



سياسة إدارة المخاطر واستمرارية الأعمال





الفصل الأول: الأحكام العامة

المادة الأولى: التمهيد

تدرك الجمعية أن تحقيق أهدافها واستدامة خدماتها يتطلبان إدارة منهجية للمخاطر، والاستعداد للاضطرابات والحوادث التي قد تؤثر في العاملين والمستفيدين والأصول والبيانات والعمليات والسمعة. وتضع هذه السياسة إطاراً متكاملًا لتحديد المخاطر وتقييمها ومعالجتها ومراقبتها، وضمان استمرارية الأعمال والتعافي من الانقطاعات.

المادة الثانية: الهدف

تهدف هذه السياسة إلى:

إنشاء إطار موحد لإدارة المخاطر.

تحديد المخاطر التي قد تعيق تحقيق أهداف الجمعية.

تقييم احتمالية المخاطر وآثارها.

تحديد شهية المخاطر وحدود تحملها.

تعيين مالك لكل خطر وخطة لمعالجته.

حماية المستفيدين والعاملين والمتطوعين والأصول.

المحافظة على استمرارية الخدمات والعمليات الحيوية.

تقليل مدة الانقطاع والخسائر الناتجة عنه.

دعم اتخاذ القرارات بناء على معلومات موثوقة.

تعزيز الالتزام والرقابة والجاهزية المؤسسية.

تنظيم الاستجابة للحوادث والأزمات والتعافي منها.





توفير تقارير دورية لمجلس الإدارة والإدارة التنفيذية.

المادة الثالثة: نطاق التطبيق

تطبق هذه السياسة على:
الجمعية العمومية في حدود اختصاصها.
مجلس الإدارة واللجان.
المسؤول التنفيذي.
جميع الإدارات والبرامج والمشروعات.
العاملين والمتطوعين والمتدربين.
الفروع والمكاتب والمواقع التابعة للجمعية.
الشركاء والمنفذين والموردين الرئيسيين.
الأنظمة والتطبيقات وقواعد البيانات.
الأصول المالية والمادية والفكرية.
جميع العمليات والخدمات والالتزامات التعاقدية.

المادة الرابعة: المرجعيات

تستند هذه السياسة إلى:
اللائحة الأساسية للجمعية.
نظام الجمعيات والمؤسسات الأهلية ولائحته التنفيذية.
قواعد وتعليمات المركز الوطني لتنمية القطاع غير الربحي.



الأنظمة والتعليمات المتعلقة بالسلامة والأمن السيبراني وحماية البيانات.

لائحة الحوكمة.

اللائحة المالية.

سياسة الرقابة الداخلية والمراجعة.

سياسة الأمن السيبراني.

سياسة حماية البيانات والخصوصية.

سياسة إدارة الأزمات والطوارئ.

سياسة استمرارية الأعمال والتعافي.

سياسة إدارة العقود والاتفاقيات.

سياسة مكافحة غسل الأموال وتمويل الإرهاب.

أي متطلبات نظامية أو تعاقدية واجبة التطبيق.

المادة الخامسة: التعريفات

الخطر: حدث أو ظرف غير مؤكد قد يؤثر سلباً أو إيجاباً في تحقيق أهداف الجمعية.

إدارة المخاطر: الأنشطة المنظمة لتحديد المخاطر وتحليلها وتقييمها ومعالجتها ومراقبتها.

الخطر الكامن: مستوى الخطر قبل تطبيق الضوابط.

الخطر المتبقي: مستوى الخطر بعد تطبيق الضوابط.

احتمالية الخطر: مدى توقع وقوع الخطر.

أثر الخطر: حجم النتائج المترتبة على وقوعه.

شهية المخاطر: مقدار ونوع المخاطر الذي تقبل الجمعية تحمله لتحقيق أهدافها.





حد التحمل: الحد الأقصى المقبول للانحراف أو الخسارة أو التعطل.

مالك الخطر: الشخص المسؤول عن إدارة خطر محدد ومتابعة خطته.

الضابط: إجراء وقائي أو كاشف أو تصحيحي يحد من احتمال الخطر أو أثره.

سجل المخاطر: السجل المركزي الذي يوثق المخاطر وتقييمها وضوابطها وخططها.

العملية الحيوية: عملية يؤدي توقفها إلى أثر جوهري في المستفيدين أو الالتزام أو الأعمال.

استمرارية الأعمال: قدرة الجمعية على مواصلة تقديم الخدمات والعمليات ذات الأولوية أثناء الاضطراب وبعده.

تحليل أثر الأعمال: عملية تحديد العمليات الحيوية وآثار توقفها واحتياجات تعافيها.

الحد الأقصى المقبول للتوقف: أطول مدة يمكن أن تتوقف خلالها العملية قبل أن يصبح أثر الانقطاع غير مقبول.

الوقت المستهدف للتعافي: المدة المستهدفة لاستعادة العملية أو النظام بعد الانقطاع.

نقطة الاستعادة المستهدفة: الحد الأقصى المقبول لفقد البيانات مقاسا بالوقت.

الحادث: واقعة تسببت أو قد تتسبب في تعطيل أو خسارة أو ضرر.

الأزمة: حدث جسيم يتطلب قيادة وتنسيقا وقرارات استثنائية.

الفصل الثاني: مبادئ إدارة المخاطر

المادة السادسة: المبادئ العامة

تلتزم الجمعية في إدارة المخاطر بما يأتي:

ربط إدارة المخاطر بالأهداف والخطط والميزانية.

إدماج تقييم المخاطر في القرارات والمشروعات والعقود.



حماية حياة وسلامة الأشخاص كأولوية أولى.

