وثيقة سياسة التخزين والاستبقاء بجامعة تبوك

تفاصيل الوثيقة

اسم المستند	وثيقة سياسة التخزين والاستبقاء بجامعة تبوك
المؤسسة	جامعة تبوك – عمادة تقنية المعلومات
مالك الوثيقة	مكتب إدارة البيانات
رقم الإصدار	1.0
الحالة	اصدار
تاريخ الإصدار	25-07-2023
التصنيف الأمني	داخلي

جدول اعتماد الوثيقة

الإصدار	التاريخ	التعديلات	تحرير	مراجعة	مو افقة
1.0	25-07-2023	لا يوجد	مكتب إدارة البيانات	25-07-2023	مدير مكتب إدارة البيانات

المو افقات

الاسم	الوظيفة	التاريخ	التوقيع
د. محمد العتيبي	مدير مكتب إدارة البيانات	01-08-2023	

جدول المحتويات

التعريفات

المصطلح	التعريف
النسخ الاحتياطية	هي أحد الاصول الهامة للجامعة. جميع منسوبي عمادة تقنية المعلومات مسؤولين عن سلامة وصحة ودقة النسخ الاحتياطية التي تم إنشاؤها أو تخزينها أو استخدامها من قبل الجامعة، بغض النظر عن نوع الوسائط التي توجد عليها البيانات او شكلها (سواء اكانت الكترونية، او ورقية أو اشكال اخرى)
مسؤول النسخ الاحتياطي	يجب أن يكون لجميع الأنظمة المملوكة في الجامعة" مسؤول نسخ احتياطي " هو **مسؤول الجهة الأول أو من يوكل إليه المهمة** "
سعة التخزين	أكبر قدر من المعلومات والبيانات التي يمكن لجهاز الحاسوب ان يحتويها
استبقاء البيانات	هي سياسة أو بروتوكول المنظمة فيما يتعلق بحفظ البيانات لأغراض تنظيمية أو لأغراض الامتثال أو التخلص منها عند عدم الحاجة إليها
استرجاع البيانات	عملية استعادة البيانات الرقمية التي أصبح الوصول إليها غير متاح نتيجة لتلفها أو تخريبها أو حذفها وتختلف عملية الاسترجاع باختلاف مسببات فقدانها

المقدمة

استجابة لمبادرة مكتب إدارة البيانات الوطنية والمبادرات ذات الصلة بضرورة وضع سياسة التخزين والاستبقاء في الجهات الحكومية. قام مكتب إدارة البيانات في جامعة تبوك بتطوير سياسة التخزين والاستبقاء لإدارة دورة حياة بيانات الجهة، بالتوافق مع سياسات مكتب إدارة البيانات الوطنية في المملكة .

أهداف الوثيقة

تهدف وثيقة سياسة التخزين والاستبقاء في الجامعة الى توضيح قواعد عمل النسخ الاحتياطي واسترجاع البيانات ، والتحقق من حفظ جميع بيانات الجامعة الإلكترونية على وسائط آمنة بشكل منتظم لغرض استرجاعها عند الكوارث أو لأغراض التحقق والمقارنة ، وذلك لضمان استمرارية وجودة العمل .

نطاق تطبيق الوثيقة

- تنطبق هذه الوثيقة على :
  - كافة الجهات الإدارية بجامعة تبوك ، و كافة الأطراف المعنية بما في ذلك الشركاء في القطاع الخاص أو الشركات التابعة لهم .
  - نظم معالجة البيانات ونظم ضبط العمليات التي تحتوي أو تستخدم معلومات أو تسهيلات تعود ملكيتها للجامعة.
  - وتسري هذه السياسة على كافة الموظفين / المستخدمين الذين يعملون بصورة مباشرة أو غير مباشرة لدى الجامعة ،أو الجهات التابعة لها.
  - أي جهة تقوم بتنفيذ عمل نيابة عن الجامعة يتضمن استخدام الأصول المعلوماتية التابعة لها.

استراتيجية وثيقة سياسة التخزين والاستبقاء

- تعزيز مساهمة الجامعة في تحقيق الأهداف الاستراتيجية الوطنية لدليل البيانات.
- رفع مؤشرات الجامعة في مجال تخزين وحفظ البيانات.
- الالتزام بالسياسات والمعايير الوطنية الصادرة عن المكتب الوطني لإدارة البيانات والهيئة السعودية للبيانات والذكاء الاصطناعي.
- تشجيع استخدام سياسة التخزين والاستبقاء للحصول على حلول مبتكرة.

الأهداف الاستراتيجية لوثيقة سياسة التخزين والاستبقاء على مستوي الجامعة

- البدء بتحديد كلاً من :
  - شروط التخزين (النسخ الاحتياطي) التي تضمن حماية البيانات الخاصة بالجامعة .
  - فترات استبقاء البيانات الخاصة بالجهة بناء على نوعها ومستوى تصنيفها وقيمتها في الأعمال وكذلك المتطلبات القانونية.
  - قواعد لعمليات الحذف والإزالة بناء على نوع بيانات الجهة وتصنيفها.
  - الإجراءات المطلوبة في حالة الفقدان الدائم الغير مقصود لبيانات الجهة.

