الإدارة العامة للإتصالات وتقنية المعلومات
General Administration for
Communicatiom and Information Technology

الدليل التنظيمي لوحدة إدارة وحوكمة البيانات

التابعة للإدارة العامة للاتصالات وتقنية المعلومات
بجامعة بيشة

الإصدار الأول (١٤٤٣ هـ - ٢٠٢٢م)


بسم الله الرحمن الرحيم

الإدارة العامة للإتصالات وتقنية المعلومات
General Administration for
Communicatiom and Information Technology

كلمة مدير الإدارة العامة للاتصالات وتقنية المعلومات

في اطار رؤية جامعة بيشة الطموحة "منظومة معرفية إبداعية لمجتمع منتج" والتي تعد المصدر الرئيس لخطتها الاستراتيجية للتحول الرقمي (2022 - 2026 م), تلعب الإدارة العامة للاتصالات وتقنية المعلومات أدواراً بالغة الأهمية في تعزيز واستثمار الموارد التقنية لتوفير خدمات تقنية متميزة تواكب التطورات المتلاحقة في مجال تقنية المعلومات والتحول الرقمي وذلك بالتكامل مع جهات الجامعة المختلفة بما يسهم في تحقيق كفاءة الإنفاق والتنمية المستدامة, كما تقوم بأنشطة وفعَّاليات متنوعة في اطار المسؤولية المجتمعية.

وقد عملت الإدارة العامة للاتصالات وتقنية المعلومات على وضع عدة مسارات للعمل في كافة الاتجاهات المتمثلة في تحسين الخدمات التقنية لمواكبة التقدم المتسارع في مجال التحول الرقمي من خلال تقديم الدعم التقني اللازم بكافة أنواعه المختلفة والمتنوعة, وتعزيز الترابط مع المجتمع المحيط في مجال التحول الرقمي، والسعي لتنمية قدرات منسوبي الجامعة وتمكينهم من أدوات العمل الدقيق و الأداء المتميز مع ضمان الجودة الفعَّالة, فضلاً عن رفع مستوى الوعي لدى منسوبي الجامعة بدورهم في المسؤولية المجتمعية وحث كافة فئات المجتمع على السعي لتحقيق كفاءة الإنفاق والتنمية المستدامة في مجال التحول الرقمي وتقنية المعلومات.

والله الموفق والمستعان

مدير الإدارة العامة للاتصالات وتقنية المعلومات
م. يحي بن علي شراحيلي

الإدارة العامة للإتصالات وتقنية المعلومات
General Administration for
Communicatiom and Information Technology

كلمة مدير إدارة البنية التحتية والعمليات

انطلاقاً من رؤية المملكة العربية السعودية 2030 و ورؤية جامعة بيشة الطموحة "منظومة معرفية إبداعية لمجتمع منتج" وإيماناً بتحقيقها تسعى الإدارة العامة للاتصالات وتقنية المعلومات على تقديم أفضل الخدمات التقنية بمعايير عالمية ومحلية وذات حماية عالية, ومن هذا المنطلق فقد دأبت إدارة البنية التحتية والعمليات التابعة للإدارة العامة للاتصالات وتقنية المعلومات على تقديم منظومة خدمات تقنية وبنية تحتية متقدمة ومتكاملة ومستقرة, كما سعت الإدارة إلى الاستفادة القصوى والمثلى من التقنية, وابتكار وتطبيق أحدث الحلول التقنية لتحقيق رؤية جامعة بيشة الطموحة ولدعم خطة التحول الرقمي للجامعة وتنفيذاً لمبادراتها المتعلقة بالبنية التحتية التقنية.

كما تعمل الإدارة وبشكل دائم على التطوير المستمر للخدمات المقدمة, والمساهمة الفعالة في تطوير العملية التعليمية من خلال تطبيق أفضل الممارسات التقنية وتوفير البنية التحتية اللازمة والدعم الفني والتقني لكافة إدارات الجامعة وفروعها ومنسوبيها, وتعمل الإدارة نحو تحقيق أهدافها من خلال فريق عمل متميز وفي ظل ما تلقاه من توجيهات ودعم لامحدود من إدارة الجامعة.

هذا والله ولي التوفيق

مدير إدارة البنية التحتية والعمليات
م. ناصر سليمان المطيري

الإدارة العامة للإتصالات وتقنية المعلومات
General Administration for
Communicatiom and Information Technology

كلمة رئيس وحدة إدارة وحوكمة البيانات

في إطار تحقيق رؤية المملكة العربية السعودية 2030 أولت المملكة اهتمامًا كبيرًا بإدارة البيانات باعتبارها مصدرًا ورافدًا ثريًا للاستثمار؛ وتحقيقًا لهذه الرؤية ولرؤية الجامعة الطموحة سعت جامعة بيشة من خلال الإدارة العامة للاتصالات وتقنية المعلومات إلى ضمان الاستفادة القصوى من البيانات التـي تشكّل جزءاً مهمـاً مـن الأصول الوطنيـة, ومن هذا المنطلق واستنادًا إلى توصيات اللجنة الدائمة للتعاملات الإلكترونية رقم 1/3/42/43 بتاريخ 21/10/1443 هـ, المتضمن اعتماد هيكلة الإدارة العامة للاتصالات وتقنية المعلومات فقد تم إنشاء وحدة إدارة وحوكمة البيانات, تعمل الوحدة على التعزيـز لمبـدأ مشـاركة البيانات وتحقيق التكامل بين جهات الجامعة المختلفة, كما تسعى للحـد مـن ازدواجيـة البيانـات وتعارضهـا وتعـدد مصادرهـا.

و تعمل الوحـدة على تنفيذ العديـد من الأنشطـة المرتبطة بنشر ثقافـة إدارة وحوكـمة البيـانـات بين منسوبـي الجامعـة, وتعميـق التواصـل بين قطاعـات الجامعـة المختلفـة, فضـلاً عن تمكين السياسـات المرتبطـة بقواعـد البيانـات لضمان جودة الاداء وتحسينـه بصـورة مستمـرة.

والله الموفق

رئيس وحدة إدارة وحوكمة البيانات
م. منيرة فايز السلولي

الإدارة العامة للإتصالات وتقنية المعلومات
General Administration for
Communicatiom and Information Technology

الفهرس:

المقدمة:

تتقدم جامعة بيشة بخطوات راسخة نحو تعزيز قدراتها في كافة المجالات لاسيما مجال التحول الرقمي مما يدعم سعيها لتحقيق رؤيتها الطموحة ويدعم سعيها للتميز في جميع المجالات, ويعزز من مساهماتها المستمرة في تحقيق متطلبات التنمية المستدامة وفق رؤية المملكة العربية السعودية 2030 وتوجهاتها الاستراتيجية؛ بصورة عامة وبصيغة خاصة فيما يتعلق بإدارة وحوكمة البيانات.

واستنادًا إلى توصيات اللجنة الدائمة للتعاملات الإلكترونية رقم 1/3/42/43 بتاريخ 21/10/1443 هـ, المتضمن اعتماد هيكلة الإدارة العامة للاتصالات وتقنية المعلومات, فقد تم إنشاء وحدة إدارة وحوكمة البيانات التابعة لقسم البنية المؤسسية بإدارة البنية التحتية والعمليات و بما يحقق اهداف الإدارة العامة للاتصالات وتقنية المعلومات ويساهم بشكل فعال في دعم خطة التحول الرقمي بالجامعة.

وتُعنى الوحدة بالعديد من الأنشطة المرتبطة بنشر ثقافة إدارة وحوكمة البيانات بين منسوبي الجامعة, وتعميق التواصل بين قطاعات الجامعة المختلفة, فضلاً عن تمكين السياسات المرتبطة بقواعد البيانات لضمان جودة الاداء وتحسينه بصورة مستمرة في إطار المحافظة على الخصوصية والسرية للبيانات والمعلومات الشخصية.

وتم إعداد هذه الوثيقة لتعتبر بمثابة المرجعية في مجال إدارة وحوكمة البيانات بالجامعة, ولتسهم في تحسين وتطوير الخدمات والتعاملات الإلكترونية بالجامعة بصورة تكاملية لبيانات معتمدة وموثقة.

الأهداف:

1. دعم وتعزيز جهود المملكة في تحقيق الرؤية والاستراتيجيات الوطنية.
2. تمكين إعداد السياسات وتنفيذ الخطط, والقيام باستشراف المستقبل.
3. توعية منسوبي الجامعة بأهمية حماية البيانات التي يتم تلقيها, أو إنشاؤها, أو التعامل معها, وتخزينها مهما كان مصدرها, أو شكلها, أو طبيعتها, و تحديد الإجراءات اللازمة لحماية سرية وسلامة وتوافر البيانات.
4. تحقيق التكامل بين الجهات الداخلية بالجامعة.
5. العمل على رفع مستوى الثقة في التعاملات التي تعتمد على البيانات.
6. ضمان حماية البيانات وتطبيق سياسات خصوصية البيانات الشخصية وسرية البيانات الحساسة.
7. دعم جهود تعزيز النزاهة ومكافحة الفساد عن طريق االطاع على المعلومات العامة كحق إنساني مكفول.

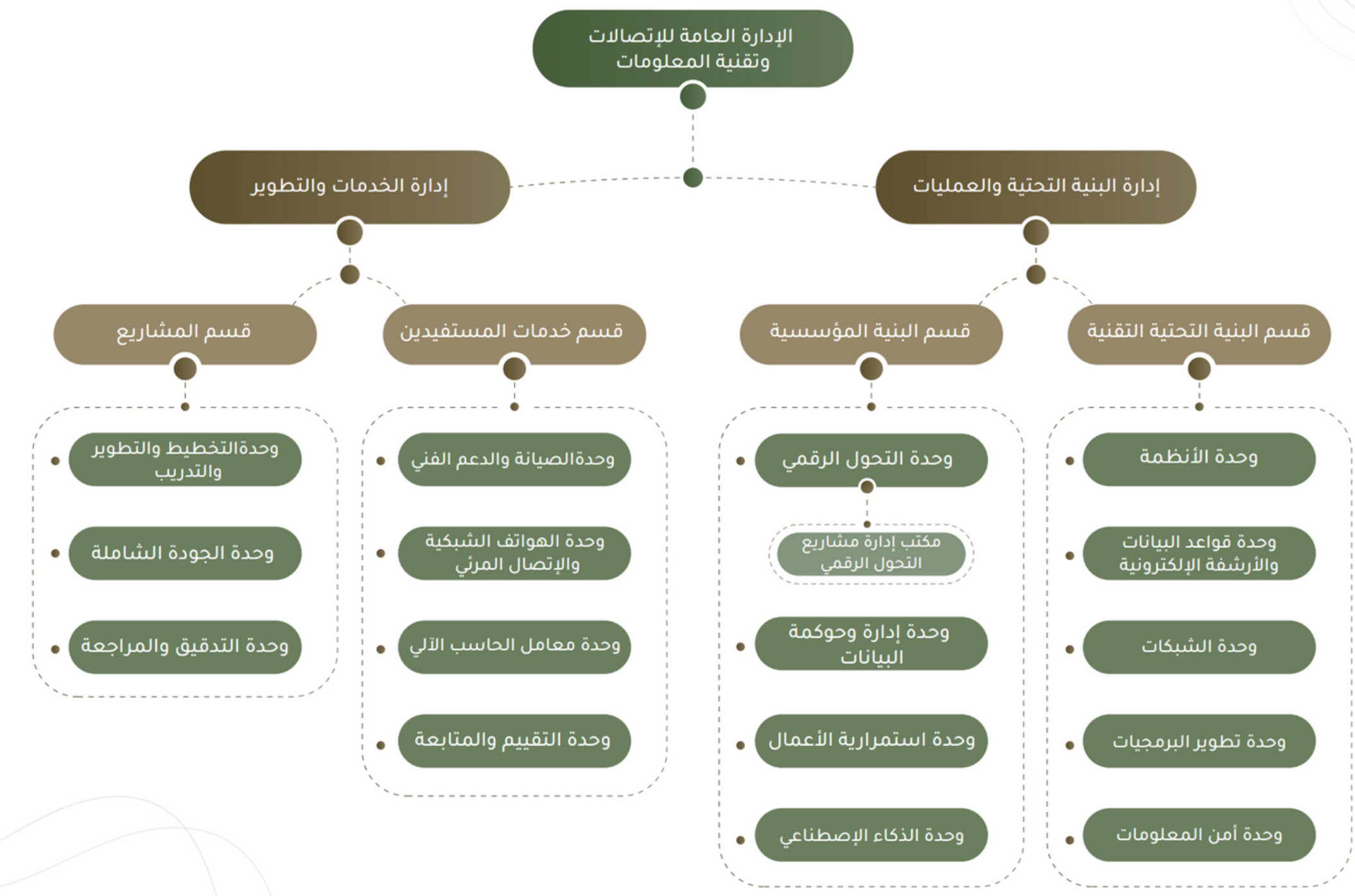
النطاق:

المساهمة في رفع مستوى نضج مجال البيانات والذكاء االصطناعي في الجامعة عن طريق زيادة الوعي بينن منسوبي الجامعة والتعريف بساسات إدارة وحوكمة البيانات ومنها: .سياسة تصنيف البيانات, .سياسة حماية البيانات الشخصية, سياسة مشاركة البيانات, سياسة حرية المعلومات,سياسة البيانات المفتوحة., وضمان تطبيق أحكام هذه السياسات على جميع البيانات التي تتلقاها أو تنتجها أو تتعامل معها الجامعة مهما كان مصدرها, أو شكلها أو طبيعتها.