اتخاذ قرارات متناسبة مع طبيعة الخطر.

تحديد واضح لملكية المخاطر والمسؤوليات.

الاعتماد على معلومات موثوقة ومحدثة.

الاستباقية وعدم انتظار وقوع الخطر.

توثيق التقييمات والقرارات والاستثناءات.

التعلم من الحوادث والملاحظات.

التحسين المستمر للضوابط والخطط.

الفصل بين ملكية الخطر والمراجعة المستقلة.

مراعاة ترابط المخاطر وتأثير بعضها في بعض.

المادة السابعة: فئات المخاطر

تشمل المخاطر التي تديرها الجمعية، دون حصر:

المخاطر الاستراتيجية.

مخاطر الحوكمة والقيادة.

المخاطر المالية والسيولة.

مخاطر التبرعات والمنح والاستثمار.

المخاطر التشغيلية.

مخاطر البرامج والمشروعات.

مخاطر الموارد البشرية والمتطوعين.





مخاطر المستفيدين والحماية والسلامة.

مخاطر الالتزام والأنظمة.

مخاطر الاحتيال وغسل الأموال وتمويل الإرهاب.

مخاطر العقود والموردين والشركاء.

مخاطر التقنية والأمن السيبراني.

مخاطر البيانات والخصوصية.

مخاطر السمعة والإعلام.

مخاطر الصحة والسلامة والطوارئ.

مخاطر استمرارية الأعمال.

المخاطر البيئية والطبيعية.

مخاطر الأصول والمرافق.

المادة الثامنة: شهية المخاطر

يعتمد مجلس الإدارة شهية المخاطر العامة للجمعية، على أن تكون:

منخفضة جدا في المخاطر المتعلقة بسلامة المستفيدين والأشخاص.

منخفضة جدا في الفساد والاحتيال وغسل الأموال وتمويل الإرهاب.

منخفضة في مخالفة الأنظمة أو التصاريح أو شروط المانحين.

منخفضة في انتهاك البيانات والخصوصية والأمن السيبراني.

منخفضة إلى متوسطة في المخاطر المالية والتشغيلية وفق الضوابط.

متوسطة في المبادرات والابتكار المنضبط الذي يخدم أهداف الجمعية.



محددة بحدود كمية أو نوعية كلما أمكن.
ولا يجوز قبول خطر يتجاوز شهية المجلس إلا بقرار مسبب من الجهة صاحبة الصلاحية وبعد تحديد خطة معالجة ومتابعة.

المادة التاسعة: ثقافة المخاطر

تعمل الجمعية على بناء ثقافة مؤسسية تشجع على:
الإبلاغ المبكر عن المخاطر والحوادث.
مناقشة الأخطاء دون إخفائها.
عدم الانتقام من المبلغ حسن النية.
اعتبار إدارة المخاطر مسؤولية مشتركة.
إدراج المخاطر في الاجتماعات والتقارير.
تدريب العاملين على أدوارهم.
الاستفادة من الدروس المستخلصة.

الفصل الثالث: الحوكمة والمسؤوليات

المادة العاشرة: مسؤولية مجلس الإدارة

يتولى مجلس الإدارة:
اعتماد السياسة ومنهجية إدارة المخاطر.
اعتماد شهية المخاطر وحدود التحمل.
متابعة المخاطر الاستراتيجية والجوهرية.



اعتماد خطط استمرارية الأعمال والتعافي.

التأكد من توفير الموارد اللازمة.

متابعة نتائج الاختبارات والحوادث.

اعتماد قبول المخاطر التي تتجاوز صلاحيات الإدارة التنفيذية.

متابعة الإجراءات التصحيحية الجوهرية.

مساءلة الإدارة التنفيذية عن فاعلية الإطار.

مراجعة السياسة مرة واحدة على الأقل سنوياً.

المادة الحادية عشرة: لجنة المخاطر أو اللجنة المختصة

يجوز لمجلس الإدارة إسناد الإشراف على المخاطر إلى لجنة مختصة تتولى:

مراجعة سجل المخاطر.

دراسة المخاطر الناشئة والجوهرية.

مراجعة تقارير استمرارية الأعمال.

متابعة خطط المعالجة.

مراجعة نتائج الاختبارات والتمارين.

التحقق من توافق المخاطر مع شهية المجلس.

رفع التوصيات إلى مجلس الإدارة.

التنسيق مع لجنة المراجعة دون ازدواجية في الاختصاص.



المادة الثانية عشرة: مسؤولية المسؤول التنفيذي

يتولى المسؤول التنفيذي:

- تطبيق السياسة والإطار المعتمد.
- تعيين مسؤول أو منسق لإدارة المخاطر.
- التأكد من تحديث سجل المخاطر.
- اعتماد خطط المعالجة الواقعة ضمن صلاحياته.
- رفع المخاطر الجوهرية إلى مجلس الإدارة.
- تفعيل خطط الطوارئ والاستمرارية عند الحاجة.
- توفير الموارد والتدريب.
- متابعة الموردين والأنظمة والعمليات الحيوية.
- الإشراف على الاستجابة للحوادث.
- اعتماد تقارير ما بعد الحوادث.

المادة الثالثة عشرة: مسؤول إدارة المخاطر

يتولى مسؤول إدارة المخاطر أو من يكلف بمهامه:

- تطوير المنهجية والنماذج.
- تنسيق عمليات تحديد وتقييم المخاطر.
- إدارة سجل المخاطر المركزي.
- متابعة ملاك المخاطر وخطط المعالجة.
- إعداد تقارير المخاطر والمؤشرات.



تنسيق تحليل أثر الأعمال.

إعداد خطة استمرارية الأعمال وتحديثها.

