State of Libya
Government of National Unity
Ministry of Education

دولـــة لـــيبيـــا
حكومـــة الـــوحـــدة الـــوطنيـــة
وزارة الـــتربيـــــة والتعـليـــــم

السياسة الشاملة لأمن وسلامـــة المعلومـــات

رقم الوثيقة: م.م.ت-س.أ.م- 01-2025
الإصدار: 1.0

الفهـــــرس

الفهـــــرس

الباب الأول: الأحكام العامة

1.1 المقدمة:

انطلاقاً من الدور المحوري الذي يلعبه "مركز المعلومات والتوثيق" كجهة مسؤولة عن جمع وحماية ومعالجة بيانات قطاع التربية والتعليم، واستجابة للمتطلبات الوطنية للتحول الرقمي والسيبراني، تم وضع هذه السياسة لتكون الإطار الرسمي الملزم الذي يحكم جميع جوانب أمن وسلامة المعلومات في المركز.

1.2 الأساس القانوني والمرجعي:

تستند هذه السياسة إلى التشريعات والسياسات الوطنية التالية:

- قانون رقم (4) لسنة 1990م بشأن النظام الوطني للمعلومات والتوثيق.
- قرار مجلس الوزراء رقم (3) لسنة 2018م بشأن إنشاء مركز المعلومات والتوثيق بوزارة التربية والتعليم.
- قرار وزير التربية والتعليم رقم (117) لسنة 2022م بشأن اعتماد التنظيم الداخلي لمركز المعلومات والتوثيق.
- السياسات الوطنية لأمن وسلامة المعلومات الصادرة عن الهيئة الوطنية لأمن وسلامة المعلومات (NISSA).
- السياسة الوطنية لحوكمة البيانات الحكومية والدليل الوطني للبيانات الحكومية الصادرين عن الهيئة العامة للمعلومات (GIA).
- السياسة الوطنية للنفاذية الرقمية.
- الاستراتيجية الوطنية للتحول الرقمي الحكومي.

1.3 الغاية والأهداف:

تهدف هذه السياسة إلى تحقيق مجموعة من الأهداف الاستراتيجية المترابطة:

- حماية الأصول المعلوماتية: وضع ضوابط صارمة لحماية بيانات وزارة التربية التعليم من كافة المخاطر والتهديدات الداخلية والخارجية.
- ضمان الامتثال: ضمان توافق إجراءات المركز مع الإطار الوطني لأمن المعلومات والتشريعات ذات الصلة.
- تعزيز الثقة والمصداقية: بناء الثقة لدى كافة الأطراف المعنية في قدرة الوزارة على حماية البيانات.
- تحقيق مبادئ أمن المعلومات الأساسية: ضمان سرية وسلامة وتوافر (Confidentiality, Integrity, Availability) جميع أصول المعلومات.

1.4. نطاق التطبيق:

تسري أحكام هذه السياسة على جميع العاملين بمركز المعلومات والتوثيق (دائمين ومتعاقدين)، والأطراف الثالثة، وكافة أصول المعلومات والأنظمة والشبكات والمرافق التابعة للمركز.

الباب الثاني: حوكمة أمن المعلومات

2.1. الهيكل التنظيمي والمسؤوليات:

استجابة مباشرة لتوصيات تقرير التدقيق، يتم اعتماد الهيكل التنظيمي والمسؤوليات التالية:

الدور	المسؤوليات الرئيسية
مدير عام مركز المعلومات والتوثيق	المسؤولية النهائية عن تطبيق هذه السياسة وتوفير الموارد اللازمة لها.
قسم الصيانة والدعم الفني وقسم الأمن السيبراني (قيد الإنشاء)	-تنفيذ الضوابط التقنية والإدارية للأمن السيبراني. -إدارة أنظمة الحماية (الجدران النارية، مكافحة الفيروسات). -مراقبة الشبكات والأنظمة للكشف عن التهديدات. -إعداد تقارير دورية عن الوضع الأمني.
فريق الاستجابة للحوادث (CSIRT) (قيد التشكيل)	-التعامل الفوري مع الحوادث الأمنية عند وقوعها وفقاً لخطة موثقة. -تحليل الحوادث وتقديم توصيات لمنع تكرارها.
فريق حوكمة البيانات (وفق الدليل الوطني)	-**رئيس الفريق:** قيادة جهود حوكمة البيانات ووضع الاستراتيجيات. -**مدير البيانات:** الإشراف على التنفيذ، مراجعة تصنيف البيانات وضمان جودتها. -**مهندس البيانات:** تنفيذ المهام التقنية مثل تصنيف البيانات وإضافة البيانات الوصفية.
جميع الموظفين والمتعاقدين	-الالتزام بجميع بنود هذه السياسة. -توقيع "إقرار وتعهّد بالالتزام بسياسة أمن وسلامة المعلومات". -الإبلاغ الفوري عن أي حوادث أمنية مشتبه بها.

الباب الثالث: إدارة الأصول وتصنيف البيانات

3.1. إدارة الأصول:

- **جرد الأصول:** يجب على قسم الصيانة والدعم بإدارة تكنولوجيا المعلومات الحفاظ على قائمة جرد محدثة ودقيقة لجميع الأصول التقنية (أجهزة، برمجيات، شبكات)، مع تحديد مسؤول مباشر عن كل أصل.
- **ملكية الأصول:** جميع الأصول المعلوماتية والتقنية التي يوفرها المركز هي ملك للدولة، ومخصصة لأغراض العمل الرسمية.

لضمان تطبيق سياسة إدارة الأصول بفعالية، يجب على قسم الصيانة والدعم اتباع الإجراءات المحددة التالية:

3.1.1. إجراءات جرد الأصول:

1. إنشاء سجل جرد الأصول المركزي:

- المسؤولية: يقع على عاتق قسم الصيانة والدعم إنشاء وإدارة سجل مركزي لجميع الأصول التقنية والمعلوماتية.
- الأداة: يتم استخدام قاعدة بيانات مخصصة أو برنامج متخصص لإدارة الأصول لضمان الدقة وسهولة التحديث.
- الحد الأدنى من الحقول المطلوبة لكل أصل في السجل:

1. معرّف الأصل الفريد (Asset ID): رقم تسلسلي فريد لا يتكرر.
2. نوع الأصل: (مثال: حاسوب محمول، خادم، طابعة، برنامج، قاعدة بيانات).
3. وصف الأصل: (مثال: Dell Latitude 7420, Microsoft Office, 2021 License).
4. الرقم التسلسلي للمصنّع: (Serial Number) إن وجد.
5. الموقع المادي: مثال: (مكتب رقم 15، غرفة الخوادم).
6. المالك المسؤول: (Owner) اسم الموظف أو القسم المسؤول عن الأصل.
7. تاريخ الاقتناء: تاريخ شراء أو استلام الأصل.
8. حالة الأصل: (مثال: في الخدمة، صيانة، خارج الخدمة).
9. تصنيف البيانات التي يحتويها (للأصول التي تخزن البيانات): سري، داخلي، عام.

