سياسة حماية البيانات بجامعة تبوك

V.1.0

تفاصيل الوثيقة

اسم المستند	سياسة حماية البيانات بجامعة تبوك
المؤسسة	جامعة تبوك
مالك الوثيقة	وحدة حوكمة البيانات
رقم الاصدار	1.0
الحالة	اصدار
تاريخ الإصدار	2024-05-15م
التصنيف الأمني	عام

جدول اعتماد الوثيقة

الاصدار	التاريخ	التعديلات	تحرير	مراجعة	موافقة
1.0	2024-05-15 م	لا يوجد	1. د. هيفاء عيد أبو شعيل مسؤول حماية البيانات الشخصية	د. حسين جائز العزيزي المسؤول القانوني	د. محمد متعب العتيبي مشرف وحدة حوكمة البيانات

الموافقات

الاسم	الوظيفة	التاريخ	التوقيع
د. محمد متعب العتيبي	مشرف وحدة حوكمة البيانات	2024-05-15 م	
اللجنة التنفيذية لحوكمة البيانات			---

قائمة المحتويات

1. المقدمة

تُمَثِّل هذه الوثيقة سياسة حماية البيانات الخاصة بجامعة تبوك والمشار إليها بالجامعة داخل هذه الوثيقة.

تتكوَّن هذه الوثيقة من تِسعة أقسام رئيسية لِتَشمل هذه المُقَدِمَة يليها الغَرض، والنطاق، والأدوار والمسؤوليات، وبنود السياسة، والمرجعيات، والالتزام، ومعايير الاستثناءات، وأخيراً المصطلحات، والتعريفات.

على جَمِيع المستخدمين القيام بالقراءة المُتأنِية والفهم الجيد والالتزام الكامل بسياسة حماية البيانات بجامعة تبوك. وفى حالة عدم وضوح أي من أجزاء هذه الوثيقة ، فإننا نامل التواصل مع وحدة حوكمة البيانات بالجامعة حتى يتسنى لنا مساعدتكم في ذلك.

تُعَدُ وحدة حوكمة البيانات بالجامعة هي المالكة لِتلك الوثيقة.

إن مدة صلاحية هذه الوثيقة هي 3 أعوام من تاريخ إصدارها، ويجب على وحدة حوكمة البيانات مراجعة وتحديث هذه الوثيقة مرة واحدة على الأقل كل عام، أو يجوز أيضاً تحديثها فور حُدوث أى تعديلات أو تغييرات تَتَعلَّق بالمُتطلبات التشريعية والتنظيمية ذات العلاقة. ويَتم تَغيير رقم إصدار الوثيقة حال القِيام بأى تَعديل سواء كان جوهرياً أو ثانوياً. ويَنبغي اعتماد تلك التحديثات أو التعديلات من قِبَلْ اللجنة الدائمة لحوكمة و إدارة البيانات بالجامعة.

2. الغرض

الغرض من هذه السياسة هو تحديد متطلبات حماية البيانات المتعلقة بالبيانات الخاصة بجامعة تبوك لتقليل المخاطر الناتجة عن التهديدات الداخلية والخارجية وذلك لتحقيق الأهداف الرئيسية للحماية وهي: سرية المعلومات، وسلامة أنظمة المعلومات، وتوافرها.

تمت موائمة هذه السياسة مع الضوابط والمعايير الصادرة من الهيئة الوطنية للأمن السيبراني والمتطلبات التنظيمية والتشريعية ذات العلاقة.

3. النطاق

تنطبق هذه الوثيقة على كافة الأصول المعلوماتية والتقنية والخدمات المقدمة، وكذلك كافة مستخدميها من الموظفين سواء كانوا يعملون بصفة دائمة أو مؤقتة، أو يعملون بدوام كامل أو دوام جزئي، أو متعاقدين كموظفي شركات الإسناد الخارجي. وكذلك مستخدمي وموظفي جميع الأطراف الخارجية كالمقاولين والموردين والشركات الاستشارية والجهات الحكومية وشركات الخدمات المُدارة والشركات والجهات الخاصة بالاستضافة والحوسبة السحابية وغيرها.

4. الأدواروالمسؤوليات

1- **اعتماد السياسة:** اللجنة الدائمة لإدارة وحوكمة البيانات

2- **مراجعة السياسة وتحديثها:** وحدة حوكمة البيانات.

