفهرس

م	السياسة	الصفحة
١	الغرض والأهداف	٤
٢	نطاق العمل وقابلية التطبيق	٤
٣	مبادئ الأمن السيبراني	٥
٤	حوكمة الأمن السيبراني والأدوار والمسؤوليات	٥
٥	متطلبات الأمن السيبراني الأساسية	٦-٧
٦	سياسة إدارة الأزمات السيبرانية	٨
٧	خطة التعافي من الكوارث التقنية	٩
٨	صمود الأمن السيبراني في استمرارية الأعمال	١٠
٩	التقييم بعد الأزمة والحادث	١٠
١٠	مؤشرات الأداء والالتزام	١١
١١	السجلات والأدلة	١١
١٢	الالتزام بالسياسة	١١
١٣	الاستثناءات	١٢
١٤	المراجعة والتحديث	١٢
١٥	متطلبات التنفيذ الأولية بعد اعتماد السياسة	١٢

١. الغرض والأهداف

تهدف السياسة إلى وضع إطار مؤسسي لحماية المعلومات والأنظمة والخدمات الرقمية للجمعية من المخاطر السيبرانية، والمحافظة على سرية المعلومات وسلامتها وتوافرها، وتقليل أثر الحوادث والاضطرابات على أعمال الجمعية وخدماتها المقدمة للمستفيدين

وتشمل الأهداف ما يلي:

- حماية بيانات الموظفين و المستفيدين وبيانات الحالات والاستشارات وأي معلومات صحية أو اجتماعية أو مالية أو شخصية ذات حساسية
- حماية الأنظمة والتطبيقات والبنية التحتية والشبكات والبريد الإلكتروني والحسابات والأجهزة
- منع أو تقليل الوصول غير المصرح به، وتسريب البيانات، وفقدانها أو العبث بها أو تعطيلها
- ضمان استمرارية الخدمات الرقمية للجمعية عند وقوع حادث سيبراني أو كارثة تقنية
- تحديد آلية واضحة للاستجابة للأزمات السيبرانية واحتوائها والتعافي منها والتقييم بعد انتهائها
- رفع مستوى الوعي والمسؤولية لدى العاملين والمتطوعين والمتعاقدين والأطراف الخارجية
- الالتزام بالمتطلبات التشريعية والتنظيمية ذات العلاقة وبالضوابط الأمنية المعتمدة لدى الجمعية

٢. نطاق العمل وقابلية التطبيق

تطبق هذه السياسة على جميع الأصول المعلوماتية والتقنية التابعة للجمعية أو التي تتم إدارتها لصالحها، وعلى جميع الإدارات والموظفين والمتطوعين والمتعاقدين ومقدمي الخدمات والأطراف الخارجية عند تعاملهم مع أصول الجمعية أو بياناتها

ويشمل النطاق – بحسب ما ينطبق فعلياً على الجمعية – الأنظمة والتطبيقات والمنصات الإلكترونية، قواعد البيانات، أجهزة المستخدمين، الخوادم، الشبكات، البريد الإلكتروني، الخدمات السحابية، النسخ الاحتياطية، الهواتف والأجهزة اللوحية، المواقع الإلكترونية، وأي أجهزة أو خدمات تقنية أخرى

وتُعد هذه السياسة المظلة الرئيسية لسياسات وإجراءات الأمن السيبراني الأخرى، وتُربط بعمليات إدارة المخاطر، والموارد البشرية، والمشاريع، واستمرارية الأعمال، وإدارة الموردين .

٣. مبادئ الأمن السيبراني

- السرية: عدم إتاحة المعلومات إلا للأشخاص المخولين وبقدر الحاجة للعمل
- السلامة/التكامل: منع التعديل أو الحذف أو العبث غير المصرح به بالمعلومات
- التوافر: ضمان إتاحة الأنظمة والبيانات والخدمات الحرجة عند الحاجة
- أقل صلاحية: منح الحد الأدنى من الصلاحيات اللازمة لأداء المهام
- الدفاع متعدد الطبقات: عدم الاعتماد على وسيلة أمنية واحدة
- الاستعداد والتعافي: اعتبار التعافي واستمرارية الأعمال جزءاً من الأمن السيبراني وليس مرحلة لاحقة له
- حماية الخصوصية: التعامل مع البيانات الشخصية والصحية بأعلى مستوى مناسب من الحماية