تنسيق الاختبارات والتمارين.

تقديم التدريب والتوعية.

رصد المخاطر الناشئة.

رفع حالات التجاوز والتأخر.

التنسيق مع المراجعة الداخلية والالتزام والتقنية.

المادة الرابعة عشرة: مالك الخطر

يتولى مالك الخطر:

تحديد الخطر وأسبابه وآثاره.

تقييم الخطر الكامن والمتبقي.

تحديد الضوابط القائمة.

اقتراح خطة المعالجة.

تنفيذ الإجراءات في مواعيدها.

مراقبة مؤشرات الإنذار.

الإبلاغ عن أي تغير جوهري.

توفير أدلة تنفيذ المعالجة.

مراجعة الخطر دوريا.

المشاركة في اختبارات الاستمرارية ذات الصلة.





المادة الخامسة عشرة: مسؤولية الإدارات

تلتزم كل إدارة بما يأتي:

- تحديد مخاطر عملياتها وبرامجها.
- تقييم أثر التغييرات والمشروعات الجديدة.
- عدم بدء نشاط عالي المخاطر دون اعتماد.
- تحديث سجل المخاطر عند وقوع حادث.
- تحديد العمليات الحيوية والموارد اللازمة لها.
- إعداد إجراءات بديلة للعمل.
- تدريب العاملين على أدوارهم.
- حفظ قوائم الاتصال والطوارئ محدثة.
- المشاركة في التمارين والاختبارات.
- رفع تقارير دورية عن المخاطر.

المادة السادسة عشرة: المراجعة الداخلية

تقدم المراجعة الداخلية تأكيداً مستقلاً بشأن:

- تصميم إطار إدارة المخاطر.
- دقة واكتمال سجل المخاطر.
- فاعلية الضوابط.
- سلامة تقارير المخاطر.
- تنفيذ خطط المعالجة.



جاهزية استمرارية الأعمال.

نتائج الاختبارات والتعافي.

التزام الإدارات بالسياسة.

ولا تتولى المراجعة الداخلية ملكية المخاطر أو تنفيذ الضوابط التي ستراجعها.

المادة السابعة عشرة: العاملون والمتطوعون

يلتزم العاملون والمتطوعون بما يأتي:

معرفة المخاطر المرتبطة بمهامهم.

تطبيق الضوابط والتعليمات.

الإبلاغ الفوري عن الحوادث أو المخاطر.

المشاركة في التدريب والتمارين.

المحافظة على الأصول والبيانات.

عدم تجاوز الضوابط دون اعتماد.

التعاون في التحقيق والتعافي.

الالتزام بإجراءات السلامة والطوارئ.

الفصل الرابع: تحديد المخاطر وتقييمها

المادة الثامنة عشرة: مصادر تحديد المخاطر

تحدد المخاطر من خلال:



التخطيط الاستراتيجي والتشغيلي.

إعداد الميزانية.

تصميم البرامج والمشروعات.

تحليل العمليات والإجراءات.

الشكاوى والبلاغات.

تقارير المراجعة والتدقيق.

الحوادث السابقة.

تقييمات الموردين والشركاء.

التغيرات النظامية والتقنية.

ورش العمل والمقابلات.

تحليل البيئة الداخلية والخارجية.

اختبارات الاستمرارية والأمن.

تقارير الأداء والانحرافات.

شروط المانحين والعقود.

المادة التاسعة عشرة: وصف الخطر

يكتب الخطر بطريقة توضح:

الحدث المحتمل.

سببه أو مصدره.

أثره المتوقع.





العملية أو الهدف المتأثر.
الأطراف أو الأصول المتأثرة.
الضوابط القائمة.
مالك الخطر.
ويجب تجنب العبارات العامة التي لا تمكن من فهم الخطر أو قياسه.

المادة العشرون: مقياس الاحتمالية

يجوز استخدام المقياس الآتي:

الدرجة	مستوى الاحتمالية	الوصف الاسترشادي
1	نادر	لا يتوقع وقوعه إلا في ظروف استثنائية
2	غير مرجح	يمكن أن يقع، لكن احتمالاه محدود
3	ممکن	قد يقع خلال دورة العمل
4	مرجح	يتوقع وقوعه في ظروف متعددة
5	شبه مؤكد	وقع مرارا أو يتوقع وقوعه بدرجة عالية

المادة الحادية والعشرون: مقياس الأثر

يقيم الأثر على أعلى نتيجة محتملة في المجالات الآتية:

سلامة الأشخاص.

المستفيدون وجودة الخدمة.

الأثر المالي.



الالتزام النظامي.

السمعة والثقة.

البيانات والأمن السيبراني.

مدة توقف العمليات.

تحقيق الأهداف الاستراتيجية.

ويستخدم المقياس الآتي:

الدرجة مستوى الأثر الوصف الاسترشادي

- 1 طفيف أثر محدود يمكن معالجته فوراً
- 2 منخفض تعطيل أو خسارة محدودة داخل إدارة واحدة
- 3 متوسط تأثير ملموس يتطلب تدخل الإدارة التنفيذية
- 4 كبير تأثير جوهري على عدة خدمات أو التزامات
- 5 جسيم تهديد للأرواح أو الاستدامة أو مخالفة جسيمة أو توقف واسع

المادة الثانية والعشرون: احتساب درجة الخطر

تحتسب درجة الخطر بضرر درجة الاحتمالية في درجة الأثر، وتصنف استرشادياً إلى:

الدرجة التصنيف الإجراء

1 إلى 4 منخفض متابعة ضمن الإجراءات المعتادة

5 إلى 9 متوسط خطة معالجة ومراقبة دورية

10 إلى 16 عال معالجة عاجلة ورفع للإدارة التنفيذية

17 إلى 25 حرج تصعيد فوري لمجلس الإدارة وإجراء عاجل



ويجوز تعديل حدود التصنيف بقرار من مجلس الإدارة بما يتناسب مع طبيعة الجمعية.