3- **تنفيذ السياسة وتطبيقها:** الإدارة العامة لتقنية المعلومات وإدارة الأمن السيبراني ووحدة حوكمة البيانات.

4- **قياس الالتزام بالسياسة:** وحدة حوكمة البيانات.

5. بنود السياسة

1- البنود العامة

1-1 يجب أن تلتزم الجامعة بالمتطلبات التشريعية والتنظيمية المتعلقة بحماية البيانات في المملكة العربية السعودية، والسياسات والإجراءات المتبعة في جامعة تبوك.

2-1 يجب أن تحدد الجامعة وتحدث متطلبات الأمن السيبراني للبيانات بشكل دوري.

3-1 يجب على الجامعة ضمان إدارة متطلبات الأمن السيبراني للبيانات بكفاءة وفقًا لسياسة الأمن السيبراني في الموارد البشرية وسياسة إدارة الأصول الخاصة ب جامعة تبوك.

4-1 يجب أن تضمن الجامعة حماية الأجهزة المحمولة وفقًا لسياسة أمن الأجهزة المحمولة في الجهة.

5-1 يجب أن تستخدم الجامعة تقنيات وحلول منع تسريب البيانات.

6-1 يحظر استخدام بيانات الجامعة في أي بيئة غير بيئة الإنتاج، إلا بعد إجراء تقييم للمخاطر وتطبيق الضوابط لحماية تلك البيانات، مثل: تقنيات تعتيم البيانات (masking) أو تقنيات مزج البيانات (data scrambling).

7-1 يجب أن تحدد الجامعة التقنيات والأدوات والإجراءات لإتلاف البيانات بطريقة آمنة حسب مستوى التصنيف.

8-1 يجب أن تعمل الجامعة على إعداد وتنفيذ استراتيجية واضحة للخروج من الخدمات السحابية لضمان الإتلاف الآمن للبيانات عند إنهاء أو انتهاء سريان العقد مع مقدم الخدمة السحابية.

9-1 يجب أن تضمن الجامعة الاستخدام المناسب والفعال لتقنيات التشفير لحماية بيانات جامعة تبوك وفقًا لسياسة ومعايير التشفير في جامعة تبوك والمتطلبات التشريعية والتنظيمية ذات العلاقة.

10-1 يجب على الجامعة تحديد الأدوار والمسؤوليات للأمن السيبراني لضمان ان البيانات متوافقة مع المتطلبات القانونية والتنظيمية.

11-1 يجب أن تستخدم الجامعة طريقة آمنة لاستخراج ونقل البيانات واستخراج ونقل البنية التحتية الافتراضية.

12-1 يجب أن تمنع الجامعة نقل أي بيانات للأنظمة الحساسة من بيئة الإنتاج إلى أي بيئة أخرى.

13-1 يجب أن تستخدم الجامعة خاصية العلامات المائية (watermark feature) لترميز الوثيقة بأكملها عند إعدادها، أو تخزينها، وطباعتها، او عرضها على الشاشة، والتأكد من احتواء كل نسخة من الوثيقة على رقم يمكن تتبعه.

14-1 يجب قياس مؤشرات الأداء الرئيسية (KPI) للتأكد من التحسين المستمر لمتطلبات الأمن السيبراني لحماية البيانات.

2- التصنيف والتعامل الآمن مع المعلومات

1-2 يجب تصنيف بيانات الجامعة وفقًا لسياسة تصنيف الأصول وترميزها المعتمدة في جامعة تبوك.

2-2 يجب تصنيف جميع بيانات الجامعة في كل الصيغ التالية:

1-2-2 الصيغ الرقمية (مثل وثائق برنامج معالج النصوص "Word"، وجداول البيانات "Spreadsheets"، وقواعد البيانات).

2-2-2 الاتصالات الإلكترونية (مثل رسائل البريد الإلكتروني وخدمات الاتصالات الصوتية والمؤتمرات والاتصالات الهاتفية وغيرها)

3-2-2 الصيغ المادية (مثل المطبوعات، والنسخ الورقية للعقود ودفاتر الملاحظات).

4-2-2 المحادثات الشفهية (مثل الاجتماعات والمقابلات).

3-2 يجب أن يتجنب العاملون مناقشة بيانات جامعة تبوك بصيغة شفهية في المناطق العامة، أو في مناطق قد تُسمع فيها مناقشاتهم. ويجب أن تتم المناقشات في مقرات جامعة تبوك وفي مواقع آمنة ضمن المقرات.