الإدارة العامة للإتصالات وتقنية المعلومات
General Administration for
Communicatiom and Information Technology

الهيكل التنظيمي:

تتبع وحدة إدارة وحوكمة البيانات قسم البنسة المؤسسية بإدارة البنية التحتية والعلميات التابعة للإدارة العامة للاتصالات وتقنية المعلومات بجامعة بيشة.
كما هو موضع بالهيكل التنظيمي التالي:



الإدارة العامة للإتصالات وتقنية المعلومات
General Administration for
Communicatiom and Information Technology

مهام مدير وحدة حوكمة البيانات:

- التنسيق لتنفيذ فعاليات نشر ثقافة مشاركة البيانات والتعاون لتعزيز وتطوير البيانات والمعلومات والأصول المعرفية.
- تنظيم عملية نشر وتبادل واستخدام/ إعادة استخدام البيانات المحمية والمعلومات العامة.
- ضمان تحقيق التكامل بين الجهات الداخلية بالجامعة فيما يتعلق بإدارة وحوكمة البيانات.
- توطين سياسات إدارة وحوكمة البيانات ومتابعة تنفيذ الخطط المرتبطة بها, والقيام باستشراف المستقبل.
- تطبيق مؤشرات المحافظة على خصوصية البيانات الشخصية, وسرية البيانات الحساسة.
- متابعة أنشطة وإجراءات المحافظة على حقوق الأفراد عند التعامل مع البيانات الشخصية والمعلومات العامة.
- رفع مستوى الثقة في الخدمات المعتمدة على البيانات.
- تفعيل أليات تحسين رفع مستوى الخدمات والتعاملات الإلكترونية بما يحقق التكاملية.

سياسات إدارة وحوكمة البيانات:

أولاً: سياسة تصنيف البيانات

الهدف

تهدف هذه الوثيقة إلى توعية منسوبي جامعة بيشة بأهمية حماية البيانات التي يتم تلقيها, أو إنشاؤها, أو التعامل معها, وتخزينها من قبل الجامعة مهما كان مصدرها, أو شكلها, أو طبيعتها, وتحديد الإجراءات اللازمة لحماية سرية وسلامة وتوافر البيانات.

المبادئ

تنطبق هذه السياسة على جامعة بيشة, وعلى كافة الأطراف المعنية بما في ذلك الشركاء, أو الشركات التابعة لها, وعلى نظم معالجة البيانات ونظم ضبط العمليات التي تحتوي على، أو تستخدم معلومات و/أو تسهيلات تعود ملكيتها للجامعة من خلال جامعة بيشة.
وتسري هذه السياسة على كافة الموظفين/ المستخدمين الذين يعملون بصورة مباشرة أو غير مباشرة لدى الجامعة, أو الجهات التابعة لها, أو أية جهة تقوم بتنفيذ عمل نيابة عنها يتضمن استخدام الأصول المعلوماتية التابعة لها.
تلتزم جامعة بيشة بتقديم الدعم الكامل في البحث العلمي بتمكين حرية وصول جميع الأشخاص المهتمين إلى البيانات الأساسية والعمليات والنتائج النهائية للبحث.
بشكل عام, تعتبر بيانات البحث مصنفة على أنها بيانات عامة ما لم تكن هناك متطلبات محددة للحفاظ على سرية البيانات, مثلا عندما يكون الباحث ملزماً بحماية المعلومات السرية لشركة متعاونة, أو عندما تتعلق البيانات بأشخاص.

الأدوار والمسؤوليات

جميع الإدارات داخل جامعة بيشة مسؤولة عن وضع الضوابط الإدارية والتشغيلية والمادية والتقنية المناسبة للوصول, أو استخدام, أو نقل, أو التخلص من البيانات وفقا لهذه السياسة.

جميع البيانات المملوكة لجامعة بيشة هي مسؤولية كل من يتعامل معها, وتنظم المسؤوليات على النحو التالي:

- **مسؤول البيانات:**

يجب أن يكون لجميع المعلومات المملوكة في الجامعة " مسؤول البيانات " لتحقيق المهام الرئيسية التالية:

1. تحديد وإنشاء تصنيف للبيانات, يتضمن إعطاء مستويات تصنيف لجميع البيانات داخل الجامعة.
2. التأكد من أن البيانات يتم مراجعتها بانتظام حسب أهميتها ومدى التغيرات المؤثرة على أهميتها عند وقوع المخاطر: كالتهديدات الجديدة, أو نقاط الضعف المكتشفة في الأنظمة, أو أية تغيرات في البيئة المحيطة بها.
3. مراجعة وتعديل التصنيف بين فترة وأخرى حسب التغيرات في أولويات العمل أو القوانين والتعليمات والأنظمة.
4. يتحمل مسؤول البيانات المسؤولية النهائية في أمن وحماية الموارد المعلوماتية في الإدارة.
5. التأكد من أن جميع المستخدمين على علم بكيفية تداول وحماية البيانات بطريقة تتناسب مع تصنيفها
6. تطوير إجراءات أمن وحماية البيانات في الجامعة.

سياسة تصنيف البيانات:

- مستضيف البيانات:

يقوم بتقييم مستويات التأثير وتحديد إرشادات استخدام البيانات وتعيين تصنيف بيانات مطابق لأنواع البيانات أو مجموعات البيانات. يصرحون بالوصول إلى البيانات التي يتحملون مسؤوليتها ويستخدمون وسائل معقولة لإبلاغ أولئك الذين يتلقون البيانات أو يصلون إليها بالتزاماتهم في القيام بذلك.

- أمناء البيانات:

يتأكدون بدورهم من أن الأنظمة التي تتعامل مع البيانات المقيدة أو الداخلية توفر الأمان وحماية الخصوصية وفقاً لتصنيف البيانات وسياسات والتزامات وتصاريح مضيف البيانات, وكما قد يتم تحديدها في دليل استخدام البيانات. يستخدمون وسائل محددة وواضحة لإبلاغ أولئك الذين يصلون إلى مجموعات البيانات في سيطرتهم بالتزاماتهم في القيام بذلك.

- الموظفون:

الالتزام والاتباع لقيود وتوجيهات مسؤول البيانات وأمناء البيانات ويتبعون دليل استخدام البيانات في تعاملهم مع المعلومات السرية.

محور السياسة

البيانات هي أحد الأصول الهامة للجامعة. جميع منسوبي الجامعة مسؤولون عن حماية سرية وسلامة وتوفر البيانات التي تم إنشاؤها أو تخزينها أو استخدامها من قبل الجامعة, مهما كان نوع أو شكل أو مصدر هذه البيانات سواء كانت ورقية أو إلكترونية أو أي أشكال أخرى.

من أجل تأمين بيانات الجامعة بشكل أمن وفعال, يجب أن يكون هناك مفردات يمكن أن يتم استخدامها لوصف البيانات وتحديد مقدار الحماية المطلوبة. تحدد هذه السياسة أربع فئات يمكن تقسيم جميع بيانات الجامعة إليها:

1) أولاً: سري للغاية
2) ثانيا: سري
3) ثالثاً: مقيد
4) رابعاً: عام

قد يتم الكشف عن بيانات الجامعة المصنفة على أنها عامة لأي شخص بغض النظر عن ارتباطه سواء بالجامعة أو بالجامعة. تعتبر جميع البيانات الأخرى معلومات حساسة, ويجب حمايتها بشكل مناسب.

يقدم هذا المستند تعريفات وأمثلة لكل فئة من الفئات الأربع. تحدد السياسات الأخرى ضمن معايير حماية البيانات ضوابط الأمان المطلوبة لكل فئة من فئات البيانات.

تحتوي الوحدات والأقسام المختلفة في الجامعة على عديد من أنواع المستندات والبيانات إلى الحد الذي لا يتم فيه تناول مستندات أو أنواع بيانات معينة بشكل صريح في هذه السياسة, يجب على كل وحدة عمل أو قسم تصنيف بياناته من خلال النظر في احتمال حدوث ضرر للأفراد أو الجامعة في حالة تم الكشف غير المقصود أو التعديل أو الضياع.

قد يساعد مسؤول البيانات في عملية التصنيف والتنسيق مع فريق أمن معلومات الجامعة لتحقيق الاتساق في جميع أنحاء الجامعة. عند تصنيف البيانات, يجب على كل قسم أن يوازن بين المخاطر الناتجة عن الإفصاح غير المقصود أو التعديل أو الخسارة مقابل الحاجة إلى تشجيع المناقشة المفتوحة, وتحسين الكفاءة وتعزيز أهداف الجامعة في إنشاء ونشر المعرفة.

يجب أن تهتم الإدارات والأقسام والوحدات بشكل خاص بحماية المعلومات الشخصية الحساسة, مثل الرقم الوظيفي أو المعلومات الوطنية كالهوية, والتي قد يؤدي الكشف عنها إلى مخاطر سرقة الهوية.

سياسة تصنيف البيانات:

يمكن تصنيف بعض المعلومات بشكل مختلف في أوقات مختلفة. على سبيل المثال, قد تصبح المعلومات التي كانت تعتبر في السابق بيانات سرية بيانات عامة بمجرد الإفصاح عنها بشكل مناسب. يجب على كل شخص لديه حق الوصول إلى البيانات ممارسة الحكم الجيد في التعامل مع المعلومات الحساسة وطلب التوجيه من الإدارة حسب الحاجة.

ا) سري للغاية

هي المعلومات التي يتم تصنيفها بموجب القوانين والأنظمة أو السياسات المتبعة على مستوى الجامعة, بأنها سرية للغاية, ولا يجوز الاطلاع عليها من قبل الأشخاص غير المصرح لهم, أو تلك التي تصنفها الإدارات على أنها بيانات سرية, هذه بعض الأمثلة من البيانات السرية:

- بيانات المستخدمين على منصات برامج التعلم الإلكتروني والتعليم عن بعد.
- بيانات الولوج إلى قواعد البيانات.
- التعهدات والمشاريع.
- أي بيانات تحددها الأنظمة الحكومية على أن تعامل على أنها سرية.