المادة الثالثة والعشرون: تقييم الضوابط

تقييم الضوابط بحسب:

ملاءمة تصميمها للخطر.

مدى تطبيقها فعلياً.

انتظام توثيقها.

استقلال مراجعتها.

وجود استثناءات أو تجاوزات.

نتائج الاختبارات والحوادث.

اعتمادها على شخص واحد أو نظام واحد.

وتصنف الضوابط إلى فعالة، أو فعالة جزئياً، أو غير فعالة، مع توثيق مبررات التصنيف.

المادة الرابعة والعشرون: الخطر المتبقي

يعاد تقييم الاحتمالية والأثر بعد تطبيق الضوابط، ويقارن الخطر المتبقي بشهية المخاطر. وإذا بقي أعلى من الحد المقبول، يجب إعداد خطة إضافية أو وقف النشاط أو رفع قرار قبول الخطر إلى صاحب الصلاحية.

الفصل الخامس: معالجة المخاطر

المادة الخامسة والعشرون: خيارات المعالجة





تعالج المخاطر بأحد الخيارات الآتية أو بمزيج منها:

التجنب: وقف النشاط أو عدم البدء فيه.

التقليل: تطبيق ضوابط تحد من الاحتمال أو الأثر.

النقل أو المشاركة: التأمين أو التعاقد أو توزيع المسؤولية، دون نقل المسؤولية النظامية للجمعية.

القبول: تحمل الخطر المتبقي بعد دراسة واعتماد.

الاستغلال: الاستفادة من الفرص الإيجابية المرتبطة بالخطر ضمن حدود مدروسة.

المادة السادسة والعشرون: خطة المعالجة

تتضمن خطة المعالجة:

وصف الإجراء.

مالك الإجراء.

الموارد والميزانية.

تاريخ البدء والانتهاء.

الأولوية.

مؤشر الإنجاز.

الخطر المستهدف بعد المعالجة.

الاعتماد المطلوب.

الاعتماد على أطراف أو أنظمة أخرى.

دليل الإغلاق.



المادة السابعة والعشرون: قبول الخطر

- لا يقبل الخطر إلا بعد:
- توثيق درجة الخطر المتبقي.
- بيان أسباب عدم المعالجة الإضافية.
- تقييم الأثر على المستفيدين والالتزام.
- تحديد مدة القبول.
- تحديد مؤشرات المراقبة.
- اعتماد صاحب الصلاحية.
- مراجعة القبول عند تغير الظروف.
- ولا يجوز قبول خطر حرج يتعلق بسلامة الأشخاص أو جريمة أو مخالفة نظامية إلزامية.

المادة الثامنة والعشرون: الاستثناءات

- أي استثناء من ضابط أو سياسة يجب أن يكون:
- مكتوبا ومسببا.
- محدد النطاق والمدة.
- متضمنا تقييما للمخاطر.
- متضمنا ضوابط تعويضية.
- معتمدا من صاحب الصلاحية.
- مسجلا ومراقبا حتى انتهائه.



الفصل السادس: سجل المخاطر والتقارير

المادة التاسعة والعشرون: سجل المخاطر

يتضمن سجل المخاطر، على الأقل:

الرقم المرجعي.

فئة الخطر.

وصف الخطر وسببه وأثره.

الهدف أو العملية المتأثرة.

مالك الخطر.

الضوابط القائمة.

الاحتمالية والأثر الكامنان.

فاعلية الضوابط.

الاحتمالية والأثر المتبقيان.

خطة المعالجة.

تاريخ الاستحقاق.

مؤشرات الإنذار.

حالة الخطر.

تاريخ آخر مراجعة.

قرار القبول أو التصعيد.



المادة الثلاثون: مؤشرات المخاطر الرئيسية

- تحدد مؤشرات إنذار قابلة للقياس، ومنها:
- انخفاض السيولة عن الحد المعتمد.
- ارتفاع الاعتماد على مانح واحد.
- زيادة الشكاوى أو الحوادث.
- ارتفاع معدل دوران الموظفين.
- تأخر المشروعات أو تجاوز ميزانياتها.
- تكرار تعطل الأنظمة.
- ازدياد محاولات الاختراق.
- ارتفاع العمليات المالية غير المعتادة.
- انتهاء تصاريح أو عقود دون تجديد.
- زيادة اعتماد العمليات على مورد أو شخص واحد.
- انخفاض النسخ الاحتياطية الناجحة.
- تأخر إغلاق الملاحظات الرقابية.

المادة الحادية والثلاثون: دورية المراجعة

- تراجع المخاطر:
- ربع سنويا للمخاطر العالية والدرجة.
- نصف سنويا للمخاطر المتوسطة.
- سنويا للمخاطر المنخفضة.



فور وقوع حادث.

عند إطلاق مشروع أو برنامج جديد.

عند تغير نظامي أو تقني أو تنظيمي.

عند تغير التمويل أو الموردين الرئيسيين.

المادة الثانية والثلاثون: تقارير المخاطر

يرفع مسؤول المخاطر تقريراً دورياً يتضمن:

خريطة المخاطر.

أعلى المخاطر المتبقية.

التغيرات منذ التقرير السابق.

المخاطر الجديدة والناشئة.

خطط المعالجة المتأخرة.

حالات تجاوز شهية المخاطر.

الحوادث والخسائر.

