وثيقة سياسة التخزين والاستبقاء بجامعة تبوك

تفاصيل الوثيقة

اسم الوثيقة	سياسة التخزين والاستبقاء
جامعة تبوك	جامعة تبوك – وحدة حوكمة البيانات
مالك الوثيقة	وحدة حوكمة البيانات
رقم الإصدار	2.0
الحال ة	إصدار
تاريخ الإصدار	٢٠٢٤/١٠/٤ م
تصنيف الوثيقة	داخلي

جدول اعتماد الوثيقة

الإصدار	التاريخ	التعديلات	تحرير	مراجعة	موافقة
2.0	٢٠٢٤/١٠/٤ م	لا يوجد	د. عائشة عبد الله الحكمي مسؤول إدارة البيانات	د .محمد العطوي مسؤول الامتثال	د. محمد متعب العتيبي مشرف وحدة حوكمة البيانات

الموافقات

الاسم	الوظيفة	التاريخ	التوقيع
د. محمد متعب العتيبي	مشرف وحدة حوكمة البيانات	٢٠٢٤/١٠/٤ م	
اللجنة التنفيذية الدائمة لإدارة وحوكمة البيانات بالجامعة			

المحتوى

مقدمة

في عصر البيانات الرقمية، تُعتبر مسألة تخزين البيانات واستبقائها من الأمور الحيوية التي تساهم في ديمومة واستمرارية المؤسسات التعليمية والأكاديمية مثل جامعة تبوك. تتطلب العمليات التعليمية والبحثية والإدارية في الجامعات إدارة فعالة للبيانات لضمان الوصول السهل والآمن للمعلومات وحمايتها من الفقدان أو التلف. لذا، تأتي أهمية تطوير سياسة شاملة للتخزين والاستبقاء حتى تتوافق مع الاحتياجات الأكاديمية والقانونية للجامعة.

تهدف سياسة التخزين والاستبقاء إلى بناء وصيانة آليات تخزين تضمن حفظ البيانات بشكل آمن وموثوق، فضلاً عن مراعاة متطلبات استبقاء البيانات لفترات محددة تتوافق مع الأنظمة والقوانين المعمول بها. هذه السياسة ستغطي جوانب متعددة تشمل الحماية من الكوارث، التصنيف المناسب للبيانات بناءً على أهميتها وخصوصيتها، فترات الاحتفاظ المناسبة لكل نوع من البيانات، إضافة إلى إجراءات محددة للحذف الآمن عند انتهاء مدة الاستبقاء.

من خلال تنفيذ هذه السياسة، تضمن الجامعة تلبية لمعايير الامتثال والاعتمادية، وتحمي مواردها المعرفية، وتوفر بيئة أكاديمية داعم تحفز على الإبداع والابتكار، وتعزز من كفاءة وفعالية العمليات التعليمية والإدارية. وعلى هذا الأساس، تُبنى سياسة التخزين والاستبقاء بجامعة تبوك لتكون قادرة على مواكبة التحديات المستقبلية وضمان استدامة وحماية البيانات الجامعية.

لإعداد سياسة شاملة ومفصلة للتخزين والاستبقاء لإدارة دورة حياة البيانات في جامعة تبوك، يجب تغطية الجوانب الأربعة الأساسية بالتفصيل:

شروط التخزين والحماية من الكوارث

1.البنية التحتية للتخزين:

- موقع آمن، يخضع للمراقبة المستمرة، ولمواصفات مراكز البيانات المعتمدة.
- اتصال شبكي عالٍ الكفاءة، وبدائل لضمان استمرارية الوصول الآمن الموثوق للبيانات.
- خوادم ووسائط تخزين بمساحات ملائمة لحجم العمل المتوقع، وتقسيمات متوافقة مع المعايير المُثلى لعمل بيئات الخوادم الفيزيائية أو المادية.

- يجب تأسيس بنية تحتية آمنة لتخزين البيانات تضمن عدم فقدان البيانات تحت أي ظرف.
- استخدام تقنيات مثل RAID) مجموعة مستقلة من الأقراص غير مكلفة(التي توفر التحمل في الأعطال وتحسين الأداء.

