NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

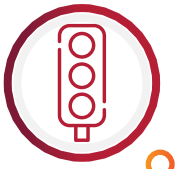
EG|CERT

سياسة تأمين النسح الاحتياطي للبيانات

(الاصدار الأول)

المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات

إشارة المشاركة: أبيض



بروتوكول الإشارة الضوئية
(TRAFFIC LIGHT PROTOCOL TLP)

يُستخدم بروتوكول الإشارة الضوئية **TLP** لتصنيف المعلومات وآلية مشاركة واستخدام هذه المعلومات، ويضم البروتوكول أربعة ألوان (إشارات ضوئية) تفصيلها كالتالي:

أحمر -شخصي وسري لمتلقيها فقط

لا يجوز لمتلقي المعلومات مشاركتها مع أي أطراف خارج منصة التبادل أو الاجتماع أو المحادثة التي تم الكشف عنها في الأصل.

برتقالي – مشاركة محدودة

يمكن لمتلقي المعلومات مشاركتها مع الأشخاص المعنيين داخل الجهة فقط، أو مع من تخصه المعلومات لاتخاذ الإجراء الملائم، أو مع الذين يحتاجون إلى معرفة المعلومات لحماية أنفسهم أو منع المزيد من الضرر.

أخضر – مشاركة في نفس الجهة

يمكن لمتلقي المعلومات مشاركتها داخل وخارج الجهة مع الأشخاص المعنيين، ولا يُسمح بنشرها أو تبادلها من خلال القنوات العامة.

أبيض – مشاركة غير محدودة

يمكن لمتلقي المعلومات مشاركتها دون أية قيود ومن خلال قنوات الاتصال.

الفهرس

تاريخ مراجعة السياسة

واضع هذه السياسة	التوصيف	الإصدار	التاريخ
المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات (EG-CERT)	تاريخ الإصدار	1.0	1/6/2022
المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات (EG-CERT)	تاريخ سريان هذه السياسة	1.0	
	تاريخ المراجعة		

التصديق على هذه السياسة

المُصدِّقون على هذه السياسة	التاريخ	الاسم	التوقيع
الإدارة العليا			
المديرون التنفيذيون			
مدير إدارة الدعم الأمني السيبرانى			
مدير إدارة تكنولوجيا المعلومات			
مدير إدارة التدقيق والمراجعة الداخلية			

١. نظرة عامة

تحدد هذه الوثيقة سياسة تأمين النسخ الاحتياطي للبيانات (Backup Policy) الخاصة بالمؤسسة والتي تساعد في التعامل مع المتطلبات الخاصة بالاحتفاظ بالبيانات وأمن المعلومات من أجل ضمان استعادة كافة المعلومات والبرامج الأساسية بعد وقوع حادث أو عطل أو فقد وسائط التخزين. لذا، كان لزامًا أن يتم وضع الخطط المطلوبة وتطبيقها مع توضيح كيفية القيام بإجراء نسخ احتياطي للمعلومات والأنظمة والبرامج.

١,١ الغرض:

قام المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات (EG-CERT) بوضع هذه السياسة والتي يمكن من خلالها استرداد البيانات أو اللأنظمة وعدم فقدها.

١,٢ نطاق هذه السياسة:

تُطبق هذه السياسة على كافة أصول وموارد تقنية المعلومات داخل المؤسسة. يتحمل جميع المتعاملين مع المؤسسة مسؤولية الالتزام بهذه السياسة

١,٣ التزام الإدارة:

قام مدير إدارة تكنولوجيا المعلومات ومدير إدارة الدعم الأمني السيبرانى بمراجعة هذه السياسة والموافقة عليها؛ وتدعم الإدارة العليا الغرض الذي تم وضعها من أجله. أي مخالفة لهذه السياسة قد يؤدي إلى اتخاذ إجراءات تأديبية ضد مرتكبها والتي قد تشمل إيقاف الموظف المخالف عن العمل، أو تقييد وصوله لبعض النُظم والمعلومات، أو توقيع عقوبة أشد عليه تشمل، على سبيل المثال لا الحصر، إنهاء خدمته.