التعامل مع البيانات السرية:

- عند تخزين البيانات في شكل إلكتروني، يجب أن تكون محمية بكلمات مرور قوية, وتخزينها على الخوادم التي تحتوي على تدابير الحماية التي تضعها تقنية المعلومات من أجل حماية البيانات ضد الضياع أو السرقة والوصول غير المصرح به, أو الاطلاع غير المصرح به.
- يجب ألا يتم الكشف عنها لأي طرف دون إذن صريح من الإدارة التنفيذية.
- يجب أن يتم تخزينها فقط في منطقة مغلقة خاضعة للمراقبة؛ لتوفير الحماية الكافية ومنع الوصول غير المصرح به.
- يجب ألا يتم نشرها في أي موقع عام.
- يجب أن يتم إتلافها عند الحاجة ولم تعد تخضع لسياسة إدارة السجلات في الجامعة والجامعة.

2) سري

البيانات السرية هي المعلومات التي في حالة تم إتاحتها لأي طرف غير مصرح له, قد تؤثر سلباً على الأفراد أو الأعمال بجامعة بيشة. يشمل هذا التصنيف أيضاً البيانات التي يتعين على الجامعة الحفاظ عليها في سرية تامة, إما بموجب القانون (على سبيل المثال مكتب إدارة البيانات الوطنية) أو بموجب اتفاقيات سرية مع طرف ثالث, مثل: مقدمي الخدمات أو مقدمي البرامج التعليمية. يجب حماية هذه المعلومات من الكشف أو التعديل غير المصرح به. بالإضافة لأنه يجب أن تستخدم هذه البيانات السرية فقط عند الضرورة, ويجب حمايتها سواء عندما تكون قيد الاستخدام أو عندما يتم تخزينها أو نقلها.
على سبيل التوضيح فقط, هذه بعض الأمثلة من البيانات السرية:

- معلومات التعريف الشخصية لأعضاء هيئة التدريس ومن في حكمهم والموظفون، والإداريون، والفنيون, والطلاب.
- سجلات لأعضاء هيئة التدريس ومن في حكمهم والموظفون والإداريون، والفنيون، والطلاب، وبياناتهم.
- السجلات الطبية للمركز الطبي الجامعي.
- سجلات الرواتب.
- أرقام الحسابات المصرفية والمعلومات المالية الشخصية الأخرى.

سياسة تصنيف البيانات:

3) مقيد

البيانات المقيدة هي المعلومات التي يحتمل أن تكون حساسة أو مقيدة للاستخدام الرسمي ولا يُقصد مشاركتها مع الجمهور بشكل عام, ولا ينبغي الكشف عن البيانات الداخلية خارج الجامعة دون إذن الشخص أو المجموعة التي أنشأت البيانات. تقع المسؤولية على عاتق مسؤول البيانات في تحديد المعلومات على أنها مقيدة عند الاقتضاء.

ويجب أن تكون محمية من الوصول غير المصرح به أو التعديل أو النقل, وإذا ما تم الإفصاح عنها فإنها يمكن أن تعرض خصوصية وأمن الجامعة أو أي من المتعاملين معها للخطر, ومن ثم فإن الإفصاح غير المرخص عن المعلومات التي للاستخدام الرسمي فقط يمكن أن يؤثر سلباً على الثقة بالموظفين والمواطنين. وعلى سبيل المثال:

- المذكرات الداخلية.
- محاضر الاجتماعات.
- أدلة الهاتف الداخلية.
- كتيبات أدلة الاستخدام.

إذا كانت لديك أسئلة حول ما إذا كانت المعلومات داخلية أو كيفية التعامل مع البيانات المقيدة, فيجب عليك التحدث إلى عميدك أو رئيس القسم.

4) عام

البيانات العامة هي معلومات قليلة الحساسية والتي قد يتم الكشف عنها لأي شخص بغض النظر عن ارتباطه بالجامعة. والتي لا يؤثر الإفصاح عنها على خصوصية أو أمن الجامعة أو أي من المتعاملين معها ولا يقتصر التصنيف العام على البيانات ذات المصلحة العامة أو التي يُقصد توزيعها على الجمهور. ينطبق التصنيف على البيانات التي لا تتطلب أي مستوى من الحماية من الإفشاء. في حين أنه قد يكون من الضروري حماية المستندات الأصلية (المصدر) من التعديل غير المصرح به, فقد تتم مشاركة البيانات العامة مع جمهور عريض داخل وخارج مجتمع الجامعة, ولا يلزم اتخاذ أي خطوات لمنع توزيعها.
وتكون عادة متاحة للنشر عبر وسائل الاتصال والإعلام, بالطرق الإلكترونية, أو الشفوية, أو المكتوبة, مثل المطبوعات المنشورة والنشرات والكتيبات وصفحات الإنترنت.

الالتزام

جميع منسوبي الجامعة من إداريين أو موظفين أو متعاقدين مسئولون عن حماية بيانات الجامعة من الوصول, أو التعديل, أو الإفشاء, أو النقل أو الإتلاف غير المصرح به, ويجب عليهم الوعي والامتثال لهذه السياسة وأن أي انتهاكات لهذه السياسة يمكن أن يؤدي إلى اتخاذ إجراءات تأديبية و / أو إجراءات قانونية, وتضمن هذه الإجراءات على سبيل المثال:

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

عند الحاجة يمكن التقدم بطلبات الحصول على استثناءات بصورة رسمية إلى إدارة الجامعة مع توضيح مسوغات الاستثناء والمزايا التي قد تنجم عنه على أن يتم الموافقة عليها من لجنة أمن المعلومات في جامعة بيشة.

سياسة تصنيف البيانات:

المواصفات الأساسية لحماية البيانات

1-سري للغاية

الجمع والاستخدام	استبعاد الجمع كلما أمكن ذلك. أو يجب أن يقتصر على الاستخدامات المصرح بها من قبل (أمناء) البيانات المناسبين. كما هو موضح في سياسة الخصوصية. يجب أن تتضمن صفحات الويب الخاصة بالجامعة التي تُستخدم لجمع البيانات ارتباطاً بسياسة خصوصية الجامعة والجامعة. يجب ألا يستخدم رقم المنسوب أو رقم الهوية الوطنية كاسم مستخدم أو كلمة مرور.
الوصول أو المشاركة	يجب أن يقتصر الوصول على مسؤولي البيانات المعتمدين أو الوكلاء الذين لديهم مصلحة أكاديمية ويحتاجون إلى المعرفة على النحو المبين في سياسة الخصوصية. وفقاً لمتطلبات سياسة الوصول إلى البيانات, يجب الموافقة على جميع عمليات الوصول من قبل مسؤول البيانات وتتبعها بطريقة كافية للتدقيق.
الإفصاح والنشر	غير مسموح به ما لم يقتضيه القانون.
التبادل مع الأطراف الثالثة ومقدمي الخدمات	يكون ضمن الاتفاقيات التعاقدية (أو مذكرة تفاهم إذا كانت وكالة حكومية) التي تحدد المسؤوليات الأمنية التي يجب أن تكون سارية ومعتمدة من قبل مكتب الشؤون القانونية قبل تبادل البيانات مع الطرف الثالث / مزود الخدمة.
التخزين أو المعالجة: الخوادم	يجب أن تمتثل الخوادم لمتطلبات الأمان على النحو المبين في الحد الأدنى من معايير الأمان للأجهزة الحساسة.
التخزين أو المعالجة على الأجهزة الإلكترونية	يجب أن تمتثل الأنظمة لمتطلبات الأمان على النحو المبين في الحد الأدنى من معايير الأمان للأجهزة الحساسة. لا يُسمح بتخزين البيانات المقيدة على الأجهزة المملوكة شخصيًا.
التخزين على الأقراص المتحركة	غير مسموح به ما لم يقتضيه القانون. إذا كان ذلك مطلوباً بموجب القانون, يجب تشفير البيانات المخزنة على الوسائط القابلة للإزالة وتخزين الوسائط في بيئة أمنة مادياً. لا يُسمح بتخزين البيانات المقيدة على الوسائط المملوكة شخصياً.
الإرسال الإلكتروني	يجب استخدام اتصالات آمنة أو مصدق عليها أو بروتوكولات آمنة لنقل البيانات المقيدة
البريد الإلكتروني والرسائل الإلكترونية الأخرى	غير مسموح به بدون إذن صريح أو ما لم يقتضيه القانون. في حالة الحصول على إذن, يتم تضمين البيانات فقط في الرسائل داخل مرفق ملف مشفر أو عبر أنظمة آمنة معتمدة. جب تشفير البيانات الحساسة بشكل خاص أو كميات كبيرة من البيانات السرية أثناء الإرسال. يوصى باستخدام خدمة البريد الإلكتروني الآمنة المتاحة إذا كان سيتم تخزين المعلومات السرية على وسائط قابلة للإزالة (/ CD DVD / USB / HD خارجي) أو في السحابة.
طباعة, بريد الإلكتروني، فاكس	يجب توزيع أو إتاحة المواد المطبوعة التي تتضمن بيانات سرية فقط للأشخاص المصرح لهم يجب تقييد الوصول إلى أي منطقة يتم فيها تخزين السجلات المطبوعة ذات البيانات المقيدة باستخدام عناصر التحكم (مثل الأقفال والأبواب والمراقبة وما إلى ذلك) الكافية لمنع الدخول غير المصرح به.
التصرف والإتلاف	يجب حذف البيانات حيث لا يمكن استردادها يجب تدمير الوسائط المادية (مثل الورق, القرص المضغوط, الشريط , إلخ) بحيث لا يمكن استعادة البيانات الموجودة على الوسائط أو إعادة بنائها. بالنسبة للمستندات الداخلية ذات المحتوى الحساس مثل(الورق , القرص المضغوط , الشريط , إلخ) , يجب إتلافها أو تدميرها كاستخدام آلة تقطيع الورق. استخدم أدوات نظام التشغيل المساعدة لحذف الملفات. بالنسبة للأقراص الصلبة والمتحركة من أفضل الممارسات مسح هذه الأجهزة بأمان قبل التخلص منها.

سياسة تصنيف البيانات:

المواصفات الأساسية لحماية البيانات

2- سري

الجمع والاستخدام	أن يقتصر الاستخدام على المصرح لهم كما هو موضح في سياسة الخصوصية. يجب أن تتضمن صفحات الويب الخاصة بالجامعة التي تُستخدم لجمع البيانات ارتباطاً بسياسة خصوصية الجامعة والجامعة.
الوصول أو المشاركة	يجب أن يقتصر الوصول على مسؤولي البيانات المعتمدين أو الوكلاء الذين لديهم مصلحة أكاديمية ويحتاجون إلى المعرفة على النحو المبين في سياسة الخصوصية. وفقًا لمتطلبات سياسة الوصول إلى البيانات, يجب الموافقة على جميع عمليات الوصول من قبل مسؤول البيانات وتتبعها بطريقة كافية للتدقيق. قبل منح حق الوصول إلى أي طرف ثالث خارجي, يجب الموافقة على الاتفاقيات التعاقدية التي تحدد المسؤوليات الخاصة بأمن البيانات.
الإفصاح والنشر	يجب ألا يتم الكشف عن البيانات الحساسة دون موافقة. يجب ألا يتم نشر البيانات الحساسة علناً. دون موافقة مسؤول البيانات. يمكن لمجلس الجامعة الكشف عن المعلومات دون موافقة.
التبادل مع الأطراف الثالثة ومقدمي الخدمات	يكون ضمن الاتفاقيات التعاقدية (أو مذكرة تفاهم إذا كانت وكالة حكومية) التي تحدد المسؤوليات الأمنية التي يجب أن تكون سارية ومعتمدة من قبل مكتب الشؤون القانونية قبل تبادل البيانات مع الطرف الثالث / مزود الخدمة.
التخزين أو المعالجة: الخوادم	يجب أن تمتثل الخوادم لمتطلبات الأمان على النحو المبين في الحد الأدنى من معايير الأمان للأجهزة الحساسة.
التخزين أو المعالجة على الأجهزة الإلكترونية	يجب أن تمتثل الأنظمة لمتطلبات الأمان على النحو المبين في الحد الأدنى من معايير الأمان للأجهزة الحساسة.
التخزين على الأقراص المتحركة	يجب تخزين البيانات الحساسة فقط على وسائط قابلة للإزالة بتنسيق ملف مشفر أو داخل وحدة تخزين مشفرة.
الإرسال الإلكتروني	يجب استخدام اتصالات آمنة أو مصدق عليها أو بروتوكولات آمنة لنقل البيانات المقيدة .
البريد الإلكتروني والرسائل الإلكترونية الأخرى	لا يتم إرسال الرسائل إلا إلى الأفراد المصرح لهم. في حالة الحصول على إذن, يتم تضمين البيانات فقط في الرسائل داخل مرفق ملف مشفر أو عبر أنظمة آمنة معتمدة
طباعة, بريد الإلكتروني، فاكس	يجب توزيع أو إتاحة المواد المطبوعة التي تتضمن بيانات سرية فقط للأشخاص المصرح لهم يجب تقييد الوصول إلى أي منطقة يتم فيها تخزين السجلات المطبوعة ذات البيانات المقيدة باستخدام عناصر التحكم (مثل الأقفال والأبواب والمراقبة وما إلى ذلك) الكافية لمنع الدخول غير المصرح به.
التصرف والإتلاف	يجب حذف البيانات حيث لا يمكن استردادها . يجب تدمير الوسائط المادية (مثل الورق, القرص المضغوط, الشريط , إلخ) بحيث لا يمكن استعادة البيانات الموجودة على الوسائط أو إعادة بنائها. بالنسبة للمستندات الداخلية ذات المحتوى الحساس مثل(الورق , القرص المضغوط , الشريط , إلخ) , يجب إتلافها أو تدميرها كاستخدام آلة تقطيع الورق. استخدم أدوات نظام التشغيل المساعدة لحذف الملفات. بالنسبة للأقراص الصلبة والمتحركة من أفضل الممارسات مسح هذه الأجهزة بأمان قبل التخلص منها.

سياسة تصنيف البيانات:

المواصفات الأساسية لحماية البيانات

3- مقيد

الجمع والاستخدام	أن يقتصر الاستخدام على المصرح لهم كما هو موضح في سياسة الخصوصية.
الوصول أو المشاركة	يجب استخدام طرق فعالة لضمان الوصول إلى البيانات المقيدة أو مشاركتها مع الاشخاص المصرح لهم أو الأشخاص الذين لديهم حاجة مشروعة إلى معرفتها. لتجنب الآثار السلبية الناجمة عن الوصول غير المصرح به.
الإفصاح والنشر	يجب أن تكون مشاركة أو الإفصاح عن البيانات ضمن القيود الداخلية للعمادة كما يوافق عليها مسؤول البيانات
التبادل مع الأطراف الثالثة ومقدمي الخدمات	يجب أن يكون الاستخدام في إطار الاتفاقيات لضمان تحديد وتوثيق مسؤوليات الطرف الثالث عن سرية / خصوصية البيانات.
التخزين أو المعالجة: الخوادم	يجب أن تتوافق الخوادم التي تتصل بشبكة جامعة بيشة مع الحد الأدنى من معايير الأمان للأجهزة المتصلة بالشبكة.
التخزين أو المعالجة على الأجهزة الإلكترونية	يجب أن تتوافق الأنظمة التي تتصل بشبكة جامعة بيشة مع الحد الأدنى من معايير الأمان للأجهزة المتصلة بالشبكة.
التخزين على الأقراص المتحركة	يجب تخزين البيانات الحساسة فقط على وسائط قابلة للإزالة بتنسيق ملف مشفر أو داخل وحدة تخزين مشفرة.
الإرسال الإلكتروني	يجب إرسال البيانات إما بتنسيق ملف مشفر أو عبر بروتوكول أو اتصال آمن.
البريد الإلكتروني والرسائل الإلكترونية الأخرى	استخدم طرق تتطلب من المستلم المصادقة قبل الاستلام, مثل البريد الإلكتروني , أو موقع ويب يتطلب تسجيل دخول عبر الويب , أو خادم ملفات يتطلب كلمة مرور. أو استخدم خدمة البريد الإلكتروني الآمنة لمزيد من البيانات الخاصة.
طباعة, بريد الإلكتروني، فاكس	يتم الإرسال بطريقة تحمي المعلومات من القراءة العرضية.
التصرف والإتلاف	يجب حذف البيانات حيث لا يمكن استردادها يجب تدمير الوسائط المادية (مثل الورق, القرص المضغوط) بحيث لا يمكن استعادة البيانات الموجودة على الوسائط أو إعادة بنائها. بالنسبة للمستندات الداخلية ذات المحتوى الحساس مثل (الورق, القرص المضغوط) , يجب إتلافها أو تدميرها كاستخدام آلة تقطيع الورق. استخدم أدوات نظام التشغيل المساعدة لحذف الملفات. بالنسبة للأقراص الصلبة والمتحركة من أفضل الممارسات مسح هذه الأجهزة بأمان قبل التخلص منها.

سياسة تصنيف البيانات:

المواصفات الأساسية لحماية البيانات

4- عام

الجمع والاستخدام	لا قيود
الوصول أو المشاركة	لا قيود
الإفصاح والنشر	لا قيود
التبادل مع الأطراف الثالثة ومقدمي الخدمات	لا قيود
التخزين أو المعالجة: الخوادم	يجب أن تتوافق الخوادم التي تتصل بشبكة جامعة بيشة مع الحد الأدنى من معايير الأمان للأجهزة المتصلة بالشبكة.
التخزين أو المعالجة على الأجهزة الإلكترونية	يجب أن تتوافق الأنظمة التي تتصل بشبكة جامعة بيشة مع الحد الأدنى من معايير الأمان للأجهزة المتصلة بالشبكة.
التخزين على الأقراص المتحركة	لا قيود
الإرسال الإلكتروني	لا قيود
البريد الإلكتروني والرسائل الإلكترونية الأخرى	لا قيود
طباعة, بريد الإلكتروني، فاكس	لا قيود
التصرف والإتلاف	لا قيود

ثانياً: سياسة حماية البيانات الشخصية

الهدف

هذه السياسة هي بيان لالتزام الجامعة بحماية حقوق وخصوصية الأفراد وفقاً لقوانين حماية البيانات. تحدد هذه السياسة المسؤوليات لجميع المسؤولين والموظفين الشركاء أو أي شخص آخر يمكنه الوصول إلى البيانات الشخصية أو استخدامها في عملهم سواء للعمادة أو للجامعة.

المبادئ

- **ما هي المعلومات المدرجة في هذه السياسة؟**

تنطبق هذه السياسة على جميع البيانات الشخصية التي تم إنشاؤها أو تلقيها أو معالجتها في سياق أعمال الجامعة بجميع التنسيقات. قد يتم الاحتفاظ بالبيانات الشخصية أو نقلها في أشكال ورقية ومادية وإلكترونية أو نقلها شفهياً في محادثة أو عبر الهاتف.

- **على من تنطبق هذه السياسة؟**

تنطبق هذه السياسة على أي موظف يقوم بمعالجة البيانات الشخصية في سياق عمله أو مشاركته. أي طالب في الجامعة يقوم بمعالجة البيانات الشخصية أثناء دراسته. الأفراد الذين لا يعملون بشكل مباشر من قبل الجامعة, ولكنهم يعملون من قبل شركاء خارجيين, والذين يعالجون البيانات الشخصية في سياق واجباتهم.

- **أين تطبق السياسة؟**

تنطبق هذه السياسة على جميع المواقع التي يتم من خلالها الوصول إلى بيانات الجامعة الشخصية, بما في ذلك الاستخدام المنزلي (عن بعد).

تضمن جامعة بيشة الخصوصية المتوقعة لجميع الأفراد من خلال الامتثال للقواعد العامة ولائحة حماية البيانات وقانون حماية البيانات, وغيرها من التشريعات واللوائح ذات الصلة:

- حماية البيانات الشخصية للأفراد ومعالجتها فقط وفقاً لقانون حماية البيانات والممارسات الجيدة.
- الوضوح بشأن الكيفية التي يجب أن تتم بها معالجة البيانات الشخصية وتوقعات الجامعة لجميع أولئك الذين يعالجون البيانات الشخصية نيابة عنها.
- معالجة البيانات الشخصية بفعالية وكفاءة لتحقيق الأغراض التي من أجلها تم الحصول عليه.
- حماية سمعة الجامعة ومن خلال ضمان البيانات الشخصية الموكلة إليها.
- حماية الجامعة من أخطار خرق البيانات الشخصية وغيرها من انتهاكات قانون حماية البيانات, وبناء عليه من المسؤولية.

ثانياً: سياسة حماية البيانات الشخصية

سيتم توضيح نهج الجامعة في معالجة البيانات الشخصية من خلال مبادئ الحماية المنصوص عليها في اللائحة العامة لحماية البيانات. تتطلب هذه البيانات الشخصية أن:

- تتم معالجتها بطريقة قانونية وعادلة وشفافة (الشرعية والإنصاف والشفافية)
- تم جمعها فقط لأغراض محددة وصريحة وشرعية.
- أن تكون كافية وذات صلة ومحدودة لما هو ضروري فيما يتعلق بالأغراض التي من أجلها يتم معالجتها.
- دقيقة ومحدثة عند الضرورة.
- لا يتم الاحتفاظ بها في أي شكل يسمح بتحديد مواضيع البيانات لفترة أطول من الأغراض الضرورية التي تتم معالجة البيانات الشخصية من أجلها.
- تتم معالجتها بطريقة تضمن أمنها, باستخدام التقنية المناسبة والتدابير التنظيمية للحماية من المعالجة غير المصرح بها أو غير القانونية وضد الفقد أو التلف أو التلف العرضي (الأمن والنزاهة والسرية).

الجامعة مسؤولة عن البيانات, ويجب أن تكون قادرة على إثبات الامتثال لمبادئ الحماية المذكورة أعلاه (المساءلة) . منسوبي الجامعة والشركاء أو غيرهم ممن سيقوم بمعالجة البيانات الشخصية نيابة عن الجامعة إلى تفعيل هذه السياسة من خلال الامتثال لمعيار حماية البيانات والسياسات والإجراءات والعمليات ذات الصلة. كما تنص هذا المعايير على كيفية تفعيل بيان السياسة والامتثال للبيانات قانون الحماية.

المسؤوليات والأدوار

مسؤول البيانات والفريق التابع له هو المسؤول عن القيادة والحفاظ على ثقافة تحترم حماية البيانات الشخصية عبر الجامعة ويكون مسؤولاً عن معالجة البيانات الشخصية.
يتحمل جميع منسوبي الجامعة مسؤولية ضمان ذلك, ويلتزم موظفو الجامعة في نطاق مسؤوليتهم بهذه السياسة ويجب عليهم تنفيذ تلك الممارسات والعمليات والضوابط المناسبة والتدريب لضمان الامتثال.
يجب أن تكون القرارات المتخذة بموجب هذه السياسة قائمة على المخاطر, مع إشارة خاصة إلى المخاطر التي تتعرض لها المصالح والحقوق الأساسية لأصحاب البيانات. يجب تصعيد عملية صنع القرار إلى المستوى المناسب بناءً على المخاطر المطروحة.
جميع منسوبي الجامعة ممن يعالجون البيانات الشخصية نيابة عن الجامعة هم المسؤولون عن الامتثال لهذه السياسة وتنفيذ السياسة في عملهم. قد يؤدي عدم الامتثال لهذه السياسة إلى اتخاذ إجراءات تأديبية.
مسؤول حماية البيانات مسؤول عن الإشراف على هذه السياسة والعمليات التي تدعمها, وتطوير السياسات والمبادئ التوجيهية ذات الصلة, وتقديم المشورة للجامعة في تلك الالتزامات بموجب قانون حماية البيانات ومراقبة الامتثال.