2. دورة حياة الأصل:

- عند إضافة أصل جديد: يقوم قسم الصيانة والدعم بتسجيل الأصل فوراً في سجل الجرد، ووضع ملصق مادي عليه يحمل "معرّف الأصل الفريد"، وإسناده إلى المالك المسؤول.
- عند نقل أو تغيير المسؤولية: يتم تحديث حقل "الموقع المادي" و "المالك المسؤول" في سجل الجرد فوراً.

- المراجعة الدورية: يتم إجراء تدقيق مادي على جميع الأصول المسجلة ومطابقتها مع السجل مرة واحدة سنوياً على الأقل للتحقق من دقة البيانات.
- عند إخراج الأصل من الخدمة: يتم الحصول على موافقة رسمية، ويتم التأكد من مسح جميع البيانات بشكل آمن وفقاً لسياسة الإتلاف (البند 3.3)، ثم يتم تحديث حالة الأصل في السجل إلى "خارج الخدمة".

3.1.2. إجراءات ملكية الأصول:

- يتم تحديد "مالك مسؤول" لكل أصل معلوماتي وتقني عند تسجيله في سجل الجرد.
- المالك المسؤول هو المسؤول المباشر عن حماية الأصل من التلف أو الفقدان وضمان استخدامه وفقاً لسياسة الاستخدام المقبول.

3.2. سياسة تصنيف البيانات:

يتم تصنيف جميع بيانات المركز وفقاً للسياسة الوطنية لحوكمة البيانات الحكومية لضمان تطبيق المستوى المناسب من الحماية:

مستوى التصنيف	الوصف	أمثلة (قطاع التعليم)	متطلبات التعامل الأساسية
سري / مقيد	بيانات عالية الحساسية، الكشف عنها يسبب ضرراً كبيراً.	السجلات الشخصية والطبية للطلاب والموظفين، نتائج الامتحانات قبل إعلانها، التحقيقات الإدارية، كلمات المرور.	**تشفير إلزامي** عند التخزين والنقل، وصول مقيد جداً على أساس "الحاجة للمعرفة"، مراقبة مشددة للوصول.
داخلي / حساس	بيانات مخصصة للاستخدام الداخلي فقط.	محاضر الاجتماعات الداخلية، المراسلات الإدارية التي لم تعمم، بيانات الميزانية التشغيلية للمركز.	تخزين على خوادم داخلية مؤمنة، يُمنع مشاركتها خارجياً إلا بموافقة رسمية، لا تتطلب تشفيراً قوياً ولكن تتطلب حماية للوصول.
عام / غير مقيد	بيانات يمكن الكشف عنها للعامة دون قيود.	النشرات الصحفية، التقويم الدراسي العام، التقارير السنوية المنشورة، معلومات الاتصال العامة بالوزارة.	يمكن نشرها على الموقع الرسمي للمركز والوزارة، مع ضرورة التأكد من سلامتها وعدم التلاعب بها.

3.2.1. إجراءات تصنيف البيانات:

لتحويل سياسة التصنيف إلى ممارسة عملية، يجب اتباع الخطوات الإجرائية التالية المعتمدة في السياسة الوطنية لحوكمة البيانات الحكومية:

1. المسؤولية عن التصنيف:

- المُنشئ: الموظف الذي يقوم بإنشاء الوثيقة أو البيانات هو المسؤول عن تحديد التصنيف المبدئي لها في لحظة الإنشاء.
- مالك البيانات/مدير البيانات: يقوم بمراجعة التصنيف المبدئي واعتماده أو تعديله لضمان دقته.

2. عملية التصنيف خطوة بخطوة:

- الخطوة الأولى: تحديد البيانات عند الإنشاء: (عند إنشاء أي وثيقة، بريد إلكتروني، أو مجموعة بيانات جديدة، يجب على الموظف أن يتوقف ويسأل: "ما هي طبيعة هذه المعلومات؟").
- الخطوة الثانية: تقييم الأثر: يجب على الموظف تقييم الأثر المحتمل في حال تم الكشف عن هذه البيانات بشكل غير مصرح به.
- هل سيؤدي الكشف عنها إلى ضرر كبير بالوزارة أو الطلاب أو الموظفين؟ إذا كانت الإجابة نعم، يتم تصنيفها "سري / مقيد".
- هل هذه المعلومات مخصصة للتداول داخل الوزارة فقط ومشاركتها خارجياً قد تسبب إحراجاً أو ضرراً محدوداً؟ إذا كانت الإجابة نعم، يتم تصنيفها "داخلي / حساس".
- هل هذه المعلومات معدة للنشر العام ولا يترتب على كشفها أي ضرر؟ إذا كانت الإجابة نعم، يتم تصنيفها "عام / غير مقيد".
- الخطوة الثالثة: وضع العلامات (Labeling) : بعد تحديد مستوى التصنيف، يجب وضع علامة واضحة على الأصل المعلوماتي:
- للوثائق الإلكترونية (Word, PDF) : يجب إضافة علامة مائية أو نص واضح في رأس وتذييل كل صفحة (Header/Footer) يشير إلى مستوى التصنيف (مثال: "سري"، "داخلي للاستخدام الرسمي فقط").
- للبريد الإلكتروني: يجب إضافة وسم التصنيف في بداية عنوان البريد (مثال: [سري] أو [داخلي]).
- للوثائق الورقية: يجب استخدام أختام واضحة بالألوان المناسبة (مثال: ختم أحمر لكلمة "سري") على كل صفحة من الوثيقة.

3. مراجعة التصنيف:

- يقوم مدير البيانات بإجراء مراجعات دورية على عينات من البيانات للتأكد من تطبيق سياسة التصنيف بشكل صحيح ومتسق.

3.3. سياسة الاحتفاظ بالسجلات وإتلافها:

يتم تحديد مدد الاحتفاظ بالسجلات لضمان الامتثال للقوانين، مع ضمان إتلافها بشكل آمن عند انتهاء الحاجة إليها. يجب إتلاف الوثائق الورقية باستخدام آلات فرم، والوسائط الإلكترونية عبر المسح الآمن أو التدمير المادي.