١,٤ التوافق مع المعايير الدولية:

تم وضع هذه السياسة بناءً على المنشور الخاص (SP) رقم ٨٠٠-٥٣ الإصدار (٥) الصادر من المعهد الوطني للمعايير والتقنية (NIST) ومعيار آيزو ٢٧٠٠١ (ISO ٢٧٠٠١) وتتوافق هذه السياسة أيضًا مع أفضل الممارسات الخاصة بضوابط أمن المعلومات ٢٧٠٠٢ (ISO ٢٧٠٠٢).

٢. التعريفات

التوافر

يُقصد به إمكانية الوصول للمعلومات وإمكانية استخدامها عند طلب ذلك من قبل طرف مصرح له.

السلامة

يُقصد بها أن المعلومات والبيانات لم يتم تغييرها أو إتلافها بطريقة غير مصرح بها.

السرية

يُقصد بها أن المعلومات والبيانات لم يتم الكشف عنها أو إتاحتها لأشخاص أو مؤسسات غير مصرح لها أو عمليات غير مصرح بها.

الهدف من وقت الاسترداد (RTO)

يُقصد به إجمالي الفترة الزمنية التي تكون فيها مكونات نظام المعلومات في مرحلة الاسترداد (recovery phase) قبل أن يتم التأثير سلبًا على مهمة المؤسسة أو المهمة /

هدف نقطة الاسترداد (RPO)

يُقصد به الفترة الزمنية التي تحتاجها لاستعادة البيانات بعد انقطاع الخدمة أو التيار.

٣. المهام والمسؤوليات

الموظف المعني	المهام والمسؤوليات
الإدارة العليا	• الموافقة على هذه السياسة واعتمادها رسميًا. • اصدار التعليمات الادارية الملزمة لكافة العاملين بالمؤسسة بتطبيق السياسات وكذلك وضع لوائح الجزاءات الخاصة بعدم تطبيق هذه السياسات بما لا يتعارض مع اللوائح والقوانين.
المسؤولون التنفيذيون	• مراجعة هذه السياسة واعتمادها رسميًا.
فريق الدعم الأمني السيبرانى	• وضع الخطط والإجراءات والسياسات والتدابير بالتعاون مع إدارة تكنولوجيا المعلومات. • مراجعة هذه السياسة وتحديثها دوريًا. • تنفيذ ومراجعة الآليات اللازمة التى تدعم هذه السياسة. • الحفاظ على أمان الأنظمة وحماية البيانات. • ادارة ومتابعة وتحديث الأدوات الخاصة بالحفاظ على أمن الأنظمة والمعلومات. • التعاون مع فريق تكنولوجيا المعلومات وفريق المراجعة الداخلية لتأمين الأصول الرقمية الخاصة بالمؤسسة. • رفض أو الموافقة على أي استثناء لضوابط هذه السياسة
فريق الموارد البشرية	• التأكد من معرفة الموظفين بسياسات التأمين الخاصة بالمؤسسة . • تحديد المسئوليات الخاصة بأمن المعلومات وبنود السرية فى العقود.

الموظف المعني	المهام والمسؤوليات
فريق تكنولوجيا المعلومات	• التعاون مع فريق الدعم الأمني السيبرانى لإصدار الخطط والإجراءات والتدابير اللازمة لتنفيذ هذه السياسة. • إبلاغ جميع موظفي المؤسسة بمهامهم ومسؤولياتهم الأمنية قبل منحهم إمكانية الوصول إلى البيانات والنُظم الحساسة. • تنفيذ الآليات اللازمة التي يطلبها فريق الدعم الأمني السيبرانى.
فريق المراجعة الداخلية	• عمل مراجعة داخلية للضوابط الأمنية الخاصة بالسياسة • وكفاءتها. • تقييم وتعزيز جاهزية المؤسسة لأي هجمات سيبرانية. • تقييم وإدارة المخاطر. التأكد من التوافق مع السياسات والمعايير.
المديرون	• التأكد من أن الموظفين المعنيين ملمون بهذه السياسة.
الموظفون	• يجب على الموظفون تطبيق هذه السياسة والتصرف وفقًا لها.