٤. حوكمة الأمن السيبراني والأدوار والمسؤوليات

الجهة/الدور	أبرز المسؤوليات
مجلس الإدارة /صاحب الصلاحية	اعتماد السياسة، الإشراف على مستوى المخاطر، دعم الموارد وتشكيل لجنة أو آلية إشراف على الأمن السيبراني والأزمات عند الحاجة
المدير التنفيذي	متابعة تطبيق الضوابط، دعم استمرارية الأعمال، واعتماد القرارات التشغيلية اللازمة أثناء الأزمات وفق الصلاحيات
مسؤول تقنية المعلومات	إدارة برنامج الأمن السيبراني، تقييم المخاطر، متابعة الضوابط، إدارة الحوادث، النسخ الاحتياطية والتعافي، ورفع التقارير
مسؤول استمرارية الأعمال /من يكلفه المدير التنفيذي	ربط مخاطر الأمن السيبراني باستمرارية الأعمال، تحديد الخدمات الحرجة، وتنسيق خطط الاستمرارية والتعافي
الموارد البشرية	تطبيق متطلبات الأمن السيبراني المتعلقة بالعاملين، خاصة التوعية السرية، الصلاحيات، وإلغاء الوصول عند انتهاء العلاقة
رؤساء الإدارات	تحديد الأنظمة والبيانات الحرجة الخاصة بإداراتهم، الالتزام بالسياسة والإبلاغ عن الحوادث والمخاطر
الموظفون والمتطوعون	الالتزام بالسياسة، حماية الحسابات والأجهزة، عدم مشاركة كلمات المرور، والإبلاغ الفوري عن أي حادث أو اشتباه
الأطراف الخارجية	الالتزام بالمتطلبات الأمنية والتعاقدية، حماية بيانات الجمعية، والإبلاغ عن الحوادث التي تؤثر على خدمات الجمعية أو بياناتها

٥. متطلبات الأمن السيبراني الأساسية

(١) استراتيجية الأمن السيبراني

إعداد أهداف ومبادرات وخطط عمل للأمن السيبراني مرتبطة بأهداف الجمعية ومستوى المخاطر.

(٢) إدارة المخاطر السيبرانية

تحديد الأصول والتهديدات والثغرات وتقييم احتمالية وتأثير المخاطر ووضع خطط المعالجة ومتابعتها.

(٣) إدارة الأصول

إنشاء سجل محدث للأصول التقنية والمعلوماتية والأنظمة والخدمات السحابية والأجهزة، مع تحديد مالك كل أصل ودرجة حيويته.

(٤) إدارة الهويات والصلاحيات

تطبيق مبدأ أقل صلاحية، ومراجعة الصلاحيات دورياً، وإلغاء وصول من تنتهي علاقته بالجمعية، واستخدام المصادقة متعددة العوامل للأنظمة والحسابات الحساسة متى ما كان ذلك متاحاً.

(٥) حماية أجهزة المستخدمين والأنظمة

تحديث أنظمة التشغيل والبرامج، مكافحة البرمجيات الخبيثة، تأمين إعدادات الأجهزة، وتطبيق آليات حماية مناسبة.

(٦) أمن الشبكات

حماية الشبكات وأجهزة الاتصال، فصل الشبكات عند الحاجة، تأمين الوصول اللاسلكي، ومراقبة الاتصالات غير المعتادة.

(٧) حماية البريد الإلكتروني

تطبيق وسائل مكافحة التصيد والبرمجيات الخبيثة، وحماية الحسابات، والتوعية بالرسائل الاحتيالية.

(٨) حماية البيانات والمعلومات

تصنيف البيانات حسب حساسيتها، تقييد الوصول، حماية البيانات أثناء النقل والتخزين، ومنع مشاركة البيانات الحساسة عبر قنوات غير معتمدة.

