سياسة جامعة تبوك في إدارة الأنظمة الالكترونية

V.1.0

تفاصيل الوثيقة

اسم الوثيقة	سياسة جامعة تبوك في إدارة الأنظمة الإلكترونية
المؤسسة	جامعة تبوك – وحدة حوكمة البيانات
مالك الوثيقة	وحدة حوكمة البيانات
رقم الإصدار	1.0
الحالة	إصدار
تاريخ الإصدار	٢٠٢٤/٧/٣١ م
تصنيف الوثيقة	داخلي

جدول اعتماد الوثيقة

الإصدار	التاريخ	التعديلات	تحرير	مراجعة	موافقة
1.0	٢٠٢٤/٧/٣١ م	لا يوجد	أ. عبد الله العطوي مدير إدارة وحدة حوكمة البيانات	د. حسين العزيزي المسؤول القانوني	د. محمد متعب العتيبي مشرف وحدة حوكمة البيانات

الموافقات

الاسم	الوظيفة	التاريخ	التوقيع
د. محمد متعب العتيبي	مشرف وحدة حوكمة البيانات	٢٠٢٣/٨/٣٠ م	
اللجنة التنفيذية الدائمة لإدارة وحوكمة البيانات بالجامعة			

١ المحتويات

٢ التعريفات ٤

3 مقدمة ٥

4 الغرض ٥

5 النطاق ٥

6 بنود السياسة ٦

6.1 المبادئ الرئيسية لمشاركة البيانات ٦

6.1.1 المبدأ الأول: تعزيز ثقافة المشاركة ٦

6.1.2 المبدأ الثاني: مشروعية الغرض ٦

6.1.3 المبدأ الثالث: الوصول المصرح به ٦

6.1.4 المبدأ الرابع: الشفافية ٧

6.1.5 المبدأ الخامس: المسؤولية المشتركة ٧

6.1.6 المبدأ السادس: أمن البيانات ٧

6.1.7 المبدأ السابع: الاستخدام الأخلاقي ٧

7 الأدوار والمسؤوليات داخل جامعة تبوك وخارجها وإمكانية الوصول واستخدام أنظمة الجامعة الالكترونية ٧

٧,١ الجهة المالكة للبيانات (Data Steward) ٧

7.2 مستخدمي النظام داخلي Internal system users ٩

7.3 مستخدمي النظام خارجي external system users ٩

٨ الجهات المساندة ٩

٨,١ إدارة تقنية المعلومات IT ٩

٨,٢ إدارة الامن السيبراني ١٠

٨,٣ وحدة حوكمة البيانات ١٠

9 المرجعيات ١٣

٢ التعريفات

المصطلح	التعريف
منسوبي الجامعة	جميع من ينتمي الى جامعة تبوك من الموظفين، أعضاء هيئة التدريس، والإداريين، والتقنيين سواء كانوا يعملون بصفة دائمة أو مؤقتة أو يعملون بدوام كامل أو دوام جزئي أو متعاقدين كمتعاقدي شركات الإسناد الخارجي.
البيانات	مجموعة من الحقائق في صورتها الأولية أو في صورة غير منظمة مثل الأرقام أو الحروف أو الصور الثابتة أو الفيديو أو التسجيلات الصوتية أو الرموز التعبيرية أو الأدلة التنظيمية والاجرائية أو الوثائق أو المخطوطات.
البيانات المحمية	البيانات المصنفة على أنها (سري للغاية، سري، مقيد)
مدير النظام الالكتروني	كل شخص له صلاحية إدارة أحد الأنظمة الالكترونية بجامعة تبوك، هو مسؤولا عن تخويل المستخدمين حق الوصول لأنظمة الجامعة حسب تصنيف وثيقة مجموعات المستخدمين للنظام .
الجهة المالكة للبيانات (Data Steward)	كأصل مالك للبيانات هي الجامعة - جهة عامة و تحكم - و الإدارة أو العمادة(جهة معالجة) التي تم بناء و تطوير نظاما الكترونيا ليلبي احتياجاتها حسب متطلبات العمل.
مستخدم النظام الالكتروني الداخلي	هو الموظف أو المتعاقد من داخل الجامعة الذي يمنح صلاحية الوصول لبيانات أحد الأنظمة حسب تصنيف وثيقة مجموعات المستخدمين .
مستخدم النظام الالكتروني الخارجي	هو شخص من خارج الجامعة يمنح صلاحية الوصول لبيانات أحد الأنظمة حسب تصنيف وثيقة مجموعات المستخدمين .
أصحاب المصلحة	جميع المستفيدين من الخدمات التي يتم تقديمها من خلال الأنظمة الالكترونية بجامعة تبوك