٤. ضوابط سياسة النسخ الاحتياطي للبيانات (BACKUP SECURITY POLICY CONTROLS)

٤,١ خطة النسخ الاحتياطي للبيانات:

- يجب وضع خطة للنسخ الاحتياطي للبيانات، مع الأخذ في الاعتبار ما يلي:
- إنشاء سجلات دقيقة وشاملة للنسخ الاحتياطية وإجراءات موثقة لاستعادة البيانات.
- تحديد أهمية وحساسية المعلومات ونوع عملية النسخ الاحتياطي (مثل النسخ الاحتياطي الكامل (full backup) أو التفاضلي (differential backup)) الذي سيتم العمل به بانتظام.
- تخزين النسخ الاحتياطية في مكان مؤَمن جيدًا، يكون بعيدًا بشكلٍ كافٍ لتجنب حدوث أي ضرر أو تلف ناتج عن وقوع كارثة في الموقع الرئيسي.
- المحافظة على مستوى مناسب من الحماية المادية والبيئية لوسائط النسخ الاحتياطي وفقًا للمعايير المطبقة في الموقع الرئيسي.
- اختبار وسائط النسخ الاحتياطي بانتظام لضمان موثوقيتها ودرجة صلاحيتها للاستخدام في حالات الطوارئ عند الضرورة.
- إجراء اختبار للقدرة على استعادة البيانات -التي تم عمل نسخ احتياطية لها -إلى نظام الاختبار، شريطةً ألا يتم ذلك عن طريق الكتابة فوق وسائط التخزين الأصلية في حالة إخفاق عملية النسخ الاحتياطي أو الفشل في استعادة البيانات، مما يؤدي إلى وقوع تلف للبيانات غير قابل للإصلاح أو فقدها وعدم القدرة على استعادتها.
- تأمين النسخ الاحتياطية بالتشفير حسبما المخاطر التي تم رصدها.
- العناية اللازمة بعملية التحقق من عدم رصد أي فقد غير مقصود للبيانات قبل إجراء عملية النسخ الاحتياطي.
- تحديد فترة زمنية معينة للاحتفاظ بمعلومات العمل الأساسية مع مراعاة الحاجة للاحتفاظ بنسخ أرشيفية منها.
- مراعاة حذف المعلومات في وسائط التخزين المستخدمة في النسخ الاحتياطي بمجرد انتهاء فترة الاحتفاظ بالمعلومات. يجب أيضًا الالتزام بالتشريعات واللوائح المعمول بها في هذا الصدد.

٤,٢ النسخ الاحتياطي للنظام

- النسخ الاحتياطي للنظام:
- يجب أخذ نسخ احتياطية لمعلومات/وثائق المستخدم أو النظام (بما في ذلك الوثائق الخاصة بالخصوصية والأمان) والتي تم إدراجها في مكونات النظام المحددة بشكل متكرر ووفقًا للهدف من وقت الاسترداد (RTO) وهدف نقطة الاسترداد (RPO).
- يجب رصد ومراقبة عملية تنفيذ النسخ الاحتياطي للبيانات ومعالجة أي إخفاق في عملية النسخ
- الاحتياطي الموضوعة للتأكد من إتمامها.
- يجب تأمين سرية المعلومات التي تم عمل نسخ احتياطية منها وتوافرها وسلامتها.
- يتعين استخدام عينة من النسخ الاحتياطية في استعادة وظائف محددة للنظام كجزء من اختبار خطة الطوارئ.
- يجب أن يتم تخزين النسخ الاحتياطية من المعلومات في منشأة منفصلة وفقًا لضوابط مادية وبيئية مصممة خصيصًا لحماية وسائط التخزين الاحتياطية مثل أنظمة الكشف عن الحريق والحماية منه وإخماده، وأجهزة استشعار الحرارة والرطوبة لاكتشاف الحرائق وفرض قيود على الوصول المادي للأنظمة.
- يتعين نقل معلومات النسخ الاحتياطية للنظام إلى موقع التخزين الاحتياطي، بحيث تتوافق الفترة الزمنية المحددة ومعدلات النقل مع الهدف من وقت استرداد البيانات (RTO) والهدف من نقطة الاسترداد (RPO)، ويكون ذلك إما إلكترونيًا أو ماديًا من خلال الشحن الفعلي لوسائط التخزين.
- يجب أن يتم استخدام آليات التشفير لتجنب حدوث أي تعديل أو إفصاح غير مصرح به لمعلومات النسخ الاحتياطية المحددة.