(٩) التشفير

استخدام التشفير لحماية البيانات الحساسة متى ما كان مناسباً ومتاحاً وفق المتطلبات الأمنية والتنظيمية.

(١٠) النسخ الاحتياطي والاستعادة

تنفيذ نسخ احتياطي منتظمة للأنظمة والبيانات الحرجة، مع حماية النسخ من الحذف أو التعديل غير المصرح به، واختبار الاستعادة دورياً.

(١١) إدارة الثغرات والتحديثات

اكتشاف الثغرات التقنية وتقييمها ومعالجتها حسب مستوى الخطورة والأثر على أعمال الجمعية.

(١٢) اختبار الاختراق

إجراء اختبارات أمنية مناسبة ومتناسبة مع الأنظمة والخدمات، خاصة الأنظمة المكشوفة على الإنترنت، وفق خطة معتمدة.

(١٣) إدارة السجلات والمراقبة

تفعيل وتوثيق السجلات الأمنية للأنظمة المهمة ومراجعتها بما يساعد على اكتشاف الأنشطة غير المعتادة والاستجابة للحوادث.

(١٤) إدارة حوادث الأمن السيبراني

توفير آلية للإبلاغ عن الحوادث وتصنيفها واحتوائها والتحقيق فيها ومعالجتها واستعادة الخدمة وتوثيق الدروس المستفادة.

(١٥) الأمن المادي

حماية غرف الأجهزة والخوادم ومعدات الشبكات والنسخ الاحتياطية والمستندات الحساسة من الوصول أو الفقد أو السرقة أو التخريب.

(١٦) أمن تطبيقات الويب والمنصات

إدراج متطلبات الأمن في التصميم والتطوير والاختبار والتحديث، ومعالجة الثغرات الأمنية في التطبيقات.

(١٧) أمن الأجهزة المحمولة و BYOD

حماية الهواتف والأجهزة اللوحية وأجهزة العمل، وتقييد استخدام الأجهزة الشخصية للوصول إلى البيانات الحساسة وفق ضوابط معتمدة.

(١٨) الموارد البشرية والتوعية

توعية العاملين بالتصيد والهندسة الاجتماعية وحماية كلمات المرور والبيانات، وإدراج الالتزامات الأمنية عند بدء وانتهاء العلاقة الوظيفية.

(١٩) الأطراف الخارجية والحوسبة السحابية

تقييم المخاطر الأمنية للموردين ومقدمي الخدمات، وإدراج الالتزامات الأمنية وحماية البيانات والإبلاغ عن الحوادث في العقود متى كان ذلك مناسباً.

(٢٠) الالتزام والمراجعة والتدقيق

مراجعة الالتزام بالسياسة والضوابط وإجراء تقييمات دورية ومعالجة الملاحظات.

٦. سياسة إدارة الأزمات السيبرانية

تُعد إدارة الأزمات السيبرانية جزءاً إلزامياً من منظومة الأمن السيبراني في الجمعية، وتهدف إلى ضمان اتخاذ قرارات سريعة ومنظمة عند وقوع حادث قد يؤثر بصورة جوهريّة على خدمات الجمعية أو بيانات المستفيدين أو سمعتها أو التزاماتها.

(١) حالات تفعيل إدارة الأزمة

- تعطل نظام أو خدمة رقمية حرجية يؤثر على تقديم الخدمات أو العمليات الأساسية
- اشتباه أو ثبوت تسريب أو فقدان بيانات شخصية أو صحية أو مالية حساسة
- هجوم فدية أو برمجيات خبيثة واسع النطاق أو تشفير للبيانات
- اختراق حسابات ذات صلاحيات مرتفعة أو أنظمة حساسة
- تعطل واسع للشبكة أو الخوادم أو الخدمات السحابية بما يتجاوز قدرة المعالجة التشغيلية المعتادة
- أي حادث يهدد سلامة البيانات أو توافرها ويستلزم تنسيقاً إدارياً بين أكثر من جهة

(٢) فريق إدارة الأزمة

عند تفعيل الأزمة، يُشكل فريق استجابة مناسب لحجم الحادث، ويضم - بحسب الحالة - الإدارة التنفيذية، تقنية المعلومات ، ممثل الإدارة المتأثرة، الموارد البشرية ، والشؤون القانونية/الخصوصية إن وجدت، مع إشراك مزودي الخدمة عند الحاجة.