3.3.1. إدارة جدول الاحتفاظ:

- المسؤولية: يقوم فريق حوكمة البيانات بالتعاون مع إدارة التوثيق والأرشفة والشؤون القانونية بإنشاء ومراجعة "جدول مدد الاحتفاظ بالسجلات" سنوياً.
- الإجراء: يحدد الجدول كل نوع من السجلات في المركز (أكاديمية، مالية، إدارية) والمدة القانونية والتشغيلية للاحتفاظ بها.

3.3.2. إجراءات الإتلاف الآمن:

1. تحديد السجلات المنتهية: يقوم مسؤول القسم المعني بتحديد السجلات التي تجاوزت مدة الاحتفاظ المحددة في الجدول.
2. طلب الإتلاف: يتم تقديم طلب رسمي إلى مدير البيانات أو القسم المختص للموافقة على عملية الإتلاف.
3. تنفيذ الإتلاف:

- السجلات الورقية: يتم إتلافها باستخدام آلات الفرم بالقطع المتقاطع (Cross-cut Shredders) لضمان استحالة إعادة تجميعها.
- الوسائط الإلكترونية (أقراص صلبة، ذاكرة فلاش):
  - إذا كان سيُعاد استخدامها: يتم مسح البيانات باستخدام برامج مسح آمن معتمدة (Secure Wipe) تضمن عدم إمكانية استرجاع البيانات.
  - إذا كانت ستُرمى: يتم تدميرها مادياً (بالثقب، الصعق الكهرومغناطيسي، أو التكسير) لضمان إتلافها بالكامل.

4. توثيق الإتلاف: يتم تسجيل عملية الإتلاف في "سجل إتلاف السجلات"، والذي يوضح تاريخ الإتلاف، ووصف للسجلات التي تم إتلافها، واسم الموظف المسؤول، واسم الشاهد (إن وجد)، ويتم الاحتفاظ بهذا السجل بشكل دائم.

الباب الرابع: سياسات الوصول والتحكم

لضمـان تطبيق سياسـات الوصول بشـكل فعال وآمـن، يتم اتباع الإجـراءات والتعليمات المحددة التالية لكل سياسة فرعية.

4.1. إجراءات تطبيق مبدأ الامتياز الأقل (Principle of Least Privilege):

- الهدف: ضمان أن كل مستخدم يمتلك الحد الأدنى من الصلاحيات اللازمة لأداء مهامه الوظيفية فقط، لمنع الوصول غير المصرح به للبيانات والأنظمة.
- الإجراءات:

1. إجراءات طلب الوصول (Access Request):

- المسؤولية: الموظف الذي يحتاج إلى صلاحيات وصول جديدة أو إضافية.
- الخطوات:

1. يقـوم الموظـف بملء "نمـوذج طلب صلاحيـات وصول" رسـمي، يوضح فيه المـوارد المطلوبـة (مثـال: الوصول إلى مجلـد مشترك معين، اسـتخدام تطبيق محدد) مع تبرير واضح للحاجة الوظيفية.
2. يتم إرسال النموذج إلى المدير المباشر للموظف للمراجعة والموافقة المبدئية.

2. إجراءات الموافقة على الوصول (Access Approval):

- المسؤولية: المدير المباشر، مالك الأصل المعلوماتي، إدارة تكنولوجيا المعلومات.
- الخطوات:

1. يقـوم المديـر المباشر بمراجعـة الطلب والتأكد مـن أن الصلاحيـات المطلوبة ضرورية لأداء مهام الموظف، ثم يوقع بالموافقة.
2. يتم تحويل الطلب الموافق عليه إلى "مالك الأصل المعلوماتي (Owner)" (مثال: رئيس قسم الشؤون المالية إذا كان الطلب يخص النظام المالي).
3. بعد موافقة مالك الأصل، يتم إرسـال الطلب إلى قسـم الصيانة والدعم لمنح الصلاحيات تقنياً.

3. إجراءات المراجعة الدورية للصلاحيات (Access Review):

- المسؤولية: قسم الصيانة والدعم بالتعاون مع مديري الأقسام.
- الخطوات:

1. يقوم قسم الصيانة والدعم بشكل سنوي (أو نصف سنوي للأنظمة الحساسة) بتزويـد كل مديـر قسـم بقائمـة بأسـماء الموظـفين التابـعين لـه والصلاحيات الممنوحة لهم على الأنظمة.
2. يقوم مدير القسم بمراجعة القائمة والتأكد من أن كل موظف لا يزال بحاجة إلى الصلاحيات الممنوحة له.
3. يتـم التوقيـع على القائمة وإعادتها إلى قسـم الصيانة والدعـم مع تحديد أي صلاحيات يجب إلغاؤها أو تعديلها.

4. إجراءات إلغاء الوصول (Access Revocation):

- المسؤولية: قسم الموارد البشرية، قسم الصيانة والدعم.
- الخطوات:

1. عند انتقال موظف إلى قسم آخر أو انتهاء خدمته، يقوم قسم الموارد البشرية بإبلاغ قسم الصيانة والدعم فوراً عبر إشعار رسمي.
2. يقوم قسم الصيانة والدعم بإلغاء جميع صلاحيات وحسابات الموظف في نفس يوم العمل الذي تم فيه استلام الإشعار.

4.2. إجراءات تطبيق سياسة كلمة المرور:

- الهدف: فرض استخدام كلمات مرور قوية ومعقدة كخط دفاع أساسي لحماية الحسابات والأنظمة.
- الإجراءات:

1. الإجراءات التقنية (مسؤولية قسم الصيانة والدعم):

- فرض السياسة مركزياً: تم تطبيق متطلبات تعقيد كلمة المرور (الطول، التنوع، التغيير الدوري، سجل كلمات المرور السابقة) بشكل إلزامي على جميع حسابات المستخدمين من خلال سياسات المجموعة (Group Policy) في نظام إدارة الدليل (Active Directory).
- ضبط قفل الحساب: يتم تفعيل خاصية قفل الحساب تلقائياً لمدة 15 دقيقة بعد 5 محاولات دخول فاشلة.