ثانياً: سياسة حماية البيانات الشخصية

الضوابط والأحكام

ستقوم الجامعة بمعالجة البيانات الشخصية فقط بصورة عادلة وقانونية ولأغراض محددة. لا تهدف هذه القيود إلى منع المعالجة, ولكن تهدف إلى ضمان معالجتنا البيانات الشخصية لأغراض مشروعة دون المساس بحقوق وحريات البيانات المواضيع. لكي يتم تبرير ذلك, يجوز للعمادة معالجة البيانات الشخصية فقط إذا كانت تستند المعالجة المعنية إلى واحد (أو أكثر) من الأسس القانونية الموضحة أدناه.

الأسس القانونية لمعالجة البيانات الشخصية غير الحساسة هي كما يلي:

- تمت المواقفة من صاحب البيانات.
- أن تكون المعالجة ضرورية لأداء عقد مع موضوع البيانات.
- الوفاء بالالتزام والامتثال القانوني.
- الأداء مهمة للمصلحة العامة أو للوظائف الرسمية حيث إن المهمة أو الوظيفة لها أساس واضح في القانون.

ستحصل الجامعة على موافقة صاحب البيانات فقط عندما يكون هناك اختيار حقيقي وسيطرة حقيقية من قبل صاحب البيانات على الموافقة على المعالجة أو لا. سوف نعتمد على أسس قانونية أخرى عندما تكون مناسبة للمعالجة.

أن يشار إلى موافقة صاحب البيانات على معالجة بياناته الشخصية بوضوح, إما من خلال بيان أو إجراء في مستند يتعامل مع أمور أخرى, سوف نتأكد من أن الموافقة منفصلة ومتميزة عن تلك الأمور الأخرى.

سنعمل على تمكين أصحاب البيانات من سحب الموافقة على المعالجة بسهولة في أي وقت وسوف نحترم ذلك القرار على الفور. عندما تكون هناك تغييرات على معالجة البيانات الشخصية تختلف عن وتتعارض مع الأغراض الأصلية, سنقوم بتجديد الموافقة قبل أي معالجة.

سوف نضمن حصولنا على دليل الموافقة والاحتفاظ بسجل لجميع الموافقات التي تم الحصول عليها حتى نتمكن من إثبات الامتثال.

مطلوب من الجامعة تقديم معلومات مفصلة ومحددة لصاحب البيانات حول ماذا يحدث لبياناتهم الشخصية. تعتمد المعلومات المقدمة على ما إذا كان قد تم جمع المعلومات مباشرة من "صاحب البيانات" أو من مكان آخر. يجب أن تكون المعلومات التي تم تقديمها من خلال إشعارات الخصوصية المناسبة التي يجب أن تكون موجزة وشفافة ومفهومة, ويمكن الوصول إليها بسهولة, وبكلمات واضحة وبسيطة بحيث يمكن لصاحب البيانات فهم ما يحدث لبياناتهم الشخصية بسهولة. هذا سوف يدعم الجامعة لتلبية احتياجات والتزامات الشفافية.

يجب جمع البيانات الشخصية فقط لأغراض محددة وصريحة قانونية. لا يجوز أن تتم معالجتها بأي طريقة لا تتوافق مع تلك الأغراض. وبناءً عليه, لن تستخدم الجامعة البيانات الشخصية لأغراض جديدة تماماً أو مختلفة أو غير متوافقة مع الأغراض التي تم الكشف عنها عند الحصول عليها لأول مرة ما لم يكن صاحب البيانات على علم بالأغراض الجديدة وعند الضرورة أعطى الموافقة.

عندما لا تستند المعالجة الإضافية إلى موافقة صاحب البيانات أو على إعفاء قانوني من متطلبات قانون حماية البيانات, سنقوم بتقييم ما إذا كان الغرض الجديد متوافقاً من خلال اتباع إجراء تغيير أغراض المعالجة.

لن يتم اعتبار المعالجة الإضافية لأغراض الأرشفة للمصلحة العامة, وأغراض البحث العلمي, والأغراض الإحصائية غير متوافقة. سنتابع تغيير المعالجة للأغراض الإجرائية؛ لتحديد ما إذا كانت الضمانات كافية.

ثانياً: سياسة حماية البيانات الشخصية

الحد من البيانات

يجب أن تكون البيانات الشخصية كافية, وذات صلة ومحدودة لما هو ضروري فيما يتعلق بالأغراض التي تتم معالجتها من أجلها. ستضمن الجامعة أن البيانات الشخصية التي تعالجها كافية وذات صلة بالأغراض التي تهدف إلى معالجتها ولن تقوم بتجميع كميات كبيرة من البيانات الشخصية غير ذات الصلة بهذه الأغراض.
سيقوم موظفو الجامعة وغيرهم ممن يعالجون البيانات نيابةً عنها بمعالجة البيانات الشخصية فقط عند أداء واجباتهم الوظيفية التي تتطلب ذلك ولن يعالجوا البيانات الشخصية لأي سبب لا علاقة له بواجبات الوظيفة هذه.
سنضمن أنه عندما لا تكون هناك حاجة للبيانات الشخصية لأغراض محددة, يتم إتلافها بشكل آمن أو إخفاء هويتها وفقًا لجداول الاحتفاظ بالبيانات بالجامعة وإجراءات إتلاف البيانات الشخصية.

حماية البيانات الشخصية

ستؤمن الجامعة البيانات الشخصية من خلال التدابير التقنية والتنظيمية المناسبة ضد المعالجة غير المصرح بها أو غير القانونية, وضد الفقد أو التلف أو التلف العرضي. سنأخذ في الاعتبار المخاطر التي يتعرض لها أصحاب البيانات على وجه الخصوص عند تطوير وتنفيذ تعديل الضمانات.
ستشمل حماية البيانات استخدام التشفير والتسمية المستعارة عند الاقتضاء. ويشمل أيضاً حماية السرية (أي أنه فقط أولئك الذين يحتاجون إلى معرفة البيانات الشخصية والمصرح لهم باستخدامها يمكنهم الوصول إليها), وسلامة البيانات الشخصية وتوافرها. سنقوم بانتظام بتقييم واختبار فعالية تلك الضمانات؛ لضمان أمان معالجتنا للبيانات الشخصية.
سيكون موظفو الجامعة مسؤولين عن حماية البيانات الشخصية التي يعالجونها في سياق مهامهم. لذلك سوف نتعامل مع البيانات الشخصية بطريقة تحميها من الفقد أو الإفشاء العرضي أو غير ذلك من المعالجة غير المقصودة أو غير القانونية وبطريقة تحافظ على سريتها. سنبذل اهتماما خاصا في حماية البيانات الشخصية الحساسة من الضياع والوصول غير المصرح به أو الاستخدام أو التسريب.
سيلتزم موظفو الجامعة بالإجراءات الوقائية الإدارية والمادية والتقنية التي ننفذها, ولن يحاولوا التحايل عليها. وتشمل هذه السياسات ذات الصلة المشار إليها في المبدأ الأول وجميع العمليات والإجراءات المعمول بها, مع إشارة خاصة إلى سياسات وإجراءات تكنولوجيا المعلومات والاتصالات لإشراك الأطراف الثالثة في معالجة البيانات الشخصية.

ثانياً: سياسة حماية البيانات الشخصية

حقوق صاحب لبيانات

يتمتع أصحاب البيانات بحقوق تتعلق بالطريقة التي نتعامل بها مع بياناتهم الشخصية. ما لم يتم تطبيق استثناءات معينة, ويجب الامتثال لهذه الحقوق عادة في غضون شهر واحد من الاستلام. سيلتزم جميع موظفي الجامعة على الفور بإجراءات ممارسة حقوق اصحاب البيانات عند تلقي طلب اصحاب البيانات فيما يتعلق بحقوقهم التالية:

الحقوق	التفاصيل
المعرفة	يحق للأفراد الحصول على معلومات واضحة وموجزة حول ما نفعله ببياناتهم الشخصية. يجب إخبار الأفراد قبل استخدام بياناتهم.
الوصول	للأفراد الحق في الوصول إلى بياناتهم الشخصية والتأكد من أن معالجة بياناتهم عادلة وقانونية.
التعديل	للأفراد الحق في تصحيح بياناتهم الشخصية إذا كانت غير دقيقة, أو أن تكون مكتملة إذا كانت غير كاملة.
المسح / الإتلاف	للأفراد الحق في محو بياناتهم الشخصية في ظروف معينة.
تقييد المعالجة	للأفراد الحق في طلب تقييد أو حذف بياناتهم الشخصية في ظروف معينة. (الاحتفاظ بالبيانات, ولكن دون الاستخدام, عادة لفترة من الوقت في انتظار قرارات أخرى)
نقل البيانات	يحق للأفراد الحصول على بياناتهم الشخصية وإعادة استخدامها عبر خدمات مختلفة. (نقل البيانات الشخصية أو نسخها أو نقلها بسهولة من بيئة تقنية معلومات إلى أخرى بأمان دون التأثير على قابلية استخدام البيانات)
الاعتراض	يحق للأفراد الاعتراض على معالجة بياناتهم الشخصية حيث تستند المعالجة إلى المصالح المشروعة أو أداء مهمة المصلحة العامة, أو عندما تكون المعالجة للتسويق المباشر أو البحث العلمي / التاريخي والإحصاءات.

طلبات الوصول إلى البيانات

يحق لأصحاب البيانات الحصول على نسخة من بياناتهم الشخصية التي تحتفظ بها الجامعة.
بالإضافة إلى ذلك يحق لهم تلقي مزيد من المعلومات حول معالجة الجامعة لبياناتهم الشخصية على النحو التالي:

- الأغراض من الجمع والمعالجة.
- نوع البيانات الشخصية التي تتم معالجتها
- المستلمين / فئات المستلمين
- فترات التخزين
- معلومات عن حقوقهم
- أي مصدر خارجي / طرف ثالث للبيانات الشخصية

سيلتزم جميع موظفي الجامعة بإجراء الاستجابة لطلبات الوصول لأصحاب البيانات.

ثالثاً: سياسة مشاركة البيانات

الهدف

كما أن أحد أهم أهداف الموقع , هو أن تكون واجهة إعلامية معرفية لجامعة بيشة , وأداة للتيسير على المستفيدين من خدماتها عبر تقديم خدمات إلكترونية فعالة, بالإضافة إلى زيادة الوعي ونشر المعرفة والتأكيد على مبدأ المشاركة والحوار البناء فضلاً عن استعراض دور الجامعة في مسيرة التنمية المستدامة في المملكة بشكل عام وتطور قطاع التعليم الجامعي بشكل خاص, وبناء عليه فإن استخدام كل ما يرد بالموقع إنما يعنى به الاستزادة العلمية والمعرفية والثقافية, وهو ما يجعل استخدام أية معلومات ترد بالبوابة على مسؤولية المستخدم الشخصية.