مؤشرات الإنذار.

حالة الاستمرارية والاختبارات.

التوصيات والقرارات المطلوبة.

الفصل السابع: تحليل أثر الأعمال

المادة الثالثة والثلاثون: هدف تحليل الأثر





يهدف تحليل أثر الأعمال إلى تحديد:

العمليات والخدمات الحيوية.

آثار توقف كل عملية.

الحد الأقصى المقبول للتوقف.

الوقت المستهدف للتعافي.

نقطة استعادة البيانات المستهدفة.

الحد الأدنى من الموارد اللازمة.

الاعتماد على الأنظمة والأشخاص والموردين.

ترتيب أولويات الاستعادة.

المادة الرابعة والثلاثون: معايير تحديد العمليات الحيوية

تعد العملية حيوية إذا أدى توقفها إلى:

تهديد سلامة المستفيدين أو العاملين.

إخلال نظامي أو تعاقدية جوهري.

انقطاع خدمة أساسية.

خسارة مالية كبيرة.

ضرر جسيم بالسمعة.

فقد بيانات أو أصول مهمة.

تعذر الوفاء بالتزامات مانح أو جهة حكومية.

تأثير متسلسل في عمليات أخرى.





المادة الخامسة والثلاثون: عناصر تحليل الأثر

- يتضمن التحليل لكل عملية:
- اسم العملية ومالكها.
- المدخلات والمخرجات.
- عدد المستفيدين أو الأطراف المتأثرين.
- أوقات الذروة والمواعيد الحرجة.
- الأنظمة وقواعد البيانات.
- الموظفين والمهارات الحرجة.
- الموردين والشركاء.
- المرافق والأجهزة.
- الحد الأدنى المقبول للخدمة.
- بدائل التشغيل اليدوية أو التقنية.
- أهداف التعافي.
- أثر التوقف حسب الفترات الزمنية.

المادة السادسة والثلاثون: تحديث تحليل الأثر

- يحدث تحليل أثر الأعمال مرة واحدة على الأقل سنوياً، وعند:
- إطلاق أو إيقاف خدمة.
- تغيير نظام جوهري.
- نقل مقر أو موقع.





تغيير مورد رئيسي.

تعديل الهيكل التنظيمي.

تغير المتطلبات النظامية.

وقوع حادث يكشف افتراضات غير صحيحة.

الفصل الثامن: خطة استمرارية الأعمال

المادة السابعة والثلاثون: محتويات الخطة

تتضمن خطة استمرارية الأعمال:

أهداف الخطة ونطاقها.

معايير التفعيل والإلغاء.

فريق إدارة الاستمرارية.

أدوار وصلاحيات الفريق.

قوائم الاتصال والتصعيد.

العمليات الحيوية وأولوياتها.

إجراءات التشغيل البديلة.

المواقع والأنظمة والموارد البديلة.

خطة الاتصال الداخلي والخارجي.

خطة استعادة البيانات والأنظمة.

إدارة الموردين والخدمات الخارجية.

نماذج التوثيق والتقارير.



آلية العودة إلى التشغيل الطبيعي.

خطة الاختبار والتحديث.

المادة الثامنة والثلاثون: معايير تفعيل الخطة

يجوز تفعيل الخطة عند:

تعذر استخدام المقر.

توقف نظام أو قاعدة بيانات حيوية.

فقد عدد مؤثر من الموظفين.

انقطاع الاتصالات أو الكهرباء لمدة مؤثرة.

وقوع هجوم سيبراني أو تسرب بيانات.

تعطل مورد أو شريك حيوي.

حريق أو كارثة طبيعية أو وباء.

توقف التدفقات المالية أو الحسابات.

وقوع أزمة تهدد سلامة الأشخاص أو استمرار الخدمات.

صدور توجيه من جهة مختصة.

المادة التاسعة والثلاثون: صلاحية التفعيل

يتولى المسؤول التنفيذي تفعيل الخطة، أو من يفوضه عند تعذر الوصول إليه. وفي الحالات الحرجة يجوز لأعلى مسؤول متاح اتخاذ إجراءات الحماية الفورية، على أن يوثق القرار ويبلغ مجلس الإدارة في أقرب وقت.



المادة الأربعون: فريق الاستمرارية

يشكل فريق استمرارية الأعمال، ويحدد لكل عضو بديل، ويشمل بحسب الحاجة:
قائد الفريق.

ممثل الإدارة التنفيذية.

ممثل البرامج والمستفيدين.

ممثل المالية.

ممثل تقنية المعلومات.

ممثل الموارد البشرية.

ممثل الاتصال والإعلام.

ممثل الأمن والسلامة.

ممثل الالتزام أو الشؤون القانونية.

أي خير أو جهة مساندة.

المادة الحادية والأربعون: الاتصال أثناء الانقطاع

تحدد الخطة:

قائمة اتصال محدثة.

وسائل اتصال أساسية وبديلة.

الشخص المخول بالتحدث باسم الجمعية.

رسائل مبدئية للعاملين والمستفيدين.





آلية التواصل مع الجهات الحكومية والمانحين.
آلية تسجيل القرارات والتعليمات.
ضوابط حماية المعلومات أثناء الأزمة.
توقيت تحديث الرسائل بحسب تطور الوضع.

المادة الثانية والأربعون: الموقع والموارد البديلة

تحدد الجمعية البدائل المناسبة، ومنها:

- العمل عن بعد.
- موقع بديل.
- أجهزة محمولة معتمدة.
- اتصالات احتياطية.
- مصادر كهرباء بديلة.
- نسخ ورقية أو إلكترونية للإجراءات الحرجة.
- موظفون بدلاء ومتعددون في المهارات.
- موردون بدلاء.
- مخزون طوارئ للمواد الضرورية.
- تفويضات مؤقتة محددة.