2. تعليمات للمستخدمين:

- عند إنشاء كلمة مرور جديدة يجب عليك التأكد من أنها تفي بالمتطلبات التالية:
- لا تقل عن 12 حرفاً.
- تحتوي على ثلاثة أنواع من الرموز على الأقل: حروف كبيرة (A-Z)، حروف صغيرة (a-z)، أرقام (0-9)، ورموز خاصة (! @#$) .
- لا تحتوي على معلومات شخصية: مثل اسمك، تاريخ ميلادك، أو أرقام هواتف.
- عند استلام كلمة مرور أولية (مؤقتة): يجب عليك تغييرها فوراً عند أول تسجيل دخول.
- حماية كلمة المرور: أنت مسؤول مسؤولية كاملة عن سرية كلمة المرور الخاصة بك، يُمنع كتابتها أو مشاركتها مع أي شخص، بما في ذلك موظفو الدعم الفني.

4.3. إجراءات تطبيق سياسة الوصول عن بعد (Remote Access):

- الهدف: تأمين اتصالات الموظفين بشبكة المركز من خارج المقر الرسمي لضمان سرية وسلامة البيانات المنقولة.
- الإجراءات:

1. طلب الحصول على صلاحية الوصول عن بعد:

- يجب على الموظف تقديم طلب رسمي عبر "نموذج طلب صلاحيات وصول عن بعد"، موضحاً سبب الحاجة.
- يخضع الطلب لنفس دورة الموافقات المذكورة في البند (4.1.2).

2. متطلبات الأجهزة المتصلة عن بعد:

- الأجهزة المملوكة للمركز: يجب أن يكون الجهاز مزوداً ببرنامج مكافحة فيروسات محدث، وآخر التحديثات الأمنية لنظام التشغيل.
- الأجهزة الشخصية (إن سُمح باستخدامها): بالإضافة إلى المتطلبات السابقة، يجب أن يتم فحص الجهاز من قبل قسم الصيانة والدعم للتأكد من خلوه من البرمجيات الخبيثة قبل منحه صلاحية الوصول.

3. إجراءات الاتصال:

- الاتصال عبر VPN : يتم تزويد الموظف المصرح له ببرنامج الشبكة الافتراضية الخاصة (VPN) مع بيانات الدخول. يُمنع منعاً باتاً محاولة الوصول إلى موارد الشبكة الداخلية دون تفعيل اتصال الـ VPN.
- المصادقة ثنائية العوامل (2FA) : بعد إدخال اسم المستخدم وكلمة المرور، سيُطلب من الموظف إدخال رمز متغير يتم إرساله إلى هاتفه المسجل أو يتم إنشاؤه عبر تطبيق مصادقة. هذا الإجراء إلزامي لجميع اتصالات الوصول عن بعد.
- مسؤولية المستخدم: أثناء الاتصال عن بعد، يجب على الموظف التأكد من أن جهازه في مكان آمن ومنع أي شخص غير مصرح له من استخدامه أو الاطلاع على شاشته.

4.4. سياسة استخدام البريد الإلكتروني:

- الهدف: ضمان استخدام البريد الإلكتروني الرسمي بطريقة آمنة ومهنية تخدم أغراض العمل وتحمي أصول المركز.
- الإجراءات:
- البريد الإلكتروني الرسمي مخصص حصراً للأعمال الوظيفية.
- يُمنع استخدام البريد الرسمي لأغراض شخصية أو للتسجيل في منصات خارجية غير متعلقة بالعمل.
- يجب توخي أقصى درجات الحذر من فتح الرسائل أو المرفقات من مصادر مجهولة أو غير موثوق بها.

- جميـع المراسلات التي تتم عبر البريد الإلكتروني الرسـمي تعـتبر ملكية للوزارة وتخضع للتدقيق عند الحاجة وفقاً للوائح المعمول بها.

4.5. سياسة استخدام الإنترنت:

- الهدف: تنظيم استخدام شبكة الإنترنت لضمان توجيه الموارد لأغراض العمل وحماية الشبكة من التهديدات الخارجية.
- الإجراءات:
- استخدام الإنترنت عبر شبكة المركز يجب أن يكون لأغراض العمل فقط.
- يُمنـع الدخـول إلى مواقـع غير قانونية، أو مشـبوهة، أو غير مرتبطـة بمهام العمل الوظيفية.
- يُمنـع منعاً باتاً تحميل أو تثبيت أي برامج أو أدوات غير معتمدة ومصرح بها من قبل الإدارة الفنية (قسم الصيانة والدعم).

4.6. سياسة أمان محطات العمل (أجهزة الكمبيوتر):

- الهـدف: تأمين أجهـزة الكمبيوتر المكتبيـة والمحمولة لمنع الوصـول غير المصرح به وحماية البيانات المخزنة عليها.
- الإجراءات:
- يجب على جميع الموظفين قفل أجهزتهم (بالضغط على Win + L في أنظمة ويندوز) عند مغادرتها ولو لفترة وجيزة، وعدم تركها دون حماية.
- يُمنع تثبيت أي برامج أو توصيل أجهزة خارجية (مثل طابعات شـخصية، أجهزة شبكة) دون الحصول على إذن مسبق وموافقة رسمية من إدارة تكنولوجيا المعلومات.
- يُمنع استخدام أجهزة المركز لأغراض شخصية قد تعرض الجهاز وبيانات المركز للخطر.

الباب الخامس: الأمن التقني والسيبراني

لضمـان تطبيق سياسـات الأمن التقني بشـكل فعـال، يتم اتبـاع الإجـراءات والتعليمات المحددة التالية لكل سياسة فرعية.

5.1. إجراءات حماية الشبكات:

5.1.1. إجراءات إدارة الجدران النارية (Firewalls) :

- الهـدف: التحكـم في حركـة مـرور البيانـات بين شـبكة المركـز والشـبكات الخارجية (مثل الإنترنت) لمنع الوصول غير المصرح به.
- الإجراءات:

1. إدارة قواعد الجدار الناري:

- يتـم تقديـم جميع طلبات إضافـة أو تعديل قواعد الجدار النـاري عبر "نموذج طلب تغيير قاعدة جدار ناري" رسمي.
- يجـب أن تتـم الموافقة على الطلب من قبل مدير قسـم الأمن السـيبراني قبل التنفيذ.
- يتم مراجعة جميع قواعد الجدار الناري بشكل نصف سنوي لإزالة أي قواعد لم تعد هناك حاجة إليها.

2. تطبيق قاعدة "الرفض الافتراضي" (Default Deny):

- يجـب أن تكون القاعـدة الأخيرة في أي قائمة قواعد للجـدار الناري هي قاعدة ترفض جميع أنواع حركة المرور التي لم يتم السماح بها صراحةً (Deny All).