المبادئ

نوقد حددت إدارة الموقع عدداً من الشروط والبنود التي تتضمن سياسة الاستخدام بحيث تحدد العلاقة بين الموقع من جهة, والمستخدمين المستفيدين منها من الجهة الأخرى؛ بدوره يضمن تقديم خدمة أفضل تساعد على تحقيق استفادة أكبر من محتويات الموقع (البوابة) من معلومات.
وبما أن هذه الموقع متاح للاستخدام الشخصي؛ فإن الدخول واستخدام هذه الموقع يخضع لبنود وشروط الاستخدام, ولأنظمة المملكة العربية السعودية, كما يعد الوصول إلى هذه الموقع والدخول إليها موافقة دون قيد أو شرط على بنود وشروط الاستخدام سواء كان المستخدم مسجلاً أم لم يكن, وتسري هذه الموافقة اعتباراً من تاريخ أول استخدام لهذه البوابة.
كما أن مستخدم الموقع الإلكتروني لجامعة بيشة, يجب أن يقر بالامتناع عن الآتي:

1. استخدام الموقع بأية طريقة لإرسال بريد إلكتروني تجاري أو غير مرغوب فيه أو أية إساءة استخدام لبوابة الجامعة.
2. توفير أو تحميل ملفات على هذه الموقع تحتوي على فيروسات أو بيانات تالفة.
3. نشر, أو إعلان, أو توزيع, أو تعميم مواد, أو معلومات تحتوي تشويهاً للسمعة, أو انتهاكاً للقوانين, أو مواد إباحية, أو بذيئة, أو مخالفة للتعاليم الإسلامية ,أو للآداب العامة أو أي مواد أو معلومات غير قانونية من خلال البوابة.
4. الاشتراك من خلال الموقع في أنشطة غير مشروعة أو غير قانونية في المملكة العربية السعودية.
5. الإعلان على الموقع عن منتج أو خدمة تجعل الجامعة في وضع انتهاك لأي قانون أو نظام مطبق في أي مجال.
6. استخدام أية وسيلة, أو برنامج, أو إجراء لاعتراض, أو محاولة اعتراض التشغيل الصحيح للبوابة.
7. القيام بأي إجراء يفرض حملاً غير معقول أو كبيرا أو بصورة غير مناسبة على البنية التحتية لمنصة الجامعة.

ثالثاً: سياسة مشاركة البيانات

المسئوليات والادوار

جميع الخدمات الإلكترونية التي تقدمها الموقع الإلكترونية لجامعة بيشة عبر شبكة الإنترنت والحصول على معلومات بشأن الوكالات, الإدارات, العمادات, الكليات, الأقسام وجميع الجهات المختلفة التابعة للجامعة يتم تقديمها فقط لتسهيل الإجراءات.

وبهذا يقر المستخدم بكامل علمه بأن الاتصالات عبر الإنترنت قد تتعرض إما للتدخل أو الاعتراض بواسطة الغير. وبناء عليه, فإن اللجوء إلى هذه الموقع يظل على مسؤولية المستخدم الخاصة, والموقع لا تتحمل بأي حال من الأحوال المسؤولية عن أي نوع خسارة أو ضرر قد يحدث للمستخدم بسبب استخدامه أو زيارته للمنصة أو اعتماده على أي بيان أو إعلان فيها أو ما قد ينجم عن أي تأخير في التشغيل أو تعثر الاتصال أو مشاكل الدخول إلى شبكة الإنترنت, أو أعطال المعدات, أو البرامج, أو سلوك, أو أفكار أي شخص يدخل إلى هذه الموقع.

وبهذا يقر المستخدم هنا ويوافق على أن الوسيلة الحصرية والوحيدة لعلاج أي ضرر أو خسارة قد تحدث نتيجة دخوله أو استخدامه لهذه البوابة هي الامتناع عن استخدامها أو الدخول إليها أو عدم الاستمرار في ذلك

الضوابط والأحكام

1. يتم تحديد الخدمة إذا ما كان الطلب يتعلق ببيانات عامة أو خاصة أو مجموعة من البيانات العامة والخاصة.
2. يحتاج مقدمو طلبات الحصول على البيانات الخاصة لإثبات "مصلحة تعليمية مشروعة". سيتم مراجعة الطلبات والموافقة عليها على أساس كل حالة على حدة من قبل مالك البيانات المطلوبة أو من قبل مسؤول البيانات في الجامعة.
3. وفقًا لتقدير مالك البيانات أو مسؤول البيانات, قد تتطلب الطلبات تقريرا مكتوباً حول كيفية استخدام البيانات وتخزينها بالإضافة إلى توقيع اتفاقية عدم الإفشاء.
4. يجب أن تطرح الاستفادة من التقارير العامة الحالية قبل اتخاذ إجراء آخر يتعلق بالبيانات الخاصة.
5. اعتماداً على نوع متطلبات الطلب المقدم, يجب إلغاء تصنيف البيانات المصنفة على أنها خاصة قبل المشاركة. في حال ليس من الممكن إلغاء تصنيف البيانات الخاصة, فقد يكون من الضروري وجود اتفاقية عدم الإفشاء.
6. عندما تتطلب حالة معينة إخفاء البيانات, يجب على إدارة البيانات تقييم الطلب حسب تصنيف وتأثير البيانات قبل مشاركة البيانات الخاصة.
7. عند مشاركة البيانات, يجب أن تقتصر البيانات والتقارير على النطاق والعمق الذي يتوافق مع احتياجات الطلب.
8. ستتم مشاركة البيانات بعدة طرق, بما في ذلك الطرق التالية:
   - عبر الويب.
   - من خلال طلبات التقارير المخصصة.
   - من خلال الإصدار العام عبر أنظمة التقارير الفرعية أو الإعلامية
9. كل مواد المحتوى المنشورة على الموقع وكذلك المواقع التابعة لها تخضع لحقوق الملكية الفكرية بما في ذلك النصوص, أو الرسوم, أو الصور, أو البرامج, أو التصاميم وغيرها.
10. تسمح إدارة الموقع للمستخدمين باستعراض وتصفح الموقع, والطباعة وذلك من أجل الاستخدام الشخصي فقط.
11. يسمح فقط للمستخدم الشخصي وللاستخدام البحثي أو التعليمي بالاستفادة من محتوى الموقع وأية معلومات منشورة عليها مع ضرورة الإشارة إلى أن موقع جامعة بيشة هو مصدر ذلك المحتوى.
12. يحق لإدارة الموقع وحسب تقديرها المطلق إنهاء أو تقييد أو إيقاف الحق في الدخول إلى البوابة واستخدامها, وذلك دون إشعار ولأي سبب بما في ذلك مخالفة شروط وقوانين الاستخدام أو أي سلوك آخر قد تعتبره الإدارة حسب تقديرها الخاص غير قانوني أو مضراً بالآخرين, وفي حالة الإنهاء, فإنه لن يكون مصرحاً للمستخدم الدخول إلى هذه الموقع.

رابعاً: سياسة حرية المعلومات

الهدف

تنطبق هذه السياسة, جنبًا إلى جنب مع سياسة حرية المعلومات, على جميع المستندات التي تحتفظ بها الجامعة أو نيابة عنها. يتضمن ذلك المستندات التي تم إنشاؤها أو استلامها من قبل الموظفين وأصحاب حقوق الملكية والمقاولين الذين يعملون نيابة عن الجامعة.
تتم تغطية المستندات بأي تنسيق, بما في ذلك رسائل البريد الإلكتروني والبيانات الإلكترونية المخزنة على قواعد البيانات والخوادم ومحركات الأقراص الثابتة

المبادئ

المبادئ العامة - وصول الأفراد إلى وثائق الجامعة

- يحق للأفراد الوصول إلى المستندات التي تحتفظ بها الجامعة, مع مراعاة الإعفاءات المحددة في سياسة حرية المعلومات على أنها تتماشى مع المصلحة العامة, بما في ذلك الحفاظ على الخصوصية الشخصية والحفاظ على السرية.
- بصرف النظر عن هذا الحق العام في الوصول, تدرك الجامعة قيمة المعلومات التجارية السرية للعمادة وغيرها. ستسعى الجامعة جاهدة؛ لتنفيذ وإدارة العمليات والبنود التعاقدية التي تحدد بوضوح المعلومات السرية وتديرها, بحيث يمكن للإعفاء المصرح به بموجب سياسة حرية المعلومات للعقود التي تحتوي على شروط سرية توفير الحماية المناسبة.
- حيثما كان ذلك مناسباً ومسموحاً به قانوناً, ستوفر الجامعة الوصول إلى المعلومات بطريقة تطوعية وتعاونية دون الحاجة إلى أولئك الذين يسعون للحصول على معلومات للجوء إلى الطلبات بموجب سياسة حرية المعلومات.
- عندما تكون الطلبات بموجب قانون حرية المعلومات ضرورية و / أو مقدمة, ستقوم الجامعة بمعالجة وتحديد جميع الطلبات وفقاً للقانون وبالرجوع إلى القيم التي تقوم عليها الخطة الاستراتيجية للعمادة, وخاصة قيم الإنصاف والنزاهة وحرية الاستفسار.
- في القرار النهائي للطلبات بموجب قانون حرية المعلومات, يجب تسهيل الوصول إلى المستندات المطلوبة حيثما كان ذلك مناسباً وقانوناً. يجب ممارسة الحرمان من الوصول أو تقييده بشكل مسؤول, وفقط عند الضرورة وبصورة قانونية بموجب القانون.
- ستضمن الجامعة تعيين مسؤولين عن تنفيذ سياسة حرية المعلومات معتمدين حسب الضرورة لتسهيل الإدارة الملائمة لواجبات الجامعة بموجب قانون حرية المعلومات.

العقود السرية

عندما يلزم إبقاء بعض أو كل شروط وثيقة العقد سرية من قبل الجامعة, يجب أن تتم الموافقة على بند السرية الذي ينفذ هذا الالتزام من قبل عميد الجامعة أو وكيله أو من ينوب عنهم قبل الانتهاء من العقد

الإدارة العامة للإتصالات وتقنية المعلومات
General Administration for
Communicatiom and Information Technology

خامساً: سياسة البيانات المفتوحة

الهدف

تنطبق أحكام هذه السياسة على جميع البيانات والمعلومات العامة (غير السرية المحمية)، والتي تمتلكها جامعة بيشة مهما كان مصدرها أو شكلها أو طبيعتها، ويشمل ذلك السجلات الورقية ورسائل البريد الإلكتروني والمعلومات المخزنة على الحاسوب، أو أشرطة الصوت، أو الفيديو، أو الخرائط، أو الصور الفوتوغرافية، أو المخطوطات، أو الوثائق المكتوبة بخط اليد، أو أي شكل من أشكال المعلومات المسجلة.

المبادئ

تضمن هذا المبدأ إتاحة بيانات جامعة بيشة للجميع من خلال الإفصاح عنها وتمكين الوصول إليها واستخدامها، مالم تقتضِ طبيعتها عدم الإفصاح عنها أو حماية خصوصيتها أو سريتها.
يتم إتاحة البيانات وتوفيرها بصيغة مقروءة آلياً تسمح بمعالجتها بشكل آلي، بحيث يتم حفظها بصيغ الملفات شائعة الاستخدام مثل (CSV, XLS, JSON, XML)
يتم نشر أحدث إصدار من مجموعات البيانات (Data Sets) المفتوحة بصفة منتظمة ودورية وإتاحتها للجميع حال توافرها، كما يتم نشر البيانات المجمعة من قبل جامعة بيشة في أسرع وقت ممكن بعد جمعها، وتعطى الأولوية للبيانات التي تقل فائدتها بمرور الوقت.
تلتزم جامعة بيشة بأن تكون مجموعات البيانات المفتوحة شاملة لتتضمن أكبر قدر ممكن من التفاصيل، وأن تعكس البيانات المسجلة بما لا يتعارض مع سياسة الخصوصية وحماية البيانات الشخصية، كما يحرص جامعة بيشة على إدراج وإتاحة البيانات الوصفية التي توضح وتشرح البيانات الأولية، مع تقديم التفسيرات أو المعادلات التي توضح كيفية استخلاص المعلومات من تلك البيانات أو احتسابها.
تلتزم جامعة بيشة بإتاحة مجموعات البيانات للجميع دون تمييز ودون الحاجة إلى تسجيل.
تخضع البيانات المفتوحة لترخيص يحدد الأساس النظامي لاستخدام البيانات المفتوحة وكذلك الشروط والالتزامات والقيود المفروضة على المستخدم كما يدل استخدام البيانات المفتوحة على قبول شروط الترخيص.
تخضع البيانات المفتوحة لترخيص يحدد الأساس النظامي لاستخدام البيانات المفتوحة وكذلك الشروط والالتزامات والقيود المفروضة على المستخدم كما يدل استخدام البيانات المفتوحة على قبول شروط الترخيص.