الفصل التاسع: استمرارية التقنية والبيانات

المادة الثالثة والأربعون: النسخ الاحتياطية





تطبق الجمعية خطة نسخ احتياطي تحدد:

الأنظمة والبيانات المشمولة.

دورية النسخ.

مواقع النسخ.

التشفير والحماية.

مدة الاحتفاظ.

الأشخاص المخولين.

اختبارات الاستعادة.

معالجة فشل النسخ.

المادة الرابعة والأربعون: أهداف التعافي

تحدد الجمعية لكل نظام حيوي:

الوقت المستهدف للتعافي.

نقطة الاستعادة المستهدفة.

الحد الأدنى من الأداء.

ترتيب الاستعادة.

الأنظمة التي يعتمد عليها.

المسؤول الفني.

البديل اليدوي أو التقني.

معايير قبول الاستعادة.



المادة الخامسة والأربعون: الاستجابة للحوادث السيبرانية

عند وقوع حادث سيبراني:

يعزل الجزء المتأثر عند الحاجة.

تحفظ الأدلة والسجلات.

يمنع استخدام أجهزة أو حسابات مشتببه بها.

يفعل فريق الاستجابة.

تقيم البيانات والأنظمة المتأثرة.

تستعاد الخدمات حسب الأولوية.

يبلغ أصحاب البيانات والجهات المختصة متى وجب ذلك.

يجرى تحليل للسبب الجذري.

تحدث الضوابط وخطط التعافي.

المادة السادسة والأربعون: صلاحيات الطوارئ التقنية

يجوز منح صلاحيات تقنية طارئة محددة المدة والنطاق، بشرط:

اعتمادها من المسؤول المخول.

تسجيل استخدامها.

مراقبة الأنشطة.

سحبها فور انتهاء الحاجة.

مراجعة ما تم من عمليات.

عدم استخدامها لتجاوز ضوابط السرية دون ضرورة موثقة.





الفصل العاشر: الموردون والأطراف الخارجية

المادة السابعة والأربعون: الموردون الحيويون

تحدد الجمعية الموردين والشركاء الذين يؤثر تعطلهم في العمليات الحيوية، وتتحقق من:

خطط استمرارياتهم.

قدرتهم المالية والفنية.

بدائلهم ومواردهم الاحتياطية.

التزامات الإبلاغ عن الحوادث.

أهداف استعادة الخدمة.

حماية البيانات.

حق الجمعية في التدقيق.

خطط الخروج ونقل الخدمة.

المادة الثامنة والأربعون: شروط العقود

تتضمن العقود الجوهرية، بحسب الحاجة:

مستوى الخدمة.

مدد الاستجابة والتعافي.

النسخ الاحتياطية.

استمرارية الخدمة.

الإبلاغ عن الحوادث.

أمن المعلومات وحماية البيانات.



المورد البديل أو خطة الخروج.

المسؤولية والتعويض.

الاختبار والتدقيق.

إعادة البيانات والأصول عند انتهاء العقد.

المادة التاسعة والأربعون: تعطل المورد

عند تعطل مورد حيوي:

يفعل البديل التعاقدي أو التشغيلي.

يحصّر أثر التعطل.

يخطر المورد رسمياً.

تتابع خطة استعادة الخدمة.

يبلغ المستفيدون أو المانحون عند الحاجة.

تطبق الجزاءات أو الحقوق التعاقدية.

يراجع تقييم المورد واستمرار العلاقة.

الفصل الحادي عشر: الاختبارات والتمارين

المادة الخمسون: برنامج الاختبارات

تعد الجمعية برنامجاً سنوياً لاختبار:

قوائم الاتصال.

الإخلاء والسلامة.





العمل عن بعد.

استعادة النسخ الاحتياطية.

تعافي الأنظمة الحيوية.

تعطل مورد رئيسي.

انقطاع الكهرباء أو الاتصالات.

الاستجابة لهجوم سيبراني.

فقد مقر أو موقع.

إدارة أزمة مالية أو سمعة.

المادة الحادية والخمسون: أنواع الاختبارات

يجوز استخدام:

مراجعة مكتوبة للخطأ.

تمرين مناقشة سيناريو.

اختبار اتصال.

اختبار فني جزئي.

تشغيل موقع أو نظام بديل.

محاكاة شاملة.

اختبار مفاجئ محدود بعد تقدير أثره.



المادة الثانية والخمسون: ضوابط الاختبار

يجب أن:

- يحدد هدف ونطاق السيناريو.
- تعتمد الخطة مسبقاً.
- تتبع سلامة الأشخاص والبيانات.
- تحدد فرق المراقبة والتقييم.
- توثق النتائج والملاحظات.
- لا يعرض الاختبار الخدمات أو الأنظمة لخطر غير مقبول.
- يعالج القصور خلال مدد محددة.
- يعاد الاختبار عند وجود فشل جوهري.

المادة الثالثة والخمسون: تقرير الاختبار

- يتضمن التقرير:
- السيناريو والهدف.
- تاريخ ومكان الاختبار.
- المشاركون.
- الإجراءات المنفذة.
- الزمن الفعلي للاستجابة والتعافي.
- مدى تحقيق الأهداف.
- أوجه النجاح والقصور.





المخاطر المكتشفة.

خطة التحسين.

المسؤوليات والمواعيد.

قرار إعادة الاختبار.

الفصل الثاني عشر: إدارة الحوادث والتعافي

المادة الرابعة والخمسون: الإبلاغ عن الحوادث

يلتزم كل من يكتشف حادثاً بإبلاغ القناة المعتمدة فوراً، مع بيان:

طبيعة الحادث.