يتولى الفريق تحديد مستوى الأزمة، اعتماد أولويات الاحتواء والتعافي، تنظيم الاتصالات، توثيق القرارات، والتنسيق مع الجهات المختصة وفق المتطلبات النظامية والتعاقدية.

(٣) مراحل إدارة الأزمة

المرحلة	المتطلب
الاكتشاف والإبلاغ	استقبال البلاغ والتحقق الأولي وتحديد الأنظمة أو البيانات المتأثرة
التصنيف والتصعيد	تحديد شدة الحادث وأثره وتفعيل فريق الأزمة إذا تجاوز حدود المعالجة التشغيلية
الاحتواء	عزل الحسابات أو الأجهزة أو الأنظمة المتأثرة، مع المحافظة على الأدلة قدر الإمكان
المعالجة	إزالة سبب الحادث، معالجة الثغرة، وإعادة تهيئة الأنظمة عند الحاجة
التعافي	استعادة الأنظمة والبيانات من مصادر موثوقة، والتحقق من سلامتها قبل الإعادة الكاملة للخدمة
التواصل	إدارة الرسائل الداخلية والخارجية من خلال الجهة المخولة، وعدم مشاركة معلومات الحادث غير المصرح بها
ما بعد الأزمة	إجراء تقييم شامل، توثيق الدروس المستفادة، وتحديث الضوابط والخطط

٧. خطة التعافي من الكوارث التقنية (Technical Disaster Recovery)

تلتزم الجمعية بوجود خطة تعافٍ من الكوارث التقنية مرتبطة بهذه السياسة، ومراجعتها واختبارها دورياً. ويجب أن تحدد الخطة الأنظمة والخدمات الحرجة، وأولويات الاستعادة، ومسؤوليات التنفيذ، ومصادر النسخ الاحتياطية، وآليات الاستعادة البديلة.

(١) تصنيف أولوية الخدمات

الأولوية	أمثلة على الخدمات	الهدف المبدئي لزمن الاسترجاع RTO	الحد الأقصى المبدئي لفقد البيانات RPO
حرجة جداً	الخدمات الرقمية المرتبطة مباشرة بالمستفيدين أو البيانات الحساسة أو العمليات الأساسية	ساعات 4 ≤	ساعة 1 ≤
حرجة	البريد الإلكتروني، أنظمة الإدارة والتشغيل، الخدمات الداخلية المهمة	ساعات 8 ≤	ساعات 4 ≤
مهمة	أنظمة مساندة لا توقف الأعمال الأساسية فوراً	ساعة 24 ≤	ساعة 12 ≤
مساندة	الخدمات غير الحرجة أو التي يمكن تشغيلها يدوياً مؤقتاً	ساعة 72 ≤	ساعة 24 ≤

ملاحظة: القيم أعلاه مستهدفات مبدئية للسياسة، ويجب اعتماد القيم النهائية لكل نظام بعد إجراء تحليل أثر الأعمال (BIA) وتقييم المخاطر وقدرات البنية التقنية ومقدمي الخدمات.

(٢) متطلبات خطة التعافي

- تحديد مالك كل نظام وخدمة وبيانات ومسؤول التعافي
- تحديد RTO (زمن الاسترجاع المستهدف) و RPO (نقطة الاسترجاع المستهدفة) لكل نظام حرج.
- تحديد ترتيب استعادة الأنظمة بحيث تبدأ الخدمات الأعلى أولوية
- توفير نسخ احتياطية دورية واختبار استعادتها، ويفضل وجود نسخة منفصلة/معزولة عن البيئة التشغيلية حسب مستوى المخاطر
- تحديد بدائل تشغيل مؤقتة عند تعذر الأنظمة الرقمية، بما يتناسب مع طبيعة الخدمة
- تحديد وسائل الاتصال البديلة لفريق الأزمة في حال تعطل البريد أو الشبكة
- توثيق إجراءات الاستعادة خطوة بخطوة ومعلومات الاتصال بمقدمي الخدمات
- التحقق من سلامة البيانات والأنظمة قبل إعادة التشغيل الكامل
- توثيق زمن الاستعادة الفعلي ومقارنته بـ RTO، وتوثيق مقدار فقد البيانات الفعلي ومقارنته بـ RPO.
- اختبار الخطة دورياً وتوثيق نتائج الاختبار والإجراءات التصحيحية