٣ مقدمة

تمثل هذه الوثيقة سياسة إدارة الانظمة الالكترونية بجامعة تبوك والمشار إليها بالجامعة داخل هذه الوثيقة. تتكون هذه الوثيقة من أقسام رئيسية لِتَشمل المصطلحات والتعريفات، المُقَدِمَة، الغَرض، والنطاق، والأدوار والمسؤوليات، وبنود السياسة، والمرجعيات، والملحقات.

تؤكد هذه الوثيقة على جَمِيع المستخدمين والمستفيدين القراءة المُتأنِية والفهم الجيد والالتزام الكامل بما تحويه وثيقة سياسة إدارة الانظمة الالكترونية بجامعة تبوك. **تعَدُ وحدة حوكمة البيانات بالجامعة هي ممثل المالك لهذه الوثيقة.**

سريان مدة هذه الوثيقة ٣ أعوام من تاريخ إصدارها. ويجب على وحدة حوكمة البيانات مراجعتها وتحديثها كل ما دعت الحاجة لذلك من تغيرات للأنظمة واللوائح والسياسات المرتبطة. ويَتم تَغيير رقم إصدار الوثيقة حال القِيام بأي تَعديل سواء كان جوهرياً أو ثانوياً. ويَنبغي اعتماد تلك التحديثات أو التعديلات من قِبَلْ وحدة حوكمة البيانات.

٤ الغرض

تهدف هذه السياسة إلى حوكمة الأنظمة الإلكترونية داخل الجامعة وتوحيد الجهود المبذولة وتحقيق أعلى معايير الامتثال بين جهات الجامعة الداخلية والجهات الخارجية لمنع وقوع التعارض في معالجة البيانات وحفظها وتنظيم إطلاع المستفيدين والموظفين والمسؤولين وأصحاب المصلحة على المعلومات والحصول عليها بكافة أشكالها من أنظمة الجامعة الالكترونية لأسباب إدارية وتنظيمية وخدميه.

٥ النطاق

تنطبق هذه السياسة على جميع المسؤولين و الموظفين و المتعاقدين بما تقتضيه مصلحة العمل من منحهم من صلاحيات لاستخدام أنظمة الجامعة الالكترونية و الاطلاع على البيانات التي توفرها تلك الأنظمة أيا كان مستوى تصنيفها و فق الضوابط و التي تنتجها جهات الجامعة مهما كان مصدرها، أو شكلها أو طبيعتها – ويشمل ذلك السجلات الالكترونية ورسائل البريد الإلكتروني والمعلومات المخزنة إلكترونياً، أو أشرطة الصوت أو الفيديو أو الخرائط أو الصور الفوتوغرافية أو المخطوطات أو الوثائق المكتوبة بخط اليد، أو أي شكل آخر من أشكال المعلومات المسجلة او المعالجة من قبل الجامعة أو التي تنتجها أنظمة الجامعة الالكترونية.