2 .نسخ احتياطي واسترجاع:

- وجود خطة نسخ ومتابعة أعمال النسخ بشكل دوري.
- رفع نسخ احتياطية في مواقع جغرافية متعددة، آمنة.
- التحقق من كفاءة أنظمة النسخ الآلية
- تنفيذ نظام نسخ احتياطي دوري يضمن إمكانية استعادة البيانات بأكملها في حالة حدوث كارثة.
- توفر النسخ الاحتياطية في مواقع متعددة لضمان استمرارية العمل.

3 .تطبيقات الأمن السيبراني:

- التحقق من سلامة بيئة الحفظ وفحصها ومتابعة تحديثاتها بشكل مستمر
- استخدام الأمان المتعدد المستويات للحماية من الهجمات الإلكترونية والتسلل.
- تشفير البيانات أثناء النقل وفي حالة السكون لحماية خصوصية وسرية المعلومات.

خطوات تأسيس البنية التحتية

لتأسيس بنية تحتية آمنة لتخزين البيانات بشكل يضمن عدم فقدان البيانات تحت أي ظرف، يجب اتباع مجموعة من الاستراتيجيات والمعايير التقنية العالية. هنا أبرز الخطوات والتوصيات:

1 .تصميم تقني متعدد المستويات:

- اختيار الموقع، والمواد، والبرمجيات الملائمة لحجم أعمال المنظمة وضمان توافقيتها.
- التحقق من التراخيص المستخدمة للأنظمة والأجهزة.
- تجهيز أعمال الربط الشبكي لأجهزة البيانات واجراء اختبارات الأمان

- **تقنية RAID**: استخدام تقنيات مثل RAIDلضمان التحمل العالي في حالة فشل الأقراص. يقوم RAIDبتخزين البيانات على عدة أقراص، مما يسمح باسترجاع البيانات حتى في حالة تعطل أحد الأقراص.
- **التوزيع الجغرافي**: توزيع البيانات عبر موقعين أو أكثر يقلل من مخاطر فقدان البيانات بسبب الكوارث الطبيعية أو الأعطال المحلية.
- **التخزين المؤقت:SSD** و استخدام وحدات التخزين المؤقتة (cache) وأقراص SSD التي تقدم أداء أعلى وموثوقية في الوصول إلى البيانات.

2.النسخ الاحتياطي والاسترجاع:

- التحقق من سلامة النسخ الاحتياطية باستعادتها بشكل عشوائي دورياً
- التشفير على مستوى أنظمة التشغيل وأثناء نقل البيانات

- **نسخ احتياطية** دورية: تنفيذ سياسات نسخ احتياطي أوتوماتيكية ودورية تشمل كل البيانات الهامة.
- **استخدام نظام النسخ المتماثل :(Mirroring)** لتحقيق مزيد من الأمان، قد يستخدم نظام المحاكاة لتكرار البيانات بين مراكز البيانات المتعددة.

الأمان السيبراني:

- **تشفير البيانات :** تشفير البيانات خلال النقل وأثناء السكون لحماية البيانات من الوصول غير المصرح به.
- **حماية المحيط الشبكي :** استخدام جدران الحماية، نظم كشف التسلل والوقاية من التسلل لحماية البيانات من التهديدات الخارجية.
- **حماية بيئة الاستضافة:** التحقق بشكل دوري ومستمر من التحديثات البرمجية على الخوادم ومتابعة حالات التراخيص للأنظمة المستخدمة في الأجهزة أو البرمجيات

إدارة ومراقبة:

- **أدوات المراقبة:** استخدام أدوات مراقبة متقدمة لتتبع أداء النظام وأي تحركات مشبوهة قد تدل على محاولات اختراق أوفشل في الأنظمة.
- **تحديثات وترقيات دورية :** الحفاظ على النظام مُحدثًا بأحدث الترقيات الأمنية والبرمجية لمواجهة أحدث التهديدات الأمنية.