3. تطبيق قاعدة "الرفض الافتراضي" (Default Deny):

- يجـب تفعيـل خاصية تسـجيل (Logging) لجميـع حركة المرور المسـموح بها والمرفوضة.
- يقوم قسـم الأمن السيبراني بمراجعة سجلات الجدار الناري بانتظام للكشف عن أي محاولات وصول مشبوهة.

5.1.2. إجراءات الحماية من البرمجيات الخبيثة:

- الهدف: حماية جميع أجهزة المركز من الفيروسـات، برامج الفدية، برامج التجسـس، وغيرها من البرمجيات الخبيثة.
- الإجراءات:

1. التثبيت والإدارة المركزية:

- يتـم تثبيت برنامـج مكافحة فيروسـات معتمد ومرخص من قبل قسـم تقنية المعلومات على جميع الخوادم وأجهزة الكمبيوتر في المركز.
- تتـم إدارة جميـع برامـج مكافحـة الفيروسـات مـن خلال وحدة تحكـم مركزية (Central Management Console) لضمـان تطبيـق السياسـات وتلقـي التحديثات بشكل موحد.

2. ضبط الإعدادات الإلزامي:

- يجب تفعيل خاصية "الحماية في الوقت الحقيقي" (Real-time Protection) على جميع الأجهزة.
- يجب ضبط البرنامج للتحقق من وجود تحديثات جديدة للتواقيع (Signatures) كل ساعة على الأقل.
- يتم جدولة فحص كامل للنظام (Full System Scan) ليتم إجراؤه أسبوعياً خارج ساعات العمل الرسمية.

3. مسؤوليات المستخدم:

- يُمنع منعاً باتاً على أي موظف تعطيل أو إزالة برنامج مكافحة الفيروسات.
- عند استلام أي تنبيه من برنامج مكافحة الفيروسات، يجب على الموظف إبلاغ قسم الأمن السيبراني فوراً.

5.2. إجراءات إدارة الثغرات والتحديثات (Vulnerability & Patch Management):

- الهدف: اكتشاف ومعالجة الثغرات الأمنية في الأنظمة والتطبيقات بشكل استباقي لمنع استغلالها من قبل المهاجمين.
- الإجراءات:

1. الفحص الدوري للثغرات:

- يقوم قسم الأمن السيبراني بإجراء فحص شامل للثغرات على جميع الخوادم والأنظمة المتصلة بالشبكة بشكل ربع سنوي على الأقل.

2. تقييم وتصنيف الثغرات:

- يتم تقييم الثغرات المكتشفة وتصنيفها حسب درجة خطورتها (حرجة، عالية، متوسطة، منخفضة) باستخدام معيار CVSS (Common Vulnerability Scoring System).

3. تطبيق التصحيحات الأمنية (Patching):

- يتم وضع جدول زمني إلزامي لتطبيق التحديثات الأمنية بناءً على درجة الخطورة:
  - الثغرات الحرجة (Critical): يتم تطبيق التحديث خلال 14 يوماً من اكتشافها.
  - الثغرات العالية (High): يتم تطبيق التحديث خلال 30 يوماً.
  - الثغرات المتوسطة (Medium): يتم تطبيق التحديث خلال 90 يوماً.
- يجب اختبار جميع التحديثات الأمنية على بيئة اختبار (Test Environment) قبل تطبيقها على الأنظمة الإنتاجية لضمان عدم تأثيرها سلباً على العمل.

4. التوثيق:
- يتم توثيق جميع نتائج الفحص والإجراءات المتخذة لمعالجة الثغرات في "سجل إدارة الثغرات".

5.3. إجراءات التشفير (Cryptography):

- الهـدف: حماية سرية البيانات الحساسـة وجعلها غير قابلة للقـراءة في حال تسربها أو سرقتها.
- الإجراءات:

1. تشفير البيانات أثناء النقل (Data-in-Transit):
- يجـب اسـتخدام بروتوكـول (HTTPS TLS 1.2) أو أعلى لتـأمين جميـع المواقع والخدمات الإلكترونية التي يقدمها المركز.
- يجـب اسـتخدام بروتوكولات آمنة مثـل SFTP لنقل الملفـات التي تحتوي على بيانات "سرية".
- يجب أن تكون جميع اتصالات الوصول عن بعد مؤمنة عبر VPN مشفر.

2. تشفير البيانات عند التخزين (Data-at-Rest):
- يجـب تفعيـل خاصيـة تشـفير القـرص الكامـل (Full Disk Encryption)، مثل BitLocker، على جميع أجهزة الكمبيوتر المحمولة الخاصة بالموظفين.
- يجب تشـفير قواعد البيانات والخـوادم التي تحتوي على بيانات مصنفة "سرية" باستخدام تقنيات مثل TDE (Transparent Data Encryption).

3. إدارة مفاتيح التشفير:
- يتـم تخزيـن مفاتيح التشـفير بشـكل آمـن ومنفصل عـن البيانـات التي تقوم بتشفيرها.
- يقـتصر الوصـول إلى مفاتيح التشـفير على عدد محدود جداً مـن الموظفين المصرح لهم في قسم الأمن السيبراني.

5.4. إجراءات النسخ الاحتياطي والاستعادة:

- الهـدف: ضمان القدرة على اسـتعادة البيانات والأنظمـة الحيوية بسرعة وفعالية في حالات الطوارئ.
- الإجراءات:

1. جدولة النسخ الاحتياطي:

- يتم إجراء نسخ احتياطي تزايدي (Incremental) للبيانات الحيوية بشكل يومي.
- يتم إجراء نسخ احتياطي كامل (Full) لجميع الأنظمة الحيوية بشكل أسبوعي.

2. تخزين النسخ الاحتياطية:

- يتم تشفير جميع وسائط النسخ الاحتياطي.
- يتم الاحتفاظ بنسخة احتياطية واحدة على الأقل في موقع جغرافي آمن.

3. اختبار الاستعادة (Restore Test):

- يقـوم قسـمي الصيانة والدعم ونظم المعلومات بإجـراء اختبار كامل لعملية استعادة البيانات من النسخ الاحتياطية مرة كل ستة أشهر على الأقل.
- يجـب أن يشـمل الاختبار اسـتعادة خـادم كامل وعينة عشـوائية مـن ملفات المستخدمين إلى بيئة اختبار معزولة.
- يتـم توثيق نتائج الاختبار (نجاح/فشـل، الوقت المسـتغرق) في "سـجل اختبارات الاستعادة" ورفع تقرير بذلك إلى مدير عام المركز.