٦ بنود السياسة

٦,١ المبادئ الرئيسية لمشاركة البيانات

٦,١,١ المبدأ الأول: تعزيز ثقافة المشاركة

١. على جميع الجهات داخل الجامعة مشاركة البيانات الرئيسية التي تنتجها وذلك لتحقيق التكامل بين الجهات لتحقيق مبدأ الحصول على البيانات من مصادرها الصحيحة والحد من ازدواجيتها وتعارضها وتعدد مصادرها وعدم حداثتها.

٢. في حال تم طلب البيانات من غير مصدرها الأساسي، فعلى الجهة – المطلوب منها مشاركة هذه البيانات – تحويل الطلب لوحدة حوكمة البيانات.

٣. لا يحق لأي جهة لا تملك صلاحيات البيانات مشاركتها مع أي جهات أخرى داخليا أو خارجياً.

٤. لا يحق لأي فرد من منسوبي الجامعة مشاركة البيانات ما لم يكون مخولا بذلك، إلا في حال كانت البيانات مصنفة في مستوى "عام".

٦,١,٢ المبدأ الثاني: مشروعية الغرض

تستند هذه السياسة لإدارة الأنظمة الإلكترونية بجامعة تبوك على الأنظمة والتشريعات واللوائح التنظيمية والتنفيذية المعنية في هذا الجانب والمشرعة لهذا الغرض المشروع والامتثال الكامل لذلك. وهو تحديد مشارك البيانات لأغراض مشروعة مبنية على أساس نظامي أو احتياج عملي مسوغ يهدف إلى تحقيق مصلحة عامة دون إلحاق أي ضرر بالمصالح الوطنية، أو أنشطة الجهات، أو خصوصية الأفراد وجميع أنشطة الجامعة.

٦,١,٣ المبدأ الثالث: الوصول المصرح به

أن تكون لدى جميع الأطراف المشاركة في تبادل البيانات ومشاركتها صلاحية الاطلاع على البيانات والحصول عليها واستخدامها، بالإضافة إلى المعرفة، والمهارة للأشخاص المؤهلين والمدربين على كيفية التعامل مع البيانات المشتركة.

٦,١,٤ المبدأ الرابع: الشفافية

يجب على جميع الأطراف المشاركة في عمليات تبادل البيانات ومشاركتها، إتاحة جميع المعلومات الضرورية لتبادل البيانات بما في ذلك: البيانات المطلوبة، الغرض من جمعها، ووسائل نقلها، وطرق حفظها، والضوابط المستخدمة لحمايتها وآلية التخلص منها.

٦,١,٥ المبدأ الخامس: المسؤولية المشتركة

أن تكون جميع الأطراف المشتركة في تبادل البيانات ومشاركتها مسؤولة مسؤولية كاملة عن قرارات مشاركة البيانات ومعالجتها وفقا للأغراض المشروعة نظاما والمحددة. وضمان تطبيق الضوابط الأمنية للأمن السيبراني وتبادل البيانات المنصوص عليها في اتفاقية مشاركة البيانات والأنظمة والتشريعات والسياسات ذات العلاقة.

٦,١,٦ المبدأ السادس: أمن البيانات

تلتزم جميع الأطراف المشاركة في تبادل البيانات ومشاركتها بتطبيق الضوابط الأمنية للأمن السيبراني لحماية البيانات ومشاركتها في بيئة آمنة وموثوقة وفقاً للأنظمة والتشريعات ذات العلاقة ووفقا لما تنص عليه لوائح وسياسات إدارة الأمن السيبراني بجامعة تبوك.

٦,١,٧ المبدأ السابع: الاستخدام الأخلاقي

تلتزم جميع الأطراف المشاركة في تبادل البيانات ومشاركتها بتطبيق الممارسات الأخلاقية خلال تشارك البيانات لضمان استخدامها في إطار من العدالة والنزاهة والأمانة والاحترام، وعدم الاكتفاء بالتزام سياسات إدارة الأمن السيبراني أو الالتزام بالمتطلبات التنظيمية والتشريعية ذات العلاقة.