الاستعداد للكوارث:

- **خطط استرداد الأعمال (BDR):** تطوير خطط لاسترداد البيانات والأعمال يضمن استمرارية العمليات حتى في حال حدوث كوارث.
- **اختبار النظام :** إجراء اختبارات منتظمة لخطط الاستجابة للكوارث للتأكد من فاعلية الإجراءات المتخذة.

بتطبيق هذه الإجراءات، تستطيع جامعة تبوك إنشاء بنية تحتية آمنة لتخزين البيانات تضمن حماية البيانات والوصول السلس إليها تحت أي ظرف.

خطوات تنفيذ نظام النسخ الاحتياطي

لتنفيذ نظام نسخ احتياطي دوري فعال يضمن إمكانية استعادة البيانات بأكملها في حالة حدوث كارثة، يمكن اتباع الخطوات التالية لضمان توافر وحماية البيانات:

تحديد أنواع البيانات وأهميتها:

- قبل إعداد سياسة النسخ الاحتياطي، من الضروري تحديد البيانات الحيوية التي تحتاج إلى حماية، والبيانات التي يمكن استرجاعها من مصادر أخرى.
- تصنيف البيانات بناءً على أهميتها وحساسيتها لتحديد أولويات النسخ الاحتياطي.

اختيار الاستراتيجية المناسبة للنسخ الاحتياطي:

- **النسخ الاحتياطي الكامل :** تخزين نسخة كاملة من جميع الملفات والمعلومات في كل مرة يُجرى فيها النسخ الاحتياطي.
- **النسخ الاحتياطي الجزئي (التراكمي أو التفاضلي):** (تخزين البيانات التي تغيرت منذ آخر نسخة احتياطية كاملة أو جزئية.

.تحديد تواتر النسخ الاحتياطي:

- النظر في تواتر التحديثات والتغييرات على البيانات لتحديد تواتر النسخ الاحتياطي، مثلاً يوميًا، أسبوعيًا، أو شهريًا.
- استخدام النسخ الاحتياطي الأوتوماتيكي لضمان التنفيذ المنتظم والموثق دون الحاجة لتدخل بشري.

اختيار الأدوات والتقنيات المناسبة:

- استخدام برمجيات نسخ احتياطي معروفة وموثوقة تدعم الميزات والوظائف المطلوبة.
- الاعتماد على حلول تخزين موثوقة مثل الأقراص الصلبة، أنظمة التخزين المتصلة بالشبكة(NAS) ، أو الحلول السحابية.

تأمين ومراقبة النسخ الاحتياطي:

- تشفير النسخ الاحتياطية لحماية البيانات من الوصول غير المصرح به.
- مراقبة وفحص النسخ الاحتياطية بانتظام لضمان كفاءتها وقابليتها للتطبيق عند الحاجة.

تخزين النسخ الاحتياطية:

- تخزين النسخ الاحتياطية في مواقع جغرافية متعددة للحد من الخسائر في حالة الكوارث الطبيعية أو الحوادث.
- النظر في الحلول السحابية كخيار للنسخ الاحتياطي لتوفير مرونة وسهولة الوصول.
- متابعة مساحات التخزين وضمان توافرها في بيئات الحفظ.

إجراء اختبارات الاستعادة:

- تنفيذ اختبارات دورية لاستعادة البيانات من النسخ الاحتياطية لضمان فعالية النظام.
- تصحيح أي مشكلات تظهر خلال الاختبارات لضمان الجاهزية الكاملة للنظام.

بتطبيق هذه الخطوات، يمكن لجامعة تبوك إنشاء نظام نسخ احتياطي دوري موثوق يضمن الحفاظ على بياناتها واستعادتها بكفاءة في حال حدوث أي كارثة.

خطوات استرجاع البيانات

إنشاء خطة استرجاع البيانات يعتبر جزءًا أساسيًا من استراتيجية استمرارية الأعمال والاستجابة للكوارث. هذه الخطة تضمن قدرة جامعة تبوك على استعادة البيانات الحيوية واستئناف العمليات بسرعة بعد حدوث فقدان بيانات بسبب خلل تقني، هجوم سيبراني،أو كارثة طبيعية. إليك خطوات عملية لتطوير خطة فعالة لاسترجاع البيانات:

تحديد الأصول الحيوية:

- قم بتحديد أي البيانات والنظم هي الأكثر أهمية لتشغيل جامعة تبوك. هذا قد يشمل قواعد البيانات العميلية، الملفات المالية،والمستندات الإدارية.