تمكّن البيانات المفتوحة عملية الاطلاع والمشاركة للجميع، وتعزز شفافية ومساءلة الجهات ودعم عملية صنع القرار وتقديم الخدمات.
الالتزام بالقيام بدور فاعل في تعزيز إعادة استخدام البيانات المفتوحة وتوفير الموارد والخبرات اللازمة الداعمة، وأن تعمل بتكامل بين الأطراف المعنية على تمكين الجيل القادم من المبتكرين في مجال البيانات المفتوحة وإشراك الأفراد والمؤسسات والجميع بوجه عام في إطلاق قدرات البيانات المفتوحة.

خامساً: سياسة البيانات المفتوحة

مستخدمو البيانات المفتوحة

تتيح جامعة بيشة لمستخدمي الموقع الالكتروني الخاص بها (https://www.ub.edu.sa), الاطلاع على البيانات المفتوحة مجاناً, كما أن لهم الحق في الاستفادة من هذه البيانات على مسؤوليتهم الشخصية, وهذا الحق مكفول لكافة المستفيدين كما أنها تقدم مجانًا.

إن مستخدم البيانات المفتوحة مسؤولاً عن إعادة استخدام البيانات في موقع جامعة بيشة الإلكتروني، ولا يجب أن ينتج عن إعادة استخدام هذه البيانات أي أخطاء تتعلق بمحتوى البيانات ومصدرها وتاريخها.

إن جامعة بيشة غير مسؤولة عن أي أضرار أو سوء استخدام قد يؤدي الى التعرض للمسألة نتيجة استخدام هذه البيانات المنشورة بموقع جامعة بيشة الإلكتروني، كما أن جامعة بيشة لا تضمن استمرارية توافر تلك البيانات أو جزء منها, كما لا تتحمل جامعة بيشة أي مسؤولية تترتب على ذلك.

الضوابط والأحكام

- يجب عند استخدام هذه البيانات الإشارة إلى أن مصدرها (موقع جامعة بيشة الإلكتروني).
- يجب على المستخدم عدم تحريف هذه البيانات أو مصدرها.
- يجب ألا تستخدم هذه البيانات في أغراض دينية أو سياسية أو لدعم نشاط غير مشروع أو إجرامي أو في تعليقات عنصرية, أو تميزية, أو التأجيج, أو التأثير السلبي في الثقافة, أو التحريض, أو أي نشاط غير نظامي أو مخالف لشريعة المملكة وعاداتها وتقاليدها وقوانينها النظامية.
- يجب الإشارة إلى مصدر المعلومات التي تم إعادة استخدامها عن طريق وضع رابط موقع جامعة بيشة الإلكتروني أو المصادر الأخرى للمحافظة على حقوق الملكية الفكرية للبيانات ومصداقيتها وصحة مصدرها.
- يتم نشر هذه السياسة في موقع الجامعة الإلكتروني.
- سياسة البيانات المفتوحة مستمدة من سياسات حوكمة البيانات الوطنية الصادر عن الهيئة السعودية للبيانات والذكاء الاصطناعي ولمزيد من التفاصيل حول المبادئ الرئيسية والقواعد العامة للبيانات المفتوحة والمبادئ الرئيسية والقواعد العامة لحرية المعلومات يمكن الاطلاع على سياسات حوكمة البيانات الوطنية

الإدارة العامة للإتصالات وتقنية المعلومات
General Administration for
Communicatiom and Information Technology

سادساً: سياسة أرشفة البيانات

النطاق

تنظيم أعمال حفظ الوثائق في الجامعة بما يحقق المحافظة على الوثائق والمحفوظات وصيانتها وتصنيفها وفهرستها وبما يكفل سرعة الرجوع إلى ما تدعو الحاجة إليه والإشراف على تحويل الوثائق والمحفوظات وأرشفتها إلكترونياً وتنظيم عمليات التداول والسيطرة على حجم تضخم المحفوظات مستقبلاً.

المبادئ

- إعداد الخطة السنوية للجامعة وتنفيذها بعد اعتمادها.
- الإشراف على تحويل الوثائق والمحفوظات في الجامعة إلى أنظمة الأرشفة الإلكترونية.
- اقتراح السياسات والقواعد والإجراءات المنظمة للعمل في الجامعة ومتابعة تنفيذها بعد اعتمادها.
- وضع التنظيمات الفنية والقواعد والتعليمات اللازمة لإنتاج وتصنيف وترميز وفهرسة وحفظ واسترجاع وفرز وترحيل وإتلاف وثائق ومحفوظات الجامعة ومتابعة تطبيقها بالتنسيق مع الوحدات الإدارية الأخرى في الجامعة.
- تهيئة وتجهيز مستودع الحفظ بجميع ما يحتاج إليه من أجهزة وأدوات ووسائل تمكنه من حفظ الوثائق والمحافظة عليها.
- إجراء الفرز الدوري لمحتويات المستودع من الوثائق غير النشطة وتطبيق لوائح الفرز والترحيل والإتلاف عليها.
- التنسيق والتعاون مع المركز الوطني للوثائق والمحفوظات والمراكز الأخرى المشابهة في مجال العمل.
- إصدار وتحديث أدلة العمل في المركز.
- تنظيم العمل داخل المركز وإعداد دليل لإجراءات العمل يشمل جميع أعمال المركز.
- إعداد وتطوير النماذج اللازمة لسير عمل المركز.
- وضع معايير لقياس الأداء لجميع الأنشطة المتعلقة بالمركز ومراجعتها وتطويرها بصفة مستمرة.
- تنظيم وحفظ الوثائق الخاصة بالمركز بالطريقة التي تسهل سرعة استرجاعها والاستفادة منها.
- تحديد احتياجات المركز من الموارد البشرية والأجهزة والمواد ومتابعة توفيرها.
- تقديم تقارير دورية عن إنجازات المركز واقتراحات تطوير العمل بها.

سادساً: سياسة أرشفة البيانات

النطاق

تنقسم مراحل الأرشفة الإلكترونية إلى مرحلتين أساسيتين:

مراحل التخطيط للأرشفة الإلكترونية:

1. مرحلة الدراسة والمسح: وتتمثل في حصر الوثائق المزمع رقمنتها وتحديد كميتها وأشكالها وأنواعها التي تختلف حسب اللون /الحجم/ الجودة الورقية.
2. مرحلة التحليل: وتتمثل في تحديد الأولويات لتحويل الوثائق من الورقية إلى الإلكترونية وإعداد قوائم تتضمن البيانات الأساسية للوثائق كتحديد أماكنها وعناوين تواجدها وحفظها ودرجة نشاطها...إلخ. وهو بمثابة الجرد الكامل للوثائق.
3. مرحلة بناء الخطة: وتتمثل في وضع خطة لحفظ الوثائق: أي قواعد لمدد استبقائها أي مدة حفظها وتاريخ وتقرير مصيرها النهائي وتحديد تاريخ إتلافها أو ترحيلها. وكذلك تحديد نظام لتصنيف الوثائق أي بإسناد رموز تصنيفية لها ومكنز يحتوي على مصطلحات موحدة ككلمات مفتاحية لاستعمالها عند البحث واسترجاع الوثيقة.
4. مرحلة اختيار البرمجيات: وتشمل التجهيزات الالية والبرمجيات المختصة بالتصرف الإلكتروني في الوثائق والمنظومات وقواعد البيانات اللزمة ووضع الحقول المناسبة اختيار أدوات البحث وإعداد التقارير المطلوبة...إلخ.
5. مرحلة إعداد قواعد البيانات: وتتمثل في أعداد قواعد للبيانات التي ستتضمنها حفظ ومعالجة الوثائق الإلكترونية.

المراحل التنفيذية للأرشفة الإلكترونية

أولا: مرحلة تحضير الوثائق والملفات:

- استبعاد الأوراق المكرره والتي لن يتم أرشفتها.
- تصوير بعض الوثائق القديمة يدويا حتى نستطيع تصويرها ضوئيا.
- إزالة الدبابيس الموجودة على الوثائق.
- فصل الأوراق إلى مجموعات حسب الحجم أو التي تحتوى على ألوان أو التي تحوى بيانات على الوجهين...إلخ.
- وضع علامات مميزه على الوثائق وتسهيل عملية تجميعها كما كانت قبل التصوير الضوئى.

ثانيا: مرحلة التصوير الضوئى:

تتم عملية التصوير الضوئى للوثائق التي تم تحضيرها سابقا بواسطة أجهزة المسح الضوئى المناسبة لحجم الوثيقة ووضوحها, وعملية التصوير الضوئى هي الخطوة الأولى لتحويل الملفات الورقيه إلى ملفات إلكترونية يتم تخزينها على أجهزة الحاسب الإلى.كما لابد من التركيز على الأجهزة المطلوبه للتخزين, نوع الملف الإلكترونى.استخدام خاصية ضغط الملفات, صلاحيات الإطلاع والتغيير... إلخ

ثالثا: مرحلة مراقبة وتدقيق الجودة:

هي مرحلة تتم بالتوازى مع عملية التصوير الضوئى حيث يقوم الموظف الذي يصور الملفات ضوئيا أو أي موظف أخر تكون مهمته مراقبة الجودة بالتدقيق على الملفات المصورة ضوئيا ومقارنتها بالأصل للتأكد من وضوحها وجودتها وعدم ضياع أي معلومه قد تحتويها الوثيقة.

رابعا: مرحلة الفهرسة:

هي مرحلة إدخال البيانات والفهارس المتعلقه بالملفات والأوراق التي يتم تصويرها وهي عملية فهرسة مادية ووصفية وتكشيف للوثائق من أجل إقامة ربط بين البطاقة الفهرسية والملف المرافق لهذه الصورة وهذا بإعطاء كاشف وحيد يتم تدوينه على الوثيقة المرقمنه وعلى بطاقة التكشيف. ويمكن أن يتم التكشيف يدويا أو اليا؛ حيث أن التكشيف اليدوى هو عبارة عن تلخيص أو تحليل للوثيقه والذي يمكن أن يتم بكشاف يحتوى على الكلمات الواصفات.

أما التكشيف الإلى (الأوتوماتيكي): هي طريقة التكشيف الأكثر استعمالا حيث يتم استخلاص كل المصطلحات وتشكيل كشاف عام مع الاستغناء عن كلمات أو أدوات الربط؛ ويمكن استعمال برمجيات في عملية التكشيف؛ إما أن تكون معدة خصيصا للهيئة أو تكون برمجيات عامة.

خامسا: مرحلة إعادة الملفات إلى أصولها:

وتتمثل هذه العملية في إعادة الملفات والوثائق التي كانت في طور التصوير الضوئى إلى بعضها وإلى أصولها التي كانت عليها قبل الرقمنه وذلك بإعادة تدبيسها بعد فكها من بعضها.

سادسا: مرحلة الحفظ والخزن

تتم مرحلة حفظ وخزن الوثائق في وسئط ودعائم مختلفه منها ذاكرة الحاسب نفسه ومنها الأقراص الممغنطة والمدمجه وكذلك في النظم المركزية وهي طريقة الحفظ الاحتياطى.

سابعا: الاطلاع على الأرشيف الإلكترونى (تبليغ وتوزيع الأرشيف الإلكتروني):

إن رقمنة الأرصدة الأرشيفية وإنفاق المبالغ المالية والبشرية والتجهيزيه عليها ليس بغرض الحفظ فقط وإنما لهدف أهم وهو تبليغ الأرشيف للمستفيدين والاطلاع عليه بشكل مباشر أو غير مباشر.