الباب السادس: الأمن المادي والبيئي

لضمـان تطبيق سياسـات الأمن المادي والبيئي بفعالية، يتم اتبـاع الإجراءات والتعليمات المحددة التالية لكل سياسة فرعية.

6.1. إجراءات التحكم بالوصول المادي:

- الهدف: منع الوصول المادي غير المصرح به إلى المرافق والمعدات والمعلومات لحمايتها من السرقة والتلف والتخريب.
- الإجراءات:

1. تحديد المناطق الحساسة:

- المسـؤولية: مديـر عام المركز بالتعاون مع قسـمي الصيانـة والدعم والأمن السيبراني.
- الإجراء: يتم تحديد وتوثيق جميع المناطق الحساسـة في المركز، والتي تشـمل كحد أدنى:
  - غرفة الخوادم الرئيسية (Data Center).
  - غرفة معدات الشبكة والاتصالات.
  - مكاتب إدارة تكنولوجيا المعلومات.
  - إدارة التوثيـق والأرشـفة (غرفـة الأرشـيف التي تحتـوي على سـجلات ورقية حساسة).
- يتـم وضـع لافتات واضحـة عند مداخل هـذه المناطق تفيـد بأنها "منطقة محظورة - الدخول للمصرح لهم فقط".

2. إجراءات وصول الموظفين المصرح لهم:

- المسؤولية: قسم الأمن السيبراني.
- الخطوات:

1. يتـم إنشـاء "قائمة وصول مصرح بـه" لكل منطقة حساسـة، يتم اعتمادها من مدير عام المركز.
2. يتـم اسـتخدام نظام تحكـم بالوصـول الإلـكتروني (مثل بطاقـات الدخول أو القياسات الحيوية) لجميع المناطق الحساسة.
3. يتـم برمجة بطاقات الدخول لتسـمح بالوصول فقـط للموظفين المدرجين في قائمة الوصول الخاصة بالمنطقة.
4. يتـم مراجعـة "قائمـة الوصـول الـمصرح به" بشـكل نصف سـنوي لإلغاء أي صلاحيات لم يعد لها حاجة.

3. إجراءات وصول الزوار والأطراف الثالثة:

- المسؤولية: موظفو قسم الخدمات العامة، الموظف المستضيف.
- الخطوات:

1. التسجيل: يجب على جميع الزوار تسجيل بياناتهم (الاسم، الجهة، وقت الدخول، اسم الموظف المستضيف) في "سجل الزوار" لدى مكتب الاستقبال عند المدخل الرئيسي.
2. التحقق من الهوية: يقوم موظف الاستقبال بالتحقق من هوية الزائر من خلال بطاقة هوية رسمية.
3. إصدار بطاقة زائر: يتم منح الزائر بطاقة "زائر" مؤقتة يجب أن تبقى ظاهرة طوال فترة تواجده.
4. المرافقة الإلزامية: يجب على الموظف المستضيف مرافقة الزائر في جميع الأوقات. يُمنع منعاً باتاً ترك أي زائر بمفرده داخل أي منطقة حساسة.
5. تسجيل الخروج: عند المغادرة، يقوم الزائر بتسجيل وقت الخروج في السجل وإعادة بطاقة الزائر لمكتب الاستقبال.

4. المراقبة والتوثيق:

- كاميرات المراقبة (CCTV): يتم تركيب كاميرات مراقبة عند جميع المداخل الخارجية للمركز ومداخل المناطق الحساسة، ويتم الاحتفاظ بالتسجيلات لمدة لا تقل عن 90 يوماً.
- سجلات الدخول الإلكترونية: يتم الاحتفاظ بجميع سجلات الدخول (الناجحة والفاشلة) من نظام التحكم بالوصول الإلكتروني ومراجعتها دورياً من قبل قسم الأمن السيبراني.

6.2. إجراءات حماية المعدات والبيئة التشغيلية:

- الهدف: ضمان استمرارية عمل المعدات الحيوية وحمايتها من المخاطر البيئية والطبيعية.
- الإجراءات:

1. ضبط البيئة التشغيلية لغرفة الخوادم:

- المسؤولية: قسم الصيانة والدعم.
- الخطوات:

1. التبريد (Cooling) : يتم الحفاظ على درجة حرارة غرفة الخوادم في نطاق 18-24 درجة مئوية ورطوبة نسبية بين 40% و 60%.
2. المراقبة: يتم تركيب حساسات بيئية لمراقبة درجة الحرارة والرطوبة بشكل مستمر، مع إعداد نظام تنبيهات يقوم بإرسال إشعارات فورية إلى فريق الصيانة والدعم في حال تجاوز النطاقات المسموح بها.
3. الصيانة: يتم إجراء صيانة وقائية دورية (ربع سنوية على الأقل) لأنظمة التكييف والتبريد.

2. حماية إمدادات الطاقة (Power Protection):

- المسؤولية: قسم الصيانة والدعم.
- الخطوات:

1. الطاقة غير المنقطعة (UPS) : يجب توصيل جميع الخوادم ومعدات الشبكة الحيوية بوحدات UPS لضمان عدم انقطاع الخدمة في حال انقطاع التيار الكهربائي الرئيسي.
2. المولد الاحتياطي: يجب التأكد من وجود مولد كهربائي احتياطي قادر على تشغيل جميع الأنظمة الحيوية، مع إجراء فحص تشغيلي له أسبوعياً والتأكد من وجود كمية وقود كافية.
3. الصيانة والاختبار: يتم إجراء اختبار شهري لوحدات الـ UPS وصيانة دورية للمولد الاحتياطي.

3. الوقاية من الحرائق (Fire Suppression):

- المسؤولية: قسم الصيانة والدعم بالتعاون مع قسم الخدمات العامة.
- الخطوات:

1. أنظمة الإطفاء: يتم تزويد غرفة الخوادم بنظام إطفاء حريق يعتمد على الغاز النظيف (Clean Agent, e.g., FM-200) بدلاً من أنظمة الرش المائي التي قد تتلف المعدات.
2. أجهزة الكشف: يتم تركيب أجهزة كشف الدخان والحرارة في غرفة الخوادم وربطها بنظام إنذار مركزي.
3. الصيانة: يتم إجراء فحص وصيانة معتمدة لأنظمة الكشف والإطفاء بشكل نصف سنوي.
4. طفايات الحريق اليدوية: يتم توفير طفايات حريق يدوية من نوع ثاني أكسيد الكربون (CO_2) مناسبة للمعدات الإلكترونية بالقرب من مداخل غرفة الخوادم والمكاتب بالمركز.