تصنيف مستويات الاسترداد:

- صنف البيانات والنظم بناءً على الوقت اللازم لاستردادها)أهداف وقت الاسترداد(وبناءً على الحد الأقصى للبيانات التي يمكن فقدانها أثناء الانقطاع)أهداف نقطة الاسترداد(

ختيار الأدوات والتقنيات:

- استخدم أدوات وبرمجيات موثوقة للنسخ الاحتياطي واستعادة البيانات. اعتماد حلول النسخ الاحتياطي السحابي يمكن أن يوفر مرونة وإمكانية الوصول إلى البيانات من أي مكان.

توثيق الخطة:

- قم بتوثيق عملية استرجاع البيانات بدقة، بما في ذلك الخطوات اللازمة لاسترداد البيانات، والفرق المسؤولة، وأرقام التواصل للطوارئ.

إنشاء اتفاقيات مستوى الخدمة:

- قم بتطوير اتفاقيات مستوى الخدمة (SLAs) مع مقدمي الخدمة الذين يديرون البيانات في الخارج أو مزودي الخدمات السحابية، لضمان تلبيتهم لأهداف الاسترداد المحددة.

تدريب الفريق:

- تدريب الفريق المسؤول عن استرجاع البيانات. يجب أن يكون الفريق على دراية بالخطة ومدربًا على تنفيذها بسرعة وفعالية.

إجراء اختبارات منتظمة:

- اختبر الخطة بانتظام للتأكد من كفاءتها. يجب أن تكشف هذه الاختبارات عن أية نقاط ضعف في الخطة وتوفر فرصة لتحسينها.

صيانة ومراجعة الخطة:

- قم بمراجعة وتحديث خطة استرجاع البيانات بانتظام لضمان أنها تواكب التغيرات التكنولوجية والتوسع في البنية التحتية للمؤسسة وأي تغييرات في متطلبات الأعمال.

بتنفيذ هذه الإجراءات، تضمن جامعة تبوك قدرة على التعامل مع حوادث فقدان البيانات بكفاءة، مما يقلل من الأثر السلبي على العمليات

خطوات تطبيق الأمان السيبراني

لزيادة الأمان السيبراني وحماية البيانات من الهجمات الإلكترونية والتسلل، يمكن اتباع نهج الأمان المتعدد المستويات مع تشفير البيانات خلال النقل والسكون. هذه الممارسات تعزز من دفاعات جامعة تبوك ضد التهديدات السيبرانية وتضمن خصوصية وسرية المعلومات .

إليك كيف يمكن تحقيق ذلك:

استخدام الأمان السيبراني المتعدد المستويات:

الأمان المتعدد المستويات يعتمد على مبدأ "الدفاع المتعدد الطبقات"، حيث يتم تأمين البيانات عبر استخدام عدة طبقات من الأمان تعمل معًا لمواجهة التهديدات السيبرانية.

1. **الحماية على مستوى الشبكة:**
   - **جدران الحماية (Firewalls)** تُستخدم لمراقبة وتنظيم البيانات الداخلة والخارجة من الشبكة.
   - **أنظمة كشف التسلل (IDS) و أنظمة منع التسلل (IPS):** لتحديد ومنع الأنشطة الخبيثة.
2. **الحماية على مستوى الأجهزة والبرمجيات:**
   - **برمجيات مكافحة الفيروسات ومكافحة البرمجيات الخبيثة:** تشغيل تحديثات دورية لكشف وإزالة التهديدات.
   - **إدارة التصحيحات:** تطبيق التحديثات الأمنية للنظم والتطبيقات بانتظام.
3. **الحماية على مستوى البيانات:**
   - **تشفير البيانات:** استخدام تقنيات تشفير قوية لحماية البيانات (سيتم توضيحها أدناه).
   - **التحكم في الوصول:** تقييد الوصول إلى البيانات بناءً على دور المستخدم والحاجة إلى المعرفة.