٧ الأدوار والمسؤوليات داخل جامعة تبوك وخارجها وإمكانية الوصول واستخدام أنظمة الجامعة الالكترونية

٧,١ الجهة المالكة للبيانات (Data Steward)

كأصل مالك للبيانات هي الجامعة (جهة عامة وتحكم).

هي جهة المعالجة التي تلتزم بتطبيق اللوائح والمهام وتمثل السلطة العليا بالجهة وهي المسؤول الأول بالجهة والممثل الرسمي للجهة، ومن مهامه الاتي:

[١]. التأكد من صحة وسلامة البيانات (جودة البيانات) التي يحتويها النظام والعمل على رفع جودة البيانات حسب دليل جودة البيانات المعتمد من وحدة حوكمة البيانات.

[٢]. الالتزام بسياسات جامعة تبوك في حماية البيانات الشخصية ومشاركة البيانات حسب دليل نظام حماية البيانات الشخصية ودليل سياسة جامعة تبوك لمشاركة البيانات والمتوفرة على صفحة وحدة حوكمة البيانات.

[٣]. منح الاذن بالوصول للنظام:

أ- منح الاذن بالوصول للمستخدمين و المستفيدين حسب الصلاحيات المخولة لهم في وثيقة تصنيف مجموعات المستخدمين و المستفيدين للنظام بعد تقديم طلب الاذن بالوصول حسب النموذج المعد لذلك.

ب- المدة الزمنية الممنوحة للوصول للنظام مقيدة بعام دراسي كامل كحد أقصى.

ت- تقدير صلاحيات الوصول للبيانات من مهام مدير النظام الإلكتروني وفقاً لهذه الوثيقة.

[٤]. المتابعة والمراجعة

١. متابعة الجهة للالتزام بسياسات وحوكمة البيانات الشخصية بجامعة تبوك.

٢. المراجعة الدورية لمستخدمي النظام وتحديث بياناتهم وأذونات الوصول بصفة دورية وتزويد وحدة حوكمة البيانات بالتقرير اللازمة حول ذلك.

[٥]. المراقبة:

١. مراقبة الأنشطة التي تتم على النظام من خلال رصدها وقيدها، بما في ذلك النشاطات المتعلقة بالشخص الذي يصل إلى هذه البيانات.

٢. اشعار وحدة حوكمة البيانات في حال وجود انشطة مشبوهة وتجاوزات من مستخدمي النظام أو إساءة استخدام بيانات النظام.

[٦]. إيقاف الاذن بالوصول للنظام:

١. يجب على مدير النظام أو من يفوضه إغلاق حسابات المستخدمين بعد انتهاء المدة المستحقة للوصول للبيانات واشعارهم بذلك.

٢. في حال انتهاء التكليف والصلاحية لممثل أحد جهات الجامعة في النظام الالكتروني فيجب إيقاف حسابه بعد اشعار الجهة بانتهاء صلاحية الوصول لممثلهم على النظام، واشعارهم بطلب التجديد او تكليف ممثل جديد.

٣. وفي حال رصد وقيد مخالفة وتجاوزات مشبوهة من أحد المستخدمين أو المستفيدين قبل إنتهاء صلاحيات الوصول لأنظمة الجامعة، يجب على مدير النظام إيقاف إذن الوصول للبيانات.

٤. وفي حال إيقاف إذن الوصول للمخالف يجب إشعار وحدة حوكمة البيانات لاتخاذ الازم حيال ذلك.

٧,٢ مستخدمي النظام داخلي Internal system users

يتبع الإجراءات التالية:

١. تقديم طلب رسمي حسب النموذج المعد ذلك لإضافته مستخدم على النظام.
٢. على الجهة المستفيدة الرفع بمرشحيها الممثلين لها على النظام وفق النماذج المعد لذلك لجهة وحدة حوكمة البيانات.
٣. الالتزام بنظام حماية البيانات الشخصية بجامعة تبوك و جميع السياسات و اللوائح ذات الصلة.
٤. يلتزم المستخدم بإتباع الإجراءات الموضحة في الملحق (أ) من خلال وحدة حوكمة البيانات.