المصادر والمراجع:

- دليل سياسات إدارة وحوكمة البيانات - جامعة بيشة (الإصدار الاول ١٤٤٣هـ - ٢٠٢٢م).
- وثيقة الخطة الإستراتيجية لجامعة بيشة (٢٠١٧ -٢٠٢٢م).
- وثيقة الخطة الإستراتيجية للتحول الرقمي بجامعة بيشة (٢٠٢٢-٢٠٢٦م).
- وثيقة الخطة الإستراتيجية للإدارة العامة للإتصالات وتقنية المعلومات بجامعة بيشة (٢٠٢٢-٢٠٢٦م)
- الهيئة السعودية للبيانات والذكاء الإصطناعي. (بلا تاريخ). الإستراتيجية الوطنية للبيانات والذكاء الإصطناعي. تم الاسترداد من https://ai.sa/index-ar.html
- مكتب إدارة البيانات الوطنية. (25 11, 2020). القواعد العامة لنقل البيانات الشخصية خارج الحدود الجغرافية للمملكة. تم الاسترداد من https://sdaia.gov.sa/ndmo/Files/Policies003.pdf
- مكتب إدارة البيانات الوطنية. (2020). سياسة حماية البيانات الشخصية للأطفا ل ومن في حكمهم. تم الاسترداد من https://sdaia.gov.sa/ndmo/Files/Policies002.pdf
- مكتب إدارة البيانات الوطنية. (2021). ضوابط ومواصفات إدارة البيانات الوطنية. تم الاسترداد من https://sdaia.gov.sa/ndmo/Files/Policies001.pdf
- هيئة الحكومة الرقمية. (29 9, 2021). سياية الحكومة الرقمية. تم الاسترداد من https://dga.gov.sa/dga?id=
- هيئة الحكومة الرقمية. (30 3, 2022). المعايير الأساسية للتحول الرقمي. المملكة العربية السعودية.

الملحقات:

الإدارة العامة للإتصالات وتقنية المعلومات
General Administration for
Communicatiom and Information Technology

قرار إعتماد إعادة هيكلة الإدارة العامة للاتصالات وتقنية المعلومات:

Kingdom Of Saudi Arabia
Ministry Of Education
University Of Bisha

المملكة العربية السعودية
وزارة التعليم
جامعة بيشة

جامعة بيشة
UNIVERSITY Of BISHA

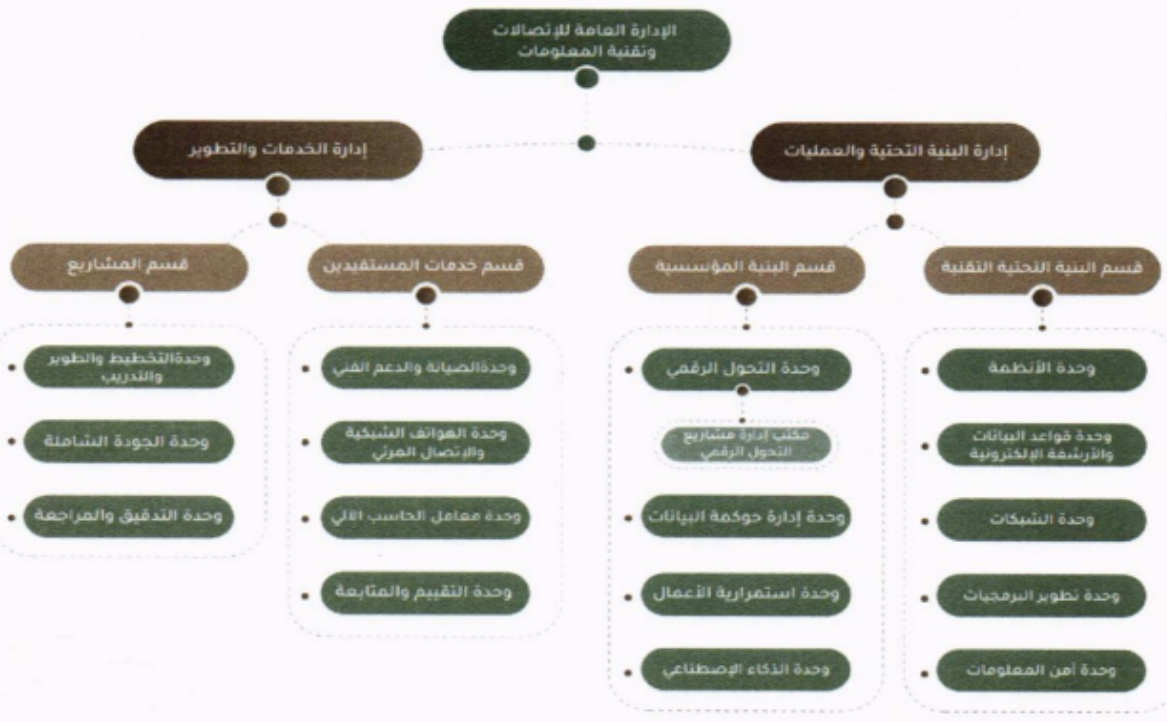
الموضوع الأول

إعادة هيكلة الإدارة العامة للاتصالات وتقنية المعلومات

القرار أو التوصية 43/42/3/1

تم عرض الموضوع للمناقشة والاستماع إلى أراء جميع أعضاء اللجنة وبعد دراسة الموضوع دراسة مستفيضة من قبل أعضاء اللجنة، اتخذت اللجنة القرار التالي:

- اعتماد الهيكل التنظيمي للإدارة العامة للاتصالات وتقنية المعلومات (مرفق رقم 1)



مرفق (1)

الإدارة العامة للإتصالات وتقنية المعلومات
General Administration for
Communicatiom and Information Technology

قرار تكليف مدير إدارة البنية التحتية والعمليات:

Kingdom of Saudi Arabia
Ministry of Education
University of Bisha
(058)
President Office

المملكة العربية السعودية
وزارة التعليم
جامعة بيشة
(٠٥٨)
مكتب رئيس الجامعة

جامعة بيشة
UNIVERSITY OF BISHA

معتمد
ACCREDITED

قرار إداري

إن رئيس الجامعة:

- بناءً على الصلاحيات الممنوحة له نظاماً.
- وبناءاً على توصيات اللجنة الدائمة للتعاملات الالكترونية بجلستها يوم الأحد الموافق ١٤٤٣/١٠/٢١هـ الموافق ٢٠٢٢/٥/٢٢م.
- وبناءً على ما تقتضيه مصلحة العمل.

يقرر ما يلي

أولاً: تكليف المهندس/ ناصر بن سليمان المطيري، بالعمل مديراً لإدارة البنية التحتية والعمليات، والتابعة للإدارة العامة للاتصالات وتقنية المعلومات.

ثانياً: يُعمل بهذا القرار اعتبارا من تاريخه، ولمدة عام.

ثالثاً: يلغي هذا القرار جميع ما يتعارض معه من قرارات سابقة.

رابعاً: يُبلغ هذا القرار لمن يلزم لإنفاذه.

وبالله التوفيق.....

رئيس الجامعة

أ.د. محمد بن محسن صفحي

الرقم: ..... التاريخ: / / المرفقات: .....

ص.ب 551 الرمز البريدي 61922
البريد الإلكتروني: ub@ub.edu.sa
هاتف : 966176238888+
فاكس : 966176238095+

www.UB.edu.sa
نحو مجتمع معرفي مبدع

قرار تكليف رئيس قسم البنية المؤسسية:

المملكة العربية السعودية
وزارة التعليم
جامعة بيشة

جامعة بيشة
UNIVERSITY OF BISHA

Kingdom of Saudi Arabia
Ministry of Education
University of Bisha

قرار إداري

إن مدير الإدارة العامة للاتصالات وتقنية المعلومات

- بناءً على الصلاحيات الممنوحة له.
- وبناءاً على قرار سعادة رئيس الجامعة بتكليف م. يحيى بن علي محمد شراحيلي مديراً للإدارة العامة للاتصالات وتقنية المعلومات رقم 58/4/105 وتاريخ 1442/03/16هـ.
- وبناءً على ما تقتضيه مصلحة العمل.

قرر ما يلي:

أولاً: تكليف م. ناصر بن سليمان المطيري، مديراً لقسم البنية المؤسسية، والتابعة للإدارة البنية التحتية والعمليات.

ثانياً: يُعمل بهذا القرار اعتبارا من تاريخه ولمدة عام.

ثالثاً: يلغي هذا القرار جميع ما يتعارض معه من قرارات سابقة.

رابعاً: يُبلغ هذا القرار لمن يلزم لإنفاذه.

والله ولي التوفيق،

مدير الإدارة العامة للاتصالات وتقنية المعلومات

م. يحيى بن علي شراحيلي

الإدارة العامة للإتصالات وتقنية المعلومات
General Administration for
Communicatiom and Information Technology

هاتف : ٩٦٦١٧٦٢٣٨٣٣+
ص ب : ٥١١ الرمز البريدي : ٦١٩٢٢
بريد الالكتروني : IT@ub.edu.sa

قرار تكليف مدير وحدة إدارة وحوكمة البيانات:

Kingdom of Saudi Arabia
Ministry of Education
University of Bisha

جامعة بيشة
UNIVERSITY OF BISHA

المملكة العربية السعودية
وزارة التعليم
جامعة بيشة

قرار إداري

إن مدير الإدارة العامة للاتصالات وتقنية المعلومات

- بناءً على الصلاحيات الممنوحة له.
- وبناءً على توصية اللجنة الدائمة للتحول الرقمي بجلستها الرابعة يوم الخميس الموافق 1444/1/6هـ الموافق 2022/8/4م.
- وبناءً على قرار سعادة رئيس الجامعة بتكليف م. يحيى بن علي محمد شراحيلي مديراً للإدارة العامة للاتصالات وتقنية المعلومات رقم 58/4/105 وتاريخ 1442/03/16هـ
- وبناءً على ما تقتضيه مصلحة العمل.

قرر ما يلي:

أولاً: تكليف م. منيرة بنت فايز السلولي، رئيساً لوحدة إدارة وحوكمة البيانات، والتابعة لقسم البنية المؤسسية بإدارة البنية التحتية والعمليات والمناطة بتطبيق سياسات حوكمة البيانات الوطنية والمتضمنة المهام التالية:

- نشر ثقافة مشاركة البيانات والتعاون لتعزيز وتطوير البيانات والمعلومات والأصول المعرفية.
- متابعة وتنظيم عملية نشر وتبادل واستخدام/ إعادة استخدام البيانات المحمية والمعلومات العامة.
- التنسيق لتحقيق التكامل بين الجهات الداخلية بالجامعة.
- ضمان جودة تمكين إعداد سياسات وتنفيذ الخطط، والقيام باستشراف المستقبل.
- تطبيق إجراءات المحافظة على خصوصية البيانات الشخصية، وسرية البيانات الحساسة.
- ضمان تفعيل إجراءات المحافظة على حقوق الأفراد عند التعامل مع البيانات الشخصية والمعلومات العامة.
- تحسين الأداء لرفع مستوى الثقة في الخدمات المعتمدة على البيانات بصورة مستمرة.
- تطوير الأداء لرفع مستوى الخدمات والتعاملات الإلكترونية بما يحقق التكاملية والاستدامة.
- ما يكلفه به صاحب الصلاحية لمصلحة العمل في إطار الضوابط واللوائح المنظمة.

ثانياً: يُعمل بهذا القرار اعتبارا من تاريخه ولمدة عام.

ثالثاً: يلغي هذا القرار جميع ما يتعارض معه من قرارات سابقة.

رابعاً: يُبلغ هذا القرار لمن يلزم لإنفاذه.

والله ولي التوفيق،

مدير الإدارة العامة للاتصالات وتقنية المعلومات

م. يحيى بن علي شراحيلي

الإدارة العامة للإتصالات وتقنية المعلومات

تم بحمد الله..

الإدارة العامة للإتصالات وتقنية المعلومات
General Administration for
Communicatiom and Information Technology