تشفير البيانات أثناء النقل وفي حالة السكون:

التشفير هو أحد أهم أساليب الحماية التي تضمن أن البيانات، حتى لو تم اعتراضها، لا يمكن قراءتها بدون المفتاح المناسب.

1. **تشفير البيانات أثناء النقل:**
   - **SSL/TLS:** استخدام بروتوكولات تأمين طبقة النقل (SSL/TLS) لتشفير البيانات المنتقلة بين العملاء والخوادم.
   - **VPN:** استخدام شبكات خاصة افتراضية (VPN) لإنشاء قنوات آمنة لنقل البيانات بين المواقع المختلفة.
2. **تشفير البيانات في حالة السكون:**
   - **تشفير على مستوى القرص:** استخدام تشفير القرص الكامل لحماية البيانات المخزنة على الأجهزة.
   - **تشفير على مستوى البيانات:** استخدام تقنيات مثل TDE (تشفير البيانات الشفاف) في قواعد البيانات لتشفير البيانات داخل قواعد البيانات.

بتطبيق هذه الإجراءات مع التدريب المستمر والتوعية للمستخدمين والعاملين، يمكن تعزيز الأمان السيبراني للمؤسسة بشكل ملحوظ وحماية البيانات بكفاءة عالية.

فترات استبقاء البيانات

تطوير سياسات استبقاء البيانات الفعالة والحفاظ على تحديثها بشكل دوري هو جزء حاسم من إدارة المعلومات في أي مؤسسة. هذه السياسات تضمن الامتثال للقوانين المحلية والدولية وتحافظ على كفاءة العمليات بإزالة البيانات غير الضرورية. إليك كيف يمكن تحقيق ذلك:

تطوير سياسات استبقاء البيانات

الهدف من سياسات الاستبقاء هو تحديد مدة بقاء البيانات المخزنة استنادًا إلى أهميتها والمتطلبات القانونية.

1. تصنيف البيانات:
   - قم بتصنيف البيانات بناءً على نوعيتها، مثلاً البيانات المالية، البيانات الشخصية، البيانات الأكاديمية، إلخ.
   - حدد متطلبات الاحتفاظ الخاصة بكل فئة، مع مراعاة المتطلبات القانونية والتشغيلية.
2. وضع معايير الاحتفاظ:
   - قم بتحديد الفترة الزمنية للاحتفاظ بالبيانات لكل فئة. على سبيل المثال، الاحتفاظ بالسجلات المالية لمدة 7 سنوات.
   - حدد متى وكيف يجب حذف البيانات أو إتلافها بعد انتهاء فترة الاحتفاظ.
3. وضع إجراءات للمراجعة والمتابعة:
   - تحديد الأشخاص أو الإدارات المسؤولة عن تطبيق سياسات الاحتفاظ.
   - تحديد كيفية مراقبة تطبيق سياسات الاحتفاظ وإجراءات التدقيق الدوري.

استعراض وتحديث السياسات بانتظام

1. **مراجعة دورية:**
   - قم بإجراء مراجعات دورية لسياسات الاحتفاظ، عادة ما يكون ذلك سنويًا أو كلما حدث تغيير في القوانين ذات الصلة أو أنظمة الصناعة.
2. **تضمين التغييرات في القوانين والمعايير:**
   - تتبع التغييرات في القوانين المحلية والدولية التي قد تؤثر على متطلبات الاحتفاظ بالبيانات.
   - تحديث السياسات لتعكس أي تغيرات في المتطلبات القانونية أو تحسينات في الأمان وممارسات الخصوصية.
3. **التدريب والتوعية:**
   - تأكد من أن جميع الموظفين يفهمون سياسات الاحتفاظ بالبيانات وأهمية الامتثال لها.
   - قدم التدريبات اللازمة لضمان الامتثال الكامل لهذه السياسات.
4. **استخدام التقنيات:**
   - استخدام أنظمة إدارة البيانات المتقدمة لأتمتة عمليات الحذف والاستبقاء بشكل يضمن الامتثال السلس للسياسات المحدثة.

