



مديم
modeem

جمعية مديم الرقمية
Modeem Digital charity

سياسة النسخ الاحتياطي والتخزين في الجمعية



الصادر عن: إدارة التقنية - الجمعية





الهدف:

تهدف هذه السياسة إلى ضمان الحفاظ على سلامة البيانات وحمايتها من فقدان أو التلف، وذلك من خلال وضع إجراءات واضحة للنسخ الاحتياطي والتخزين الآمن للبيانات داخل الجمعية. تهدف الجمعية إلى ضمان استمرارية الأعمال وحماية البيانات الحيوية الخاصة بالجمعية.

يعمل النسخ الاحتياطي على ما يلي:

- توفير تخزين آمن لأصول البيانات الهامة لسير العمل في الجمعية
- منع فقدان البيانات في حالة الحذف العرضي أو تلف البيانات أو فشل النظام أو حدوث الكوارث.
- السماح باستعادة البيانات المؤرشفة في الوقت المناسب في حالة حدوث مشكلة أو فشل في النظام.

المبادئ الأساسية للسياسة:

1. أهمية النسخ الاحتياطي:

- يُعد النسخ الاحتياطي أداة أساسية لضمان استعادة البيانات في حالة حدوث أي تلف أو فقدان غير متوقع. تهدف الجمعية إلى حفظ جميع البيانات الهامة المرتبطة بالأنشطة الإدارية والفنية في مكان آمن يسهل استرجاعها عند الحاجة.
- تشمل البيانات التي يجب عمل نسخ احتياطي لها: المستندات، التقارير، قواعد البيانات، سجلات البريد الإلكتروني، الأنظمة المحاسبية، وبيانات العملاء.

2. تواتر النسخ الاحتياطي:

- النسخ الاحتياطي اليومي: يتم إجراء نسخ احتياطي يومي للبيانات المتجددة مثل السجلات المالية والبيانات المتعلقة بالعمل اليومي .
- النسخ الاحتياطي الأسبوعي: يتم إجراء نسخ احتياطي أسبوعي للملفات والبيانات الثابتة التي لا تتغير بشكل متكرر.
- النسخ الاحتياطي الشهري: يتم إجراء نسخ احتياطي شهري لجميع البيانات الهامة، ويشمل النسخ الاحتياطي شهريًا حفظ النسخ طويلة المدى التي يمكن استخدامها لاسترجاع البيانات من فترات طويلة.



3. طرق النسخ الاحتياطي:

- النسخ الاحتياطي المحلي: يتم تخزين النسخ الاحتياطي على أجهزة تخزين داخل مقر الجمعية، مثل الأقراص الصلبة أو خوادم الملفات المحلية.
- النسخ الاحتياطي السحابي: يتم استخدام منصات النسخ الاحتياطي السحابية لحفظ البيانات على الإنترنت، مثل خدمات Google Drive ، Microsoft OneDrive ، Dropbox ، أو خدمات سحابية متخصصة لتخزين النسخ الاحتياطية.
- نسخ احتياطي مشفر: لضمان أمان البيانات، يجب أن تكون النسخ الاحتياطية مشفرة لحمايتها من التلاعب أو الوصول غير المصرح به.

4. إجراءات الاستعادة:

- يجب على الجمعية توفير آلية لاستعادة البيانات بسرعة وكفاءة في حال حدوث فقدان للبيانات.
- يجب اختبار عملية الاستعادة بشكل دوري لضمان فعاليتها.
- يتم تخصيص موظفين مسؤولين عن متابعة عملية استعادة البيانات في حالات الطوارئ.

5. تخزين البيانات:

- التخزين المادي: يتم تخزين النسخ الاحتياطية في مكان آمن داخل مقر الجمعية أو في مستودعات تخزين خاصة لحمايتها من التلف أو السرقة.
- التخزين السحابي: يتم تخزين النسخ الاحتياطية في بيئة سحابية تتمتع بمستويات عالية من الأمان والموثوقية.
- يجب التأكد من أن جميع البيانات المخزنة على أجهزة محلية أو سحابية محمية بكلمات مرور قوية وتكنولوجيا تشفير لضمان أمان البيانات.

6. إجراءات الأمان للنسخ الاحتياطي:

- التحكم في الوصول: يجب أن يكون الوصول إلى النسخ الاحتياطية محصوراً فقط للأفراد المعتمدين الذين لديهم صلاحيات الوصول اللازمة.
- الرقابة والمراجعة: يجب أن تتم مراقبة الوصول إلى النسخ الاحتياطية بشكل مستمر ومراجعة الأنشطة المتعلقة بالنسخ الاحتياطي بانتظام للتأكد من عدم وجود اختراقات أو انتهاكات.



- الحماية ضد الفيروسات والهجمات الإلكترونية: يجب على النظام المستخدم للنسخ الاحتياطي أن يكون محميًا ضد الفيروسات والهجمات الإلكترونية من خلال تثبيت برامج مكافحة الفيروسات والتأكد من تحديثها بانتظام.

7. الاحتفاظ بالنسخ الاحتياطية القديمة:

- الاحتفاظ بالنسخ الاحتياطية الشهرية: يجب أن تحتفظ الجمعية بالنسخ الاحتياطية الشهرية لفترة لا تقل عن 12 شهرًا لضمان إمكانية الوصول إلى البيانات القديمة في حالة الضرورة.
- تحديد مدة الاحتفاظ: يتم تحديد مدة احتفاظ النسخ الاحتياطية بناءً على طبيعة البيانات (المالية، القانونية، التقنية)، ووفقًا لسياسات الجمعية ومتطلبات القوانين المحلية.
- يتم حذف النسخ الاحتياطية القديمة بعد انتهاء المدة المحددة وفقًا لإجراءات الحذف الآمنة.

8. التدريب والتوعية:

- يجب أن يتم تدريب الموظفين المعنيين بعملية النسخ الاحتياطي بشكل دوري لضمان أنهم على دراية بالإجراءات الصحيحة والممارسات الجيدة في إدارة النسخ الاحتياطي.
- يجب توعية الموظفين بأهمية النسخ الاحتياطي وضرورة اتباع الإجراءات المحددة لضمان حماية البيانات الحيوية.

9. التقييم والمراجعة:

- يجب تقييم فعالية سياسة النسخ الاحتياطي والتخزين بشكل دوري من خلال مراجعة الإجراءات المتبعة، وتحديد ما إذا كانت هناك حاجة لتحديث أو تعديل الإجراءات لتواكب التطورات التكنولوجية أو الاحتياجات التنظيمية.

المسؤوليات:

- مدير قسم تكنولوجيا المعلومات: المسؤول عن تنفيذ السياسة وتنسيق عملية النسخ الاحتياطي والتأكد من تنفيذها وفقًا للمعايير المحددة.
- الموظفون المعنيون: يجب أن يتبع الموظفون المعنيون إرشادات النسخ الاحتياطي والتخزين لضمان حماية البيانات.
- فريق الأمن: مسؤول عن تأمين النسخ الاحتياطية وحمايتها من أي تهديدات أمنية.