الموقع والوقت.

الأشخاص أو الأنظمة المتأثرة.

الخطر العاجل.

الإجراء الأولي المتخذ.

وسائل التواصل المتاحة.

ويحظر إخفاء الحادث أو تعديل الأدلة أو نشر معلومات غير معتمدة عنه.

المادة الخامسة والخمسون: أولويات الاستجابة

تكون الأولويات:

حماية الأرواح والسلامة.

منع توسع الحادث.



- حماية المستفيدين.
- حفظ الأدلة والبيانات.
- استعادة العمليات الحيوية.
- الوفاء بالالتزامات النظامية.
- التواصل مع الأطراف.
- الحد من الأثر المالي والسمعة.
- العودة المنظمة للتشغيل الطبيعي.

المادة السادسة والخمسون: سجل الحوادث

يتضمن سجل الحوادث:

- رقم الحادث.
- تاريخ ووقت الاكتشاف.
- وصف الحادث.
- التصنيف والخطورة.
- العمليات والأشخاص المتأثرين.
- القرارات والإجراءات.
- مدة الانقطاع.
- الخسائر أو الأضرار.
- الاتصالات والإبلاغات.
- تاريخ استعادة الخدمة.



السبب الجذري.

الإجراءات التصحيحية.

تاريخ الإغلاق.

المادة السابعة والخمسون: العودة إلى الوضع الطبيعي

لا يعلن انتهاء حالة الاستمرارية إلا بعد:

استقرار العمليات الحيوية.

التحقق من سلامة الأنظمة والبيانات.

تسوية العمليات المؤجلة أو اليدوية.

استعادة الصلاحيات المعتادة.

إشعار الأطراف المعنية.

توثيق الخسائر والالتزامات.

اعتماد قائد الفريق أو المسؤول التنفيذي.

بدء مراجعة ما بعد الحادث.

المادة الثامنة والخمسون: مراجعة ما بعد الحادث

تجرى مراجعة تتضمن:

التسلسل الزمني للحادث.

فاعلية الاستجابة.

مدى تحقق أهداف التعافي.





أوجه القصور في الخطة.

جودة الاتصال والتصعيد.

أثر الموردين والأنظمة.

السبب الجذري.

التكاليف والخسائر.

الإجراءات التصحيحية.

الدروس المستفادة وتحديث الخطة.

الفصل الثالث عشر: التدريب والتوعية

المادة التاسعة والخمسون: التدريب العام

تعرف الجمعية جميع العاملين والمتطوعين بما يأتي:

مفهوم المخاطر.

آلية الإبلاغ.

إجراءات الطوارئ والإخلاء.

قنوات الاتصال.

حماية البيانات والأصول.

أدوارهم عند الانقطاع.

ضوابط العمل البديل.

منع نشر معلومات غير معتمدة.



المادة الستون: التدريب المتخصص

يقدم تدريب متخصص إلى:

فريق إدارة المخاطر.

فريق استثمارية الأعمال.

فريق الطوارئ والأزمات.

تقنية المعلومات والأمن السيبراني.

الإدارة المالية.

مسؤولي البرامج والمستفيدين.

الاتصال والإعلام.

الأمن والسلامة.

ملاك العمليات الحيوية.

البدلاء المعتمدين للوظائف الحرجة.

المادة الحادية والستون: الإحلال وتعدد المهارات

تحدد الجمعية الوظائف والمهارات الحرجة، وتوفر لها:

بديلا مؤهلا.

توثيقا للإجراءات.

تدريباً تبادلياً.

صلاحيات طوارئ منظمة.

خطط تسليم واستلام.





مراجعة دورية لمدى جاهزية البديل.

الفصل الرابع عشر: الرقابة ومؤشرات الأداء

المادة الثانية والستون: مؤشرات الأداء والمخاطر

تشمل المؤشرات:

نسبة المخاطر المحدثة في موعدها.

نسبة خطط المعالجة المنفذة.

عدد المخاطر المتجاوزة للشهية.

عدد الحوادث حسب التصنيف.

متوسط زمن اكتشاف الحادث.

متوسط زمن استعادة العمليات.

نسبة نجاح النسخ الاحتياطية.

نسبة نجاح اختبارات الاستعادة.

نسبة العمليات الحيوية التي لها خطط محدثة.

نسبة الموظفين المدربين.

عدد الموردين الحيويين دون خطط استمرارية.

نسبة إغلاق ملاحظات الاختبارات.

مقدار الخسائر الناتجة عن الحوادث.

نسبة الالتزام بأهداف وقت التعافي.



المادة الثالثة والستون: التقارير الدورية

ترفع تقارير المخاطر والاستمرارية إلى المسؤول التنفيذي ومجلس الإدارة أو اللجنة المختصة، وتشمل:

- أعلى المخاطر.
- التغيرات والاتجاهات.
- حالة خطط المعالجة.
- الحوادث والانقطاعات.
- نتائج الاختبارات.
- جاهزية العمليات الحيوية.
- حالة الموردين.
- التجاوزات والاستثناءات.
- الموارد المطلوبة.
- القرارات والتوصيات.

المادة الرابعة والستون: المراجعة المستقلة

تراجع المراجعة الداخلية أو جهة مستقلة إطار المخاطر والاستمرارية دورياً، وتتحقق من تصميمه وتطبيقه وفاعليته، وترفع النتائج وخطط المعالجة إلى لجنة المراجعة ومجلس الإدارة.

الفصل الخامس عشر: المخالفات والأحكام الختامية

المادة الخامسة والستون: المخالفات

تعد من المخالفات:





عدم الإفصاح عن خطر أو حادث جوهري.

