جامعة الحدود الشمالية
NORTHERN BORDER UNIVERSITY
عمادة تقنية المعلومات

دليل السياسات

والإجراءات لعمادة تقنية المعلومات

الإصدار الأول

1443هـ/ 2021 م

المحتويات


بسم الله الرحمن الرحيم

عمادة تقنية المعلومات

أنشئت عمادة تقنية المعلومات عام 1431 هـ بعد أن كانت إدارة تحت مسمى "مركز البيانات" .

الرؤية

أن تصبح جامعة الحدود الشمالية نموذجًا للجامعة الوطنية في اعتمادها على التقنية الحديثة في تنفيذ برامجها وتقديم خدماتها إلكترونيًا بطريقة تضمن الوصول إليها من أي مكان وفي أي وقت.

الرسالة

العمل بروح الفريق الواحد و التفاني في تقديم خدمات الكترونية متميزة وتوفير بنية تحتية الكترونية متكاملة للجامعة معتمدة في التركيز على تأهيل الموارد البشرية لديها.

المصطلحات المستخدمة

يكون للتعابير التالية الواردة ضمن هذه الوثيقة المعاني المبينة بجانبها ما لم يقتضِ السياق خلاف ذلك:

السياسات	هي حزمة القواعد والقوانين التي تُنظم علاقة المستخدمين والإدارة داخل المؤسسة.
الجامعة	جامعة الحدود الشمالية في عرعر وفروعها في شطري الطلاب والطالبات.
العمادة	عمادة تقنية المعلومات في الجامعة.
الأجهزة المدعومة	الأجهزة الإلكترونية والتي تشمل الخوادم والأجهزة المكتبية الثابتة والمنقولة، السلكية واللاسلكية والأجهزة الطرفية مثل الشاشات والطابعات وآلات التصوير وأجهزة العرض والموجهات مثل الراوترات والسويتشات والسبورات الذكية وغيرها المملوكة للجامعة.
البرامج المدعومة	أنظمة التشغيل، والأنظمة التجارية المرخصة قانونيًا، والبرمجيات التي تطورها الجامعة.
المستخدمون	منسوبو الجامعة من أعضاء هيئة التدريس والموظفين والطلاب والزائرين وكذا موظفي الشركات التي تتعامل مع الجامعة ممن له صلاحية الدخول على شبكة الجامعة أو أجهزتها أو أجهزة قاعات التدريس وأجهزة المعامل.
البوابة	بوابة الدخول على الموقع الإلكتروني للجامعة.
أصول المعلومات	مخزون المعلومات وقواعد البيانات المتوفرة على الأجهزة المدعومة بالجامعة.
المصادر التقنية	الأجهزة والبرمجيات والمعدات والأدوات وخطوط الاتصال والانترنت والخدمات الإلكترونية بكافة أشكالها.

الهدف من الدليل

تمثل هذه الوثيقة علاقة تعاقد بين الجامعة ومنسوبيها وزوارها، تهدف إلى خلق بيئة عمل آمنة لاستخدام موارد تقنية المعلومات والاستفادة القصوى من مصادرها، والحد من وقوع جرائم المعلوماتية. تحتوي الوثيقة على سياسات تمثل الإطار التنظيمي للتعاملات الإلكترونية وعدد من الإجراءات التي تمثل قواعد السلوك المعتمدة بالجامعة وفقاً لشروط ونماذج مخصصة لكل خدمة. إن هذه السياسات تمثل الإطار التنظيمي للاستعمال الآمن لوسائل تقنية المعلومات في جامعة الحدود الشمالية وقد روعي فيها الاستخدام المقنن للموارد بما يحقق مصلحة الجامعة ومنسوبيها، ولذلك فمن الضروري أن يكون منسوبو الجامعة على اطلاع وفهم لهذه السياسات في مجملها والتقيد بما ورد فيها. وعمادة تقنية المعلومات إذ تضع هذه السياسات والإجراءات، فإنها تتوقع من الجميع الالتزام بها، كما تؤكد أن أي مخالفة لها أو انحراف عنها يعد انتهاكاً قد يؤدي إلى اتخاذ إجراءات عقابية بحق مخالفيها.

نطاق الدليل

تنطبق هذه السياسات على جميع مصادر التقنية وأصول المعلومات وكافة التجهيزات الحاسوبية وعلى كافة المستخدمين لتلك الأصول والتجهيزات من منسوبي الجامعة أو المتعاقد معهم بشكل دائم أو مؤقت للقيام بمهام لصالح الجامعة، ويجب عليهم جميعًا الالتزام بما جاء في هذه الوثيقة عند استخدام أو التعامل مع أصول المعلومات الخاصة بالجامعة .

السياسات العامة

- **الاستخدام المقبول:**

يقتصر الاستخدام المقبول لمصادر التقنية وأصول المعلومات على الأنشطة المتعلقة بشكل مباشر بأعمال الجامعة الرسمية وأغراض البحث والتعليم.

- **الاستخدام غير المناسب:**

يعد استخدام مصادر التقنية التي توفرها الجامعة لأية أغراض تخالف الأنظمة والقوانين والأعراف المجتمعية والقيم الإسلامية استخدامًا غير مناسب، ويشمل ذلك ولا يقتصر على إعداد أو تحميل أو تنزيل أو نشر محتويات تتضمن عنفًا أو تهديداً أو تضليلًا أو فكراً متطرفًا، أو غير ذلك من المواد المجرمة معلوماتياً، ويدخل في ذلك أيضًا اتخاذ أي خطوات من شأنها أن تنتهك حقوق الملكية الفكرية لأي طرف، كما يدخل في الاستخدام غير المناسب توظيف موارد الجامعة التقنية لأية أغراض لا تتعلق بأنشطة الجامعة، بما في ذلك الأغراض التجارية أو لتحقيق مكاسب شخصية. وفي كل الأحوال يجب على المستخدمين عدم محاولة تخطي الإجراءات الأمنية لأنظمة الجامعة التقنية أو التحايل عليها.

- **مستوى الأمان:**

يتعين على المستخدمين الإبلاغ عن حوادث أمن المعلومات أو تلك المشتبه بها، كما يجب عليهم الإبلاغ عن أية انتهاكات لبنود هذه السياسات ضمن الطرق المبينة في هذه الوثيقة.

- **الامتثال من جانب المستخدم:**

جميع المواد والبنود والشروط المنصوص عليها في هذه الوثيقة تمثل اتفاقًا بين جميع الأطراف، ويجب أن تصنف وتفسر طبقًا للسياسات والإجراءات المذكورة أعلاه. ويترتب على عدم التزام المستخدمين ببنود هذه الوثيقة اخضاعهم للمساءلة القانونية و/أو اتخاذ إجراءات تأديبية متوافقة مع درجة المخالفة ووفقا للقوانين والأنظمة المرعية أو أية إجراءات نظامية أخرى تعتبرها جامعة الحدود الشمالية مناسبة.

- **إدارة الاصول:**

يجب تحديد مالك محدد لكل أصـل من أصـول التقنية، ويقع على عاتق مالكي الأصـول حمايتها وجردها وتزويد إدارة الاصول بالعمادة ببيانات تلك الأصول بشكل دوري، وتخضع لجميع السياسات الواردة بالدليل.

- **التعهد:**

أنا أفهم وأتعهد بالالتزام بسياسة استخدام