٨. صمود الأمن السيبراني في استمرارية الأعمال

يجب أن تتضمن إدارة استمرارية الأعمال متطلبات صمود الأمن السيبراني، بحيث تستمر الجمعية في تقديم خدماتها الأساسية أو تعود إليها خلال فترة مقبولة عند حدوث اضطراب سيبراني أو تقني.

- تحديد الخدمات والعمليات التي لا يمكن للجمعية الاستغناء عنها، وتحديد الحد المقبول لتعطل كل منها
- تحديد الاعتماديات التقنية والبشرية والخارجية لكل خدمة حرجية
- توفير بدائل تشغيل مناسبة، بما في ذلك الإجراءات اليدوية المؤقتة عند الحاجة
- ربط نتائج تحليل أثر الاعمال (BIA) مع تصنيف الأنظمة والنسخ الاحتياطية و RTO/PRO
- اختبار سيناريوهات انقطاع الشبكة، تعطل الخادم، فقد البيانات، اختراق الحسابات، وهجوم الفدية
- التأكد من قدرة الموردين والخدمات السحابية المهمة على دعم التعافي واستمرارية الخدمة
- إعادة الأنظمة إلى وضع آمن قبل استعادة التشغيل الكامل، وليس مجرد إعادة الخدمة بسرعة

٩. التقييم بعد الأزمة والحادث

بعد انتهاء الأزمة أو الحادث السيبراني المؤثر، يجب تنفيذ مراجعة ما بعد الحادث خلال مدة مناسبة يحددها مستوى الحادث، بهدف معرفة السبب الجذري وقياس فعالية الاستجابة والتعافي ومنع تكرار الحادث.

محور التقييم	ما يجب قياسه/توثيقه
الاستجابة	وقت اكتشاف الحادث، وقت التبليغ، وقت التصعيد، ووقت بدء الاحتواء
الأثر	الخدمات المتأثرة، الأنظمة والبيانات المتأثرة، مدة الانقطاع، والأثر التشغيلي والمالي والسمعة عند انطباقه
التعافي	RTO المستهدف مقابل الفعلي RPO المستهدف مقابل الفعلي
السبب الجذري	الثغرة أو السبب الذي أدى إلى الحادث والعوامل التي سمحت باستمراره
فعالية الضوابط	ما الذي نجح وما الذي لم ينجح، ومدى كفاية النسخ الاحتياطية والمراقبة والاستجابة
الإجراءات التصحيحية	الإجراءات المطلوبة، مالك كل إجراء، الموعد المستهدف، وحالة التنفيذ
الدروس المستفادة	تحديث السياسة والخطط والإجراءات والتوعية بناءً على نتائج الحادث

١٠. مؤشرات الأداء والالتزام

تستخدم الجمعية مؤشرات مناسبة لقياس نضج وفعالية الأمن السيبراني والتعافي .

المؤشر	المستهدف/القياس
نسبة الأنظمة الحرجة المصنفة	١٠٠٪ من الأنظمة والخدمات التي تم تحديدها ضمن النطاق
نسبة نجاح اختبارات استعادة النسخ الاحتياطية	٩٥٪ ≤ ، مع معالجة أي فشل موثق
الالتزام بـ RTO	نسبة الأنظمة التي تم استعادتها ضمن RTO المعتمد
الالتزام بـ RPO	نسبة الأنظمة التي لم يتجاوز فقد بياناتها RPO المعتمد
زمن اكتشاف الحوادث الحرجة MTTD	قياس الاتجاه وتحسينه دورياً
زمن الاستجابة الأولية MTTA	قياس الاتجاه وتحسينه دورياً
زمن احتواء الحوادث MTTC	قياس الاتجاه وتحسينه دورياً
التوعية الأمنية	١٠٠٪ من العاملين المستهدفين سنوياً، وفق الخطة المعتمدة
مراجعة الصلاحيات	مراجعة دورية موثقة للحسابات والصلاحيات الحساسة
اختبارات التعافي والأزمات	اختبار دوري موثق للسيناريوهات الحرجة والإجراءات التصحيحية