٧,٣ مستخدمي النظام خارجي external system users

يتبع الإجراءات التالية:

١. تقديم طلب رسمي حسب النموذج المعد ذلك لإضافته مستخدم على النظام.
٢. على الجهة المستفيدة الرفع بمرشحيها الممثلين لها على النظام وفق النماذج المعد لذلك لجهة وحدة حوكمة البيانات.
٣. الالتزام بنظام حماية البيانات الشخصية بجامعة تبوك و جميع السياسات و اللوائح ذات الصلة.
٤. يلتزم المستخدم بإتباع الإجراءات الموضحة في الملحق (أ) من خلال وحدة حوكمة البيانات.

٨ الجهات المساندة

٨,١ الادارة العامة لتقنية المعلومات IT

تتولى المهام والمسؤوليات التالية :

١. تقديم الدعم والمساندة التقنية للجهات المستفيدة والمنفذة لسياسات أنظمة الجامعة.
٢. توفير البرمجيات والأدوات المساعدة التي تساعد في منح الصلاحيات للجهات داخل الجامعة ومنها أنظمة وبرامج الذكاء الاصطناعي.
٣. اعداد قوائم لمجموعات المستخدمين لكل نظام الكتروني وتحديد صفة صلاحيات الوصول المخولة لهم، وتزويد مالك البيانات بنسخة من تلك القوائم بصفة دورية.
٤. إضافة صلاحيات مدراء الأنظمة الالكتروني المملوك لجهاتهم من تاريخ تكليفهم رؤساء للجهات، وتحدد مدة صلاحية إدارة النظام الالكتروني بمدة التكليف الإداري.

٨,٢ إدارة الامن السيبراني

يتولى المهام والمسؤوليات التالية :

المتابعة والتأكد من تطبيق سياسات جامعة تبوك في الأمن السيبراني على كافة الأنظمة وسلوك المستخدمين وضمان عدم تسرب البيانات وتوفير الأدوات المناسبة لضمان ذلك، بالتنسيق مع وحدة حوكمة بيانات جامعة تبوك.

٨,٣ وحدة حوكمة البيانات

ويتولى المهام والمسؤوليات التالية :

١. الاشراف على عمليات سير صلاحيات منح الوصول لكافة أنظمة الجامعة وضمان تطبيق حماية البيانات.
٢. التأكد من تطبيق سياسات جامعة تبوك في حماية البيانات وتطبيق الأنظمة واللوائح المرتبطة بذلك.
٣. استقبال اشعارات مخالفة نظام حماية البيانات الشخصية أو إساءة استخدامها، من مدراء الأنظمة والتعامل معها حسب النظام.

٩ مصفوفة الصلاحيات :

	الجهة / المهمة	مدير النظام الالكتروني	الادارة العامة لتقنية العلومات	إدارة الأمن السيبراني	وحدة حوكمة البيانات	الجهات المستفيده (داخليا/خارجيا)	مستخدمي النظام الداخلي	مستخدمي النظام الخارجي
١	التأكد من صحة وسلامة البيانات (جودة البيانات) التي يحتويها النظام والعمل على رفع جودة البيانات حسب دليل جودة البيانات المعتمد من وحدة حوكمة البيانات.	✓						
٢	منح الاذن بالوصول للنظام:							