بتنفيذ هذه الخطوات، تستطيع جامعة تبوك الحفاظ على مستويات عالية من الامتثال وحماية المعلومات بكفاءة، مع تقليل المخاطر القانونية والتشغيلية المرتبطة بإدارة البيانات.

قواعد الحذف والإزالة

إنشاء وتنفيذ إجراءات آمنة وفعالة لحذف البيانات بعد انتهاء فترات الاستبقاء الملائمة وضمان أن البيانات المحذوفة لا يمكن استعادتها ،يتطلب تخطيطًا دقيقًا واستخدام تقنيات متخصصة، بالإضافة إلى الامتثال للمتطلبات التنظيمية. إليك كيفية تنفيذ ذلك:

تبني إجراءات موثقة وفعالة لحذف البيانات

1.توثيق الإجراءات

.وضع سياسة واضحة وموثقة لحذف البيانات تشمل الخطوات، المسؤوليات، والجداول الزمنية

.التأكد من أن هذه السياسات تتطابق مع متطلبات الامتثال والأمان للمؤسسة والصناعة

2. تعيين المسؤوليات

.تحديد أدوار ومسؤوليات واضحة لمن يجب أن ينفذ عمليات الحذف ومن يقوم بالتدقيق والمراقبة

3. اعتماد الأتمتة

.استخدام أنظمة معلومات تمكّن من تطبيق سياسات حذف البيانات بشكل أوتوماتيكي بعد انتهاء مدة الاحتفاظ المحددة

استخدام تقنيات حذف آمنة

- **التطهير** :(**Data Wiping**) استخدام برمجيات معتمدة لتطهير القرص الصلب بالكامل أو جزء محدد، مما يضمن عدم قدرة استعادة البيانات
- **التمزيق** :(**Shredding**) تمزيق البيانات، وهو محو الملفات وكتابة بيانات عشوائية فوقها عدة مرات لحجب أي آثار للبيانات الأصلية.
- **التحطيم الفيزيائي** (للأجهزة المتقاعدة(: استخدام تقنيات مثل الطحن، التفتيت، أو التدمير بالمغناطيس للتأكد من أن الأقراص الصلبة ووسائط التخزين الأخرى لا يمكن استخدامها أو استعادة البيانات منها

دمج متطلبات الامتثال التنظيمي

- **مراجعة اللوائح** :التأكد من معرفة وفهم جميع التزامات الامتثال القانونية والتنظيمية المطبقة على بيانات جامعة تبوك
- **تطبيق المعايير** :دمج متطلبات الامتثال كجزء من السياسات والإجراءات الرسمية للحذف
- **التدقيق والمراجعة** :تنظيم تدقيقات داخلية وخارجية بانتظام للتحقق من امتثال عمليات حذف البيانات للقوانين واللوائح

بتنفيذ هذه الخطوات بدقة، تستطيع المؤسسات ضمان إدارة فعالة وآمنة لعمليات حذف البيانات بعد انتهاء فترات استبقائها، مما يحمي جامعة تبوك من المخاطر القانونية ويضمن احترام خصوصية وأمان المعلومات

الإجراءات المطلوبة في حالة فقدان البيانا ت

للتعامل بفعالية مع حوادث فقدان البيانات وتقليل تأثيرها على العمليات الأكاديمية والإدارية للجامعة، من المهم تطوير وتنفيذ استراتيجيات محددة للتعامل مع الأزمات واسترداد البيانات. إليك خطة مفصلة لتحقيق ذلك:

الجزء الأول: التعامل مع فقدان البيانات

أ. تشكيل فريق استجابة للطوارئ:

1. **تحديد المسؤوليات:** تحديد أدوار ومسؤوليات الأعضاء الأساسيين في فريق الاستجابة للطوارئ، بما في ذلك مدير الإدارة العامة لتقنية المعلومات، ومدير إدارة الأمن السيبراني، مشرف وحدة حوكمة البيانات، مستشار قانوني.
2. **تدريب الفريق:** إجراء التدريبات الدورية لضمان استعداد الفريق للتعامل مع حوادث فقدان البيانات بكفاءة.