الباب السابع: إدارة الحوادث واستمرارية العمل

لضمـان اسـتجابة فعالـة ومنظمـة للحـوادث الأمنيـة والكـوارث، يتـم اتبـاع الإجراءات والتعليمات المحددة التالية:

7.1. إجراءات خطة الاستجابة للحوادث (Incident Response Plan):

- الهـدف: توفير إطار عمل منهجي وموحد للكشـف عن الحـوادث الأمنية، احتوائها، القضاء عليها، والتعافي منها بأسرع وقت ممكن لتقليل الأضرار.
- الإجراءات:

1. تطوير وصيانة الخطة:

- المسـؤولية: يقوم قسـم الأمن السـيبراني بإعداد وتحديث "خطة الاسـتجابة للحوادث" بشكل سنوي.
- المصادقة: يتم اعتماد الخطة رسمياً من قبل مدير عام المركز.
- التوزيع: يتم توزيع نسخة محدثة من الخطة على جميع أعضاء فريق الاستجابة للحوادث (CSIRT).

2. آلية الإبلاغ عن الحوادث:

- قنوات الإبلاغ: يتم إنشـاء قنوات واضحة ومتاحة لجميع الموظفين للإبلاغ عن أي نشاط أمني مشبوه، وتشمل:
  - بريد إلكتروني مخصص: Support@moe.gov.ly
  - خط هاتف مباشر للدعم الفني.
- مسـؤولية الموظف: يجـب على أي موظف يلاحظ حادثـة أمنية محتملة (مثل رسـالة بريد إلكتروني احتيالية، سـلوك غريب في جهازه) أن يقوم بإبلاغ قسم الأمن السيبراني فوراً ودون تأخير.

3. دورة حياة الاستجابة للحادث (Incident Response Lifecycle):

- يقوم فريق الاسـتجابة للحوادث (CSIRT) باتباع المراحل التالية عند التعامل مع أي حادثة أمنية موثقة:
  - **المرحلة الأولى:** الكشف والتحليل (Detection & Analysis):
    1. استلام البلاغ من الموظف أو من أنظمة المراقبة الأمنية.
    2. التحقق من صحة البلاغ وتحديد ما إذا كان يمثل حادثة أمنية حقيقية.
    3. تصنيف الحادثة وتحديد مستوى خطورتها وتأثيرها المحتمل على العمل.

- **المرحلة الثانية: الاحتواء (Containment):**
4. اتخاذ إجراءات فورية لمنع انتشار الحادثة وتقليل الضرر.
5. أمثلة: فصل الجهاز المصاب عن الشبكة، حظر عنوان IP مشبوه على الجدار الناري، تعطيل حساب مستخدم تم اختراقه مؤقتاً.

- **المرحلة الثالثة: الاستئصال (Eradication):**
6. تحديد السبب الجذري للحادثة.
7. إزالة جميع مكونات التهديد من الأنظمة المتأثرة (مثل حذف البرمجيات الخبيثة، إزالة ملفات المخترقين).

- **المرحلة الرابعة: التعافي (Recovery):**
8. استعادة الأنظمة المتضررة إلى حالتها التشغيلية الطبيعية من نسخ احتياطية سليمة.
9. مراقبة الأنظمة المستعادة للتأكد من عدم عودة التهديد.
10. إعادة تفعيل الحسابات والخدمات بعد التأكد من أمانها.

- **المرحلة الخامسة: الدروس المستفادة (Lessons Learned):**
11. في غضون أسبوعين من إغلاق الحادثة، يعقد فريق CSIRT اجتماعاً لمراجعة الحادثة.
12. يتم إعداد "تقرير ما بعد الحادثة" يوثق تفاصيل الحادثة، الإجراءات المتخذة، وما يمكن تحسينه في المستقبل.
13. يتم تحديث خطة الاستجابة بناءً على الدروس المستفادة.

4. اختبار الخطة:
- المسؤولية: قسم الأمن السيبراني.
- الإجراء: يتم إجراء اختبار واحد على الأقل لخطة الاستجابة للحوادث سنوياً (مثل محاكاة هجوم تصيد احتيالي) لتقييم جاهزية الفريق وفعالية الإجراءات.

7.2. إجراءات خطة التعافي من الكوارث واستمرارية الأعمال (BCDR Plan):

- الهدف: ضمان قدرة المركز على استعادة أنظمته وعملياته الحيوية في حالة وقوع كارثة (مثل حريق، انقطاع طويل للتيار الكهربائي) ومواصلة تقديم الخدمات الأساسية.
- الإجراءات:

1. تطوير وصيانة الخطة:
- المسؤولية: يقوم فريق مكون من قسم الصيانة والدعم وقسم نظم المعلومات وقسم الأمن السيبراني بإعداد وتحديث "خطة التعافي من الكوارث واستمرارية الأعمال" بشكل سنوي.

- المصادقة: يتم اعتماد الخطة رسمياً من قبل مدير عام المركز.

2. مكونات الخطة الرئيسية:

- تحليل تأثير الأعمال (Business Impact Analysis - BIA):
  1. تحديد جميع العمليات والأنظمة الحيوية للمركز (مثال: نظام بيانات التعليم، نظام الأرشفة الالكترونية، نظام البريد الإلكتروني).
  2. تحديد هدف وقت التعافي (RTO - Recovery Time Objective) لكل نظام، وهو أقصى مدة زمنية يمكن للعمل أن يتحملها لتوقف هذا النظام.
  3. تحديد هدف نقطة التعافي (RPO - Recovery Point Objective) لكل نظام، وهو أقصى حجم للبيانات يمكن للمركز تحمل فقدانه.
- تقييم المخاطر (Risk Assessment): تحديد الكوارث المحتملة وتقييم احتمالية حدوثها وتأثيرها.
- استراتيجيات التعافي: بناءً على تحليل تأثير الأعمال، يتم تحديد استراتيجيات التعافي، مثل الاعتماد على النسخ الاحتياطية خارج الموقع (Off-site) لاستعادة الأنظمة.
- توثيق إجراءات التعافي: يجب أن تحتوي الخطة على:
  1. قوائم الاتصال بفريق التعافي من الكوارث.
  2. إجراءات خطوة بخطوة لاستعادة كل نظام حيوي، مرتبة حسب الأولوية.
  3. إجراءات تفعيل موقع العمل البديل (إن وجد).