٢,١	منح الاذن بالوصول للمستخدمين و المستفيدين حسب الصلاحيات المخولة لهم في وثيقة تصنيف مجموعات المستخدمين و المستفيدين للنظام بعد تقديم طلب الاذن بالوصول حسب النموذج المعد لذلك.	✓						
2.2	تقدير صلاحيات الوصول قبل منح الاذن للبيانات بالوصول	✓						
٣	المتابعة والمراجعة							
3.1	المراجعة الدورية لمستخدمي النظام وتحديث بياناتهم وأذونات الوصول بصفة دورية وتزويد وحدة حوكمة البيانات بالتقرير اللازمة حول ذلك.	✓						
٤	المراقبة:							
4.1	مراقبة الأنشطة التي تتم على النظام من خلال رصدها وقيدها، بما في ذلك النشاطات المتعلقة بالشخص الذي يصل إلى هذه البيانات.	✓		✓				
4.1	اشعار وحدة حوكمة البيانات في حال وجود انشطة مشبوهة وتجاوزات من مستخدمي النظام أو إساءة استخدام بيانات النظام.	✓		✓				
٥	إيقاف الاذن بالوصول للنظام:							
5.1	إغلاق حسابات المستخدمين بعد انتهاء المدة المستحقة للوصول للبيانات واشعارهم بذلك.	✓						
5.2	في حال انتهاء التكليف والصلاحية لممثل أحد جهات الجامعة في النظام الالكتروني فيجب إيقاف حسابه بعد اشعار الجهة بانتهاء صلاحية الوصول لممثلهم على النظام، واشعارهم بطلب التجديد او تكليف ممثل جديد.	✓						
5.3	إيقاف إذن الوصول للبيانات.في حال رصد وقيد مخالفة وتجاوزات مشبوهة من أحد المستخدمين أو المستفيدين قبل إنتهاء	✓						

	صلاحيات الوصول لأنظمة الجامعة							
5.4	وفي حال إيقاف إذن الوصول للمخالف يجب إشعار وحدة حوكمة البيانات لاتخاذ الازم حيال ذلك.	✓						
6	تقديم طلب رسمي حسب النموذج المعد ذلك لإضافته مستخدم على النظام.						✓	✓
٧	على الجهة المستفيدة الرفع بمرشحيها الممثلين لها على النظام وفق النماذج المعد لذلك لجهة وحدة حوكمة البيانات.					✓		
٨	الالتزام بنظام حماية البيانات الشخصية بجامعة تبوك و جميع السياسات و اللوائح ذات الصلة.	✓	✓	✓	✓	✓	✓	✓
٩	تقديم الدعم والمساندة التقنية للجهات المستفيدة والمنفذة لسياسات أنظمة الجامعة.		✓					
١٠	توفير البرمجيات والأدوات المساعدة التي تساعد في منح الصلاحيات للجهات داخل الجامعة ومنها أنظمة وبرامج الذكاء الاصطناعي.		✓					
١١	اعداد قوائم لمجموعات المستخدمين لكل نظام الكتروني وتحديد صفة صلاحيات الوصول المخولة لهم، وتزويد مالك البيانات بنسخة من تلك القوائم بصفة دورية.		✓					
١٢	إضافة صلاحيات مدراء الأنظمة الالكتروني المملوك لجهاتهم من تاريخ تكليفهم رؤساء للجهات، وتحدد مدة صلاحية إدارة النظام الالكتروني بمدة التكليف الإداري.		✓					
١٣	المتابعة والتأكد من تطبيق سياسات جامعة تبوك في الأمن السيبراني على كافة الأنظمة وسلوك المستخدمين وضمان عدم تسرب البيانات وتوفير الأدوات المناسبة لضمان	✓	✓	✓	✓	✓	✓	✓

	ذلك، بالتنسيق مع وحدة حوكمة بيانات جامعة تبوك.							
١٤	الاشراف على عمليات سير صلاحيات منح الوصول لكافة أنظمة الجامعة وضمان تطبيق حماية البيانات.			✓				
١٥	استقبال اشعارات مخالفة نظام حماية البيانات الشخصية أو إساءة استخدامها، من مدراء الأنظمة والتعامل معها حسب النظام.				✓			

١٠ المرجعيات

١. الهيئة السعودية للبيانات والذكاء الصناعي (SDAIA)

٢. وحدة حوكمة البيانات الوطنية (MDMO)