ب. إجراء تحليل السبب الجذري:

1. **جمع البيانات:** تحديد ما تم فقدانه، كيفية حدوث ذلك، والكشف عن الأخطاء أو الثغرات الأمنية التي ساهمت في الحادث.
2. **استخدام أدوات التحليل:** استخدام أدوات تحليل السبب الجذري مثل خمس لماذات، التحليل الإحصائي، أو رسم السمكة لفهم أعمق للجذور الأساسية للمشكلة.
3. **وضع توصيات:** تطوير توصيات لتحسين النظم، السياسات، والعمليات لمنع تكرار مثل هذه الحوادث.

الجزء الثاني: إعادة البناء بعد فقدان البيانات

أ. وضع خطط لاسترداد البيانات:

1. **استخدام النسخ الاحتياطية:** تأكد من أن النظام الحالي للنسخ الاحتياطي كافٍ وقادر على استعادة البيانات بسرعة وفعالية.
2. **قواعد البيانات المستعادة:** فحص وتحقق من سلامة البيانات المستعادة لضمان أنها لم تتأثر أو تتلف خلال الحادث.

2.1. استئناف العمليات:

- **خطة استمرارية الأعمال:** تفعيل خطة استمرارية الأعمال لضمان أقل تأثير على الأنشطة التعليمية والإدارية.
- **التواصل الفعّال:** إبقاء جميع الأطراف المعنية، بما في ذلك الطلاب والموظفين، مطلعين على الوضع وأي تدابير تم اتخاذها.

2.2. مراجعة وتعزيز الخطط:

- **تحليل الأداء:** بعد استئناف العمليات، قم بتحليل كيفية عمل خطة الاستجابة واسترداد البيانات.
- **تحديث الخطط:** تحديث خطط استجابة الطوارئ واسترداد البيانات بناءً على المعلومات المستخلصة من تحليل هذه الحادثة.

باتباع هذه الإجراءات، يمكن للجامعة تخفيض المخاطر والتأثير السلبي لفقدان البيانات والعمل على سرعة استعادة الأنظمة لضمان استمرارية العمليات الأكاديمية والإدارية بكفاءة وفعالية.

فريق الاستجابة والحوكمة لأمن البيانات بجامعة تبوك

في عالم يتزايد فيه الترابط الرقمي وتكثر فيه التهديدات السيبرانية، أصبح من الضروري ضمان حماية البيانات من خلال استراتيجيات فعالة ومدروسة. جامعة تبوك، مدركة لأهمية البيانات كأصول حيوية لعملياتها التعليمية والإدارية، قد أسست "فريق الاستجابة والحوكمة لأمن البيانات" لتعزيز الأمن، وضمان الامتثال، والحفاظ على سلامة البيانات الجامعية.

هذا الفريق هو العمود الفقري لإدارة البيانات والأمن السيبراني في الجامعة، مسؤول عن تطوير وتنفيذ وصيانة سياسات فعالة للتخزين، الاستبقاء، الإتلاف، واسترداد البيانات في حالات الطوارئ. مهمته تشمل الاستجابة السريعة لأي حوادث تتعلق بالبيانات، تحليل الأسباب الجذرية للحوادث لتجنب تكرارها، وضمان استمرارية العمليات الأكاديمية والإدارية بأقل تأثير ممكن.

بناءً على تقارب الخبرات والمهارات المتخصصة في تقنية المعلومات، الأمن السيبراني، حوكمة البيانات، والجوانب القانونية، يقدم هذا الفريق نموذجًا شاملاً للحفاظ على بيئة بيانات آمنة وصحية تدعم الابتكار والنمو المستدام في جامعة تبوك.

معايير الفريق:

1. **الكفاءة الفنية**: يجب أن يكون جميع أعضاء الفريق مدربين بشكل ملائم ومطلعين على أحدث التقنيات والمعايير التكنولوجية والأمنية.
2. **الاستجابة للطوارئ**: يجب أن يكون فريق الطوارئ قادراً على التجاوب بسرعة وفعالية في حالة حوادث فقدان البيانات أو تلفها.
3. **الامتثال للقوانين واللوائح**: يجب أن تكون أنشطة الفريق وسياساته متوافقة مع القوانين المحلية والدولية.
4. **التعاون والتنسيق**: القدرة على العمل مع بعضهم البعض ومع الأقسام الأخرى بفعالية.