٤,٣ خطة/اختبار الطوارئ

- يجب وضع خطة طوارئ للنظام يتم فيها تحديد ما يلي:
  - مهام العمل ووظائف التشغيل والأصول الهامة ومتطلبات الطوارئ ذات الصلة ومحددات وأولويات استعادة النظام.
  - المهام والمسؤوليات ذات الصلة والأفراد المعنيين ومعلومات الاتصال الخاصة بهم.
- يتعين ضمان استمرارية مهام العمل الأساسية بالرغم من حدوث أعطال في النظام أو انقطاع للخدمة.
- يجب استعادة الأنظمة والبيانات مع مراعاة الضوابط المعمول بها.
- يتعين تحديد إجراءات تبادل المعلومات المتعلقة بالطوارئ.
- يجب مراجعة الخطة بانتظام واعتمادها.
- يجب تقديم نسخ من الخطة لموظفي الطوارئ الرئيسيين المعنيين بالمؤسسة (يجب أن يتم تحديدهم بالاسم و/أو وفقًا للمهام المكلفين بها).
- يجب أن يتم تنسيق الجهود بين تنفيذ أنشطة التخطيط للطوارئ وتلك المتعلقة بالتعامل مع الحوادث.
- يجب أن يتم تحديث خطة الطوارئ للتعامل مع أي تغييرات تمت للأنظمة أو بيئة التشغيل وحتى يمكن معالجة أي مشكلات تطرأ خلال تطبيق خطة الطوارئ أو تنفيذها أو اختبارها.
- يجب إطلاع مسؤولي الطوارئ المعنيين بالمؤسسة (يجب أن يتم تحديدهم بالاسم و/أو وفقًا للمهام المكلفين بها) على أي تغييرات تم إدخالها على خطة الطوارئ.
- يتعين دمج الدروس المستفادة من أنشطة خطة الطوارئ الفعلية في الاختبارات والتدريب المتعلق بالطوارئ.
- يجب حماية هذه الخطة من أي تعديل أو إفصاح غير مصرح به عنها.
- يجب - عند وضع/اختبار خطة الطوارئ- التنسيق مع المعنيين بالمؤسسة المسؤولين عن خطط المؤسسة ذات الصلة مثل خطة التعافي من الكوارث (disaster recovery plan) وخطة استمرارية الأعمال (Business Continuity Plan) وما إلى ذلك.
- يجب تنفيذ الخطط الخاصة بتنمية الموارد البشرية والمهارات حتى يتم توفير الطاقة الإنتاجية والإمكانيات اللازمة لمعالجة المعلومات والاتصالات ودعم البيئة التشغيلية في كافة عمليات الطوارئ.
- يتعين اختبار خطة الطوارئ الخاصة بالنظام بانتظام وذلك باستخدام اختبارات محددة يتم من

٤,٤ الاستثناءات

يجب إبلاغ فريق الدعم الأمني بأي تغييرات مقترحة على النظام؛ أيضًا يتعين توثيق الموافقة على أي استثناء للضوابط والمواد الأساسية المنصوص عليها في هذه السياسة واعتمادها رسميًا من قبل مدير إدارة تكنولوجيا المعلومات. يجب أن يحدد أي استثناء ما يلي:

- طبيعة هذا الاستثناء.
- توضيح لضرورة الاستثناء.
- أي مخاطر ناتجة عن الاستثناء.
- ما يفيد موافقة مدير إدارة تكنولوجيا المعلومات على هذا الاستثناء