مدة صلاحية الوثيقة

- إن مدة صلاحية هذه الوثيقة هي 3 أعوام من تاريخ إصدارها، ويجب على مكتب إدارة البيانات مراجعة وتحديث هذه الوثيقة مرة واحدة على الأقل كل ثلاث سنوات ، أو يجوز أيضاً تحديثها فور حُدوث أي تعديلات أو تغييرات تَتَعلَّق بالمُتطلبات التشريعية والتنظيمية ذات العلاقة. ويتم تغيير رقم إصدار الوثيقة حال القِيام بأي تَعديل سواء كان جوهرياً أو ثانوياً. ويَنبغي اعتماد تلك التحديثات أو التعديلات من قِبل وحدة حوكمة البيانات.

الأدوار والمسئوليات

م	الدور	المسئوليات
١	عمادة تقنية المعلومات	- وضع الضوابط الإدارية ،التشغيلية ، المادية ، والتقنية المناسبة لعمليات الحفظ واسترجاع البيانات والتعامل معها ومعالجتها وفقاً لهذه السياسة . - تحقيق سلامة البيانات والأنظمة الحكومية المحفوظة والتأكد من تطبيق السياسات المتعلقة بذلك . - استخدام الأدوات الضامنة لتحقيق (سلامة البيانات) سواءً التي تم أتمتتها من خلال تحوير النماذج الورقية ، أو تلك البيانات التي تعد تعريفية لترابط قواعد البيانات في الأنظمة .
٢	مسؤول نسخ احتياطي	- حفظ النسخ الإحتياطية لمعلومات وبيانات الجامعة والبرمجيات بشكل دائم في مصادر داخلية/خارجية. - التحقق من قابلية النسخ المحفوظة للإسترداد بشكل كامل. - تصنيف عمليات الحفظ وربطها بكل نظام/قواعد بيانات. - تحديد عدد مرات تكرار حفظ النسخ الإحتياطية بحسب تصنيف أهمية المعلومات ووضع الحدود الدنيا لمدد الحفظ وعدد مرات التكرار. - الاحتفاظ بنسخة احتياطية واحدة صالحة كحد أدنى في بيئة آمنة بشكل دائم وخارج حدود الحرم الجامعي. - توثيق عمليات استعادة البيانات والتحقق منها بشكل دوري. - توثيق آليات طلب التحقق من صحة معلومات الواردة من الجهات ووضع النماذج الملائمة لذلك.
٣	مسؤول إدارة البيانات	المتابعة الدورية مع عمادة تقنية المعلومات ومسؤول النسخ الاحتياطي عن تنفيذ سياسات التخزين والنسخ الاحتياطي .
٤	إدارة الأمن السيبراني	التأكد من تطبيق لوائح الامن السيبراني في مجال تخزين البيانات .
٥	مدير مكتب إدارة البيانات	التأكد من تطبيق اللوائح والأنظمة مع الأطراف المعنية .

السياسة والإجراءات

يجب على عمادة تقنية المعلومات توفير الحد الأدنى للنسخ الإحتياطي في كافة الأنظمة التي تعمل عليها جهات الجامعة وهي:

- رمز/اسم نموذج الحفظ.
- حداثة البيانات.
- الإشارة إلى مصدرها الحقيقي أو إرفاق نسخة منه –في حال وُجِد-
- توصيف النسخة والنظام.
- ترقيم تسلسل النسخة.
- تقنين الوصولية لموقع حفظ النسخ.
- التحقق من سلامة إجراء الحفظ.
- التحقق بشكل دوري وعشوائي من إمكانية تطبيق نسخة إحتياطية على بيئة العمل.

الالتزام

على مسؤولي التطبيقات في عمادة تقنية المعلومات التأكد من موافقة آليات حفظ النسخ الإحتياطي للبيانات والبرامج مع هذه السياسات، وعلى أصحاب الصلاحية في عمادة تقنية المعلومات مراقبة عمليات الإدخال والمعالجة لكافة طلبات الحفظ والإسترجاع لتلك البيانات ، ويجب عليهم الوعي والامتثال لهذه السياسة وأن أي انتهاكات لهذه السياسة يمكن أن يؤدي إلى اتخاذ إجراءات تأديبية و / أو إجراءات قانونية.

الإجراءات القانونية لانتهاك سياسة التخزين والاستبقاء

وتضمن هذه الإجراءات التالي :

- حجب جميع الامتيازات الممنوحة للموظف .
- حجب الدخول للأنظمة الخاصة بالجامعة .
- جزاءات قد تكون مالية أو تأديبية .

معايير الإستثناء

عند الحاجة يمكن التقدم بطلبات الحصول على استثناءات بصورة رسمية إلى إدارة الجهة مع توضيح مسوغات الاستثناء والمزايا التي قد تنجم عنه على أن يتم الموافقة عليها من إدارة النظم والبرامج بعمادة تقنية المعلومات .