الأدوار والمسؤوليات:

1. مدير الإدارة العامة لتقنية المعلومات:

- **المسؤوليات**: إدارة البنية التحتية التكنولوجية للجامعة، ضمان توفر وتأمين البيانات، والإشراف على تنفيذ سياسات التخزين والاستبقاء.
- **الدور**: القيادة الفنية لجميع العمليات التكنولوجية وضمان تكامل جهود الأمن السيبراني مع العمليات التكنولوجية.

2. مدير إدارة الأمن السيبراني:

- **المسؤوليات**: تطوير وتنفيذ الأمن السيبراني وسياسات الرد على الحوادث، حماية البيانات من الهجمات الإلكترونية ،والإشراف على التحقيقات الأمنية والامتثال.
- **الدور**: إنشاء تدابير الأمان والرصد الأمني لكشف ومنع حوادث الأمان.

3. مشرف وحدة حوكمة البيانات:

- **المسؤوليات**: تنظيم ومراقبة سير البيانات داخل الجامعة، إدارة سياسات البيانات ومعايير الجودة.
- **الدور**: التأكد من أن جميع البيانات تتوافق مع سياسات الاستبقاء والإتلاف وأن تكون البيانات دقيقة ومحدثة.

4. المستشار القانوني:

- **المسؤوليات** :تقديم الاستشارات القانونية بخصوص الامتثال للقوانين واللوائح المتعلقة بتخزين البيانات وحوكمتها، والدفاع القانوني في حالة المسائل المتعلقة بخروقات بيانات.
- **الدور** :ضمان أن تكون جميع السياسات والإجراءات متوافقة قانونيًا، وتقديم المشورة حول المخاطر القانونية وكيفية تجنبها.

التضمين:

تضمين عمليات التخزين، الاستبقاء، الإتلاف، والإجراءات المتعلقة باسترداد البيانات في سياسات وإجراءات شاملة يجب أن يشمل اتساقا وتنسيقًا بين هذه الدوائر والأدوار المختلفة، مع التركيز على الوقاية والاستجابة السريعة والفعالة لحماية أصول البيانات الجامعية.

خاتمة

في ختام تطوير سياسة التخزين والاستبقاء لجامعة تبوك، نؤكد على الأهمية البالغة لإدارة البيانات بطريقة فعالة وآمنة تضمن الحفاظ على سلامة وخصوصية المعلومات وتعزز من قدرة الجامعة على الامتثال للمتطلبات التنظيمية والقانونية المتغيرة. من خلال التخطيط الدقيق لشروط التخزين، فترات الاستبقاء الملائمة، الإجراءات المحكمة لحذف البيانات، واستراتيجيات فعّالة لإدارة البيانات في حالات الطوارئ، تقدم الجامعة نموذجًا يضمن الاستفادة القصوى من الموارد التكنولوجية لدعم أهدافها التعليمية والبحثية.

هذه السياسة ليست مجرد وثيقة تنظيمية، بل هي خارطة طريق حية يجب مراجعتها وتحديثها بانتظام للتكيف مع التطورات التكنولوجية الجديدة، المتطلبات القانونية، والتغيرات في بيئة عمل الجامعة. كما يجب التأكد من توفير التدريب المستمر للموظفين والطلاب لضمان الوعي والتزام الجميع بأفضل الممارسات في مجال رعاية البيانات وأمن المعلومات.

إن التزامنا بمتابعة إجراء النسخ الاحتياطي الفعّال، توفير الأمان المتعدد المستويات، وتطوير أنظمة استجابة سريعة وكفاءة في إدارة أية حوادث متعلقة بالبيانات، سيعزز من قدرة جامعة تبوك على مواجهة التحديات المستقبلية وإدارة أصولها الرقمية بأمان وثقة. تنفيذ هذه السياسات بنجاح يعد خطوة هامة نحو رفع الكفاءة الأكاديمية وتعزيز الشفافية والمسؤولية.