تقديم تقييم أو تقرير مضلل.

تجاهل خطة معالجة معتمدة.

تجاوز شهية المخاطر دون اعتماد.

تعطيل اختبار أو تمرين.

إساءة استخدام صلاحيات الطوارئ.

إتلاف الأدلة أو سجلات الحوادث.

نشر معلومات غير معتمدة أثناء الأزمة.

عدم تطبيق إجراءات السلامة.

عدم إلغاء صلاحيات الطوارئ بعد انتهاء الحاجة.

تجاهل تعطل مورد أو نظام حيوي.

عدم تحديث بيانات الاتصال أو الخطط رغم التكليف.

المادة السادسة والستون: الإجراءات التصحيحية

يجوز للجمعية اتخاذ واحد أو أكثر من الإجراءات الآتية:

وقف النشاط أو العملية عالية المخاطر.

تطبيق ضوابط إضافية.

نقل ملكية الخطر أو المسؤولية التشغيلية.

تقييد الصلاحيات.





إعادة التدريب.

فتح تحقيق إداري.

تطبيق جزاء وظيفي أو تعاقد.

إنهاء علاقة مع مورد أو شريك.

معالجة الضرر واسترداد الخسائر نظاماً.

الإبلاغ إلى الجهة المختصة عند وجوبه.

تحديث الخطة والسياسات.

إعادة الاختبار للتحقق من فاعلية المعالجة.

المادة السابعة والستون: حفظ السجلات

تحفظ سجلات المخاطر وتحليل أثر الأعمال وخطط الاستمرارية والاختبارات والحوادث والتقارير للمدة المعتمدة في سياسة الاحتفاظ بالوثائق، ولا تتلف أثناء تحقيق أو نزاع أو مراجعة أو طلب رسمي.

المادة الثامنة والستون: عدم التعارض

تفسر هذه السياسة بما لا يتعارض مع الأنظمة واللوائح والتعليمات النافذة. وعند التعارض يطبق النص الأعلى مرتبة، وتحدث السياسة بما يزيل التعارض.

المادة التاسعة والستون: المراجعة والتعديل

تراجع السياسة سنوياً، أو عند:





تغير جوهري في استراتيجية الجمعية.

إطلاق أو إيقاف خدمة حيوية.

وقوع حادث أو أزمة جوهري.

تغير نظام أو مورد أو مقر رئيسي.

صدور متطلب نظامي جديد.

ظهور قصور في اختبار الاستمرارية.

تغير شهية المخاطر.

ولا تعدل إلا بقرار من مجلس الإدارة.

المادة السبعون: النفاذ

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

النماذج والسجلات المرتبطة

سجل المخاطر المؤسسي.

نموذج تحديد وتقييم خطر.

مصفوفة الاحتمالية والأثر.

نموذج خطة معالجة خطر.

نموذج قبول خطر متبق.

سجل الاستثناءات وتجاوز شهية المخاطر.

نموذج مؤشرات المخاطر الرئيسية.





نموذج تحليل أثر الأعمال.

سجل العمليات والخدمات الحيوية.

خطة استمرارية الأعمال.

خطة الاتصال في الأزمات.

قائمة الاتصال والطوارئ.

نموذج تقييم مورد حيوي.

خطة التعافي من الكوارث التقنية.

نموذج بلاغ حادث.

سجل الحوادث والانقطاعات.

نموذج تفعيل خطة الاستمرارية.

نموذج تقرير اختبار أو تمرين.

نموذج مراجعة ما بعد الحادث.

سجل الإجراءات التصحيحية والدروس المستفادة.

نموذج سجل المخاطر

الحقل البيانات

رقم الخطر

فئة الخطر

الهدف أو العملية المتأثرة

وصف الخطر

الأسباب



..... الآثار المحتملة

..... مالك الخطر

..... الضوابط القائمة

5 / 4 / 3 / 2 / 1 الاحتمالية الكامنة

5 / 4 / 3 / 2 / 1 الأثر الكامن

..... درجة الخطر الكامن

فاعلية الضوابط فعالة / جزئية / غير فعالة

5 / 4 / 3 / 2 / 1 الاحتمالية المتبقية

5 / 4 / 3 / 2 / 1 الأثر المتبقي

..... درجة الخطر المتبقي

خيار المعالجة تجنب / تقليل / نقل / قبول

..... إجراءات المعالجة

..... مسؤول التنفيذ

..... تاريخ الاستحقاق

..... مؤشر الإنذار

حالة التنفيذ لم يبدأ / جار / مكتمل / متأخر

..... تاريخ المراجعة

..... قرار صاحب الصلاحية

نموذج تحليل أثر الأعمال

..... اسم الإدارة:



اسم العملية أو الخدمة:

مالك العملية:

وصف العملية:

المستفيدون أو الأطراف المتأثرون:

أثر التوقف:

أثر على سلامة الأشخاص:

أثر على المستفيدين:

أثر مالي:

أثر نظامي أو تعاقدية:

أثر على السمعة:

أثر على البيانات والأنظمة:

الحد الأقصى المقبول للتوقف:

الوقت المستهدف للتعافي:

نقطة استعادة البيانات المستهدفة:

الحد الأدنى المقبول للخدمة:

الموارد الحرجة:



الموظفون والمهارات:

الأنظمة والبيانات:

الأجهزة والمرافق:

الموردون والشركاء:

المستندات والصلاحيات:

الإجراء أو البديل التشغيلي:

.....

.....

تاريخ آخر اختبار:

نتيجة الاختبار:

التحسينات المطلوبة:

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.