3. اختبار الخطة:

- المسؤولية: قسم الصيانة والدعم.
- الإجراء: يتم إجراء اختبار واحد على الأقل لخطة التعافي من الكوارث سنوياً.
- يتضمن الاختبار محاكاة لسيناريو كارثة واستعادة نظام حيوي واحد على الأقل في بيئة معزولة.
- يتم توثيق نتائج الاختبار في تقرير رسمي وتقديمه لمدير عام المركز لمناقشة أي تحسينات مطلوبة.

الباب الثامن: الالتزام والمراجعة

8.1. إجراءات التوعية والتدريب:

- الهـدف: بناء ثقافة أمنية راسـخة لدى جميع الموظفين وتقليـل المخاطر الناتجة عن الخطأ البشري.
- الإجراءات:

1. برنامج التدريب الإلزامي للموظفين الجدد:

- المسـؤولية: قسـم التدريب بإدارة الدراسـات والتخطيط بالتنسـيق مع قسم شؤون الموظفين وقسم الأمن السيبراني.
- الخطوات:

1. كجـزء من إجراءات التعيين، يقوم قسـم التدريـب بجدولة الموظف الجديد لحضور برنامج التوعية الأمنية الإلزامي.
2. يجب على الموظف الجديد إكمال هذا التدريب خلال أول 30 يوماً من تاريخ مباشرته للعمل.
3. بعد إتمام التدريب، يقوم الموظف بتوقيع "إقرار وتعهّد بالالتزام بسياسـة أمن وسلامة المعلومات"، ويتم حفظ نسـخة مـن الإقرار في ملفه الوظيفي، ونسخة في ملف الأمن السيبراني.

2. برنامج التدريب السنوي الدوري:

- المسؤولية: قسم الأمن السيبراني.
- الخطوات:

1. يقوم قسـم الأمن السيبراني سنوياً بتحديث محتوى برنامج التوعية ليشمل أحدث التهديدات السـيبرانية (مثل أساليب التصيد الاحتيالي الجديدة) وتذكير الموظفين بالسياسات الرئيسية.
2. يتـم الإعلان عن جدول التدريب السـنوي وإلزام جميع الموظفين بحضوره وإكماله قبل نهاية الربع الأول من كل عام.
3. يتـم متابعة سـجلات الحضور ورفع تقرير بأسـماء المتخلفين إلى مدير عام المركز لاتخاذ الإجراء اللازم.

3. حملات التوعية المستمرة:

- المسؤولية: قسم الأمن السيبراني.
- الإجـراء: بالإضافة إلى التدريب الرسـمي، يقوم قسـم الأمن السـيبراني بتنفيذ أنشطة توعية مستمرة، وتشمل:

1. إرسال نشرات بريدية دورية تحتوي على نصائح أمنية.
2. إجراء حملات محاكاة للتصيد الاحتيالي (Phishing Simulation) بشـكل ربع سـنوي لتقييم مسـتوى وعي الموظفين وتدريبهم على اكتشـاف الرسـائل الخبيثة.

8.2. إجراءات التدقيق والمراجعة:

- الهدف: التحقق من مدى الالتزام بالسياسة بشكل مستمر، والتأكد من أن السياسة تظل مواكبة للمتغيرات والمخاطر.
- الإجراءات:

1. إجراءات مراجعة وتحديث السياسة:

- المسؤولية: إدارة تكنولوجيا المعلومات.
- التوقيت: تتم مراجعة هذه السياسة بشكل سنوي، أو فور حدوث تغييرات جوهرية (مثل تبني تقنيات جديدة أو وقوع حادثة أمنية كبيرة).
- الخطوات:

1. يقوم فريق من إدارة تكنولوجيا المعلومات مشكل من جميع الأقسام بمراجعة بنود السياسة ومقارنتها مع أحدث المعايير والتهديدات.
2. يتم إعداد مسودة بالتعديلات المقترحة وتقديمها لمدير عام المركز للموافقة.
3. بعد الاعتماد، يتم إصدار نسخة جديدة من السياسة برقم إصدار وتاريخ جديدين، وتعميمها على جميع الموظفين.

2. إجراءات التدقيق الداخلي:

- المسؤولية: يتم تكليف جهة داخلية مستقلة (مثل إدارة الدراسات والتخطيط أو فريق يتم تشكيله خصيصاً) للقيام بالتدقيق.
- التوقيت: يتم إجراء تدقيق داخلي على ضوابط أمن المعلومات مرة واحدة سنوياً.
- الخطوات:

1. يقوم فريق التدقيق بفحص عينة من الضوابط المطبقة (مثال: مراجعة سجلات الوصول، التحقق من تطبيق سياسة كلمة المرور، فحص سجلات تحديث الأنظمة).
2. يتم إعداد "تقرير تدقيق داخلي" مفصل يوضح نقاط القوة وأي حالات عدم امتثال (Findings).
3. يتم رفع التقرير إلى مدير عام المركز، مع وضع خطة عمل تصحيحية لمعالجة نقاط الضعف المكتشفة.

8.3. إجراءات الإقرار بالالتزام:

- الهدف: الحصول على توثيق رسمي يفيد بأن جميع الأفراد الذين يتعاملون مع أصول المركز قد قرأوا وفهموا والتزموا بالسياسة الأمنية.
- الإجراءات:

1. للموظفين الجدد:

- المسؤولية: قسم الصيانة والدعم بالتعاون مع قسم شؤون الموظفين.
- الإجراء: يتم تسليم "إقرار وتعهّد" للموظف الجديد ليقوم بتوقيعه بعد إكماله للتدريب الأمني الإلزامي. يتم حفظ الأصل في ملفه الوظيفي.

2. للموظفين الحاليين:

- المسؤولية: قسم الصيانة والدعم بالتعاون مع قسم شؤون الموظفين.
- الإجـراء: يتم تعميم "إقرار وتعهّد" على جميع الموظفين الحاليين لتوقيعه عند إصـدار أي تحديـث جوهري على السياسـة، أو بشـكل دوري كل سـنتين لتجديد الالتزام.

3. للأطراف الخارجية (المقاولون، الموردون، الاستشاريون):

- المسؤولية: الإدارة المسؤولة عن التعاقد.
- الإجراء: يجب أن يكون توقيع "إقرار وتعهّد" جزءاً إلزامياً من إجراءات التعاقد قبل منح أي طرف خارجي وصولاً إلى شـبكة أو بيانات المركز. يتم الاحتفاظ بالنسـخة الموقعة مع وثائق العقد.

تمت المصادقة عليه من قبل:

مدير عام مركز المعلومات والتوثيق

التوقيع: .....

التاريـــخ: .....

مركز المعلومات والتوثيق

Information Documentation Center

dic@moe.gov.ly