١١. السجلات والأدلة

- سجل الأصول والأنظمة والخدمات الحرجة
- سجل المخاطر السيبرانية وخطط المعالجة
- سجلات الحوادث والاستجابة والأزمات
- سجلات النسخ الاحتياطي واختبارات الاستعادة
- نتائج اختبارات التعافي من الكوارث واختبارات استمرارية الأعمال
- تقارير التقييم بعد الحوادث وخطط الإجراءات التصحيحية
- سجلات التدريب والتوعية
- سجلات الصلاحيات والمراجعات والتدقيق

١٢. الالتزام بالسياسة

يلتزم جميع العاملين والمتطوعين والأطراف الخارجية ذات العلاقة بهذه السياسة وبالإجراءات والمعايير المنبثقة عنها. ويجوز اتخاذ إجراءات تصحيحية أو تأديبية وفق الأنظمة واللوائح الداخلية المعتمدة عند وقوع مخالفة.

ويتحمل مسؤول تقنية المعلومات مسؤولية المتابعة الدورية للالتزام ورفع الملاحظات والمخاطر إلى الإدارة المختصة.

١٣. الاستثناءات

لا يجوز تجاوز متطلبات هذه السياسة أو ضوابطها دون استثناء رسمي موثق ومعتمد من صاحب الصلاحية، بعد تقييم المخاطر ووضع الضوابط التعويضية المناسبة، وبما لا يتعارض مع المتطلبات التشريعية والتنظيمية ذات العلاقة
يجب أن يتضمن طلب الاستثناء: سبب الاستثناء، الأنظمة أو البيانات المتأثرة، مدة الاستثناء، المخاطر، الضوابط التعويضية، والجهة المعتمدة

١٤. المراجعة والتحديث

تراجع هذه السياسة مرة واحدة سنوياً على الأقل، وكذلك عند حدوث تغيير جوهري في الأنظمة أو الخدمات أو المتطلبات التنظيمية، أو بعد حادث سيرراني مؤثر أو اختبار تعافٍ يكشف عن فجوة جوهريّة
تتولى الجهة المسؤولة عن الأمن السيرراني توثيق التعديلات ورفع النسخة المحدثة للاعتماد

١٥. متطلبات التنفيذ الأولية بعد اعتماد السياسة

- حصر الأنظمة والخدمات والبيانات الحرجة للجمعية وتصنيفها .
- تنفيذ تحليل أثر الأعمال (BIA) واعتماد RTO\RPO لكل خدمة حرجة .
- إعداد واعتماد خطة إدارة الأزمات السيررانية وخطة التعافي من الكوارث التقنية .
- مراجعة النسخ الاحتياطية واختبار الاستعادة وتوثيق النتائج .
- تحديد فريق الأزمة ومسؤولياته وقنوات الاتصال البديلة .
- تنفيذ تمرين محاكاة لحادث سيرراني مؤثر مرة دورية مناسبة، وتوثيق التحسينات .
- اعتماد سجل مؤشرات الأمن السيرراني والتعافي ورفع تقرير دوري للإدارة .
- مراجعة العقود مع مزودي الخدمات التقنية والسحابية للتأكد من وجود متطلبات أمنية واستمرارية وإبلاغ عن الحوادث .

الاعتماد

الحمد لله والصلاة والسلام على رسول الله وبعد:

تم اعتماد مجلس الإدارة سياسة الأمن السيبراني وإجراءات التعافي من الكوارث التقنية في اجتماعهم (٢٥) بتاريخ ١٠ / ٩ / ٢٠٢٤م الدورة (٣) وقرروا العمل بموجبها ونشرها على الموقع الإلكتروني للجمعية وفق الصيغة المرفقة بالاعتماد.

رئيس مجلس الإدارة



محمد بن عبد العزيز الغفالق