4-2 يجب تصنيف جميع البيانات التي تحتفظ فيها جامعة تبوك في كل الأنظمة (بما في ذلك الأنظمة الحساسة وأنظمة الحوسبة السحابية) وترميزها وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة، وسياسة تصنيف الأصول وترميزها المعتمدة في جامعة تبوك.

5-2 يجب أن يتولى المسؤولون عن البيانات، الذين عينتهم جامعة تبوك للعمل مع الأطراف المعنية ذات العلاقة مع جامعة تبوك، مسؤولية تصنيف الأصول وترميزها على النحو الوارد في هذه السياسة.

6-2 يجب إبلاغ وحدة حوكمة البيانات في جامعة تبوك على الفور عن أي مخالفة لهذه السياسة ولضوابط تصنيف البيانات من خلال النظام الإلكتروني المخصص لذلك.

7-2 يجب تطبيق ضوابط الوصول عن بُعد للبيانات وفقًا لنموذج سياسة العمل عن بعد المعتمدة في جامعة تبوك.

8-2 يجب عدم حفظ البيانات المصنفة (سرية، سرية للغاية) في أجهزة تخزين محمولة مثل الأقراص الصلبة الخارجية أو وحدات التخزين "USB"، بغض النظر عن مستوى التشفير المستخدم في جهاز التخزين المحمول.

9-2 يجب عدم إدخال أو معالجة أو تغيير أو حفظ أو نقل البيانات المصنفة (سرية، وسرية للغاية) إلى الأجهزة التي يملكها الموظفون، والتي يُطلق عليها استخدام الأجهزة الشخصية للعاملين في الجهة (BYOD)، ما لم تكن تلك البيانات خاصة بالموظفين.

10-2 يجب حماية البيانات المصنفة (سرية، وسرية للغاية) التي يمكن الوصول إليها أو معالجتها أو حفظها أو نقلها من خلال أنظمة الدخول عن بعد، ما لم تكن تلك البيانات خاصة بالموظفين.

11-2 يجب تحديد المجموعات الفرعية من البيانات المصنفة (مثل سرية، وسرية للغاية)، التي يمكن الوصول إليها أو معالجتها أو حفظها أو نقلها من خلال أنظمة العمل عن بُعد، وفقًا للمتطلبات التنظيمية ذات العلاقة.

12-2 يجب ألّا تحتوي الأصول التقنية لإدارة حسابات مواقع التواصل الاجتماعي لجامعة تبوك على بيانات مصنفة، وفقًا للمتطلبات التنظيمية ذات العلاقة.

3- الاحتفاظ بالسجلات

1-3 يجب أن تحتفظ جامعة تبوك بالسجلات المعتمدة المقدمة من ملاك البيانات، ويجب أن تحتفظ بسجلات سحب أو إلغاء الموافقات لفترة زمنية محددة وفقًا للمتطلبات التشريعية والتنظيمية.

2-3 يجب أن تحتفظ جامعة تبوك بسجل لجميع عمليات الإتلاف الآمن للبيانات التي تم تنفيذها.

3-3 يجب أن تحتفظ جامعة تبوك بالبيانات طوال المدة المحددة وفقًا للمتطلبات التشريعية والتنظيمية أو عندما تصبح البيانات الحساسة غير مطلوبة للغرض الذي جمعت من أجله.

4-3 يجب أن تُنشئ جامعة تبوك سجل بأنشطة المعالجة وتحدثه عند الحاجة مع الاحتفاظ بنسخ طوال المدة المحددة وفقًا للمتطلبات التشريعية والتنظيمية.

5-3 يجب تحديد فترة الاحتفاظ بجميع البيانات المتعلقة بالأنظمة وفقًا للتشريعات ذات العلاقة، والاحتفاظ فقط بالبيانات المطلوبة في بيئة الإنتاج.

6. التحديث والمراجعة

يجب على إدارة الأمن السيبراني مراجعة السياسة مرة واحدة سنويا على الأقل أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في جامعة تبوك أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

7. الالتزام بالسياسة

1- يجب على إدارة الأمن السيبراني التأكد من التزام جامعة تبوك بهذه السياسة دوريًا.

2- يجب على جميع العاملين في جامعة تبوك الالتزام بهذه السياسة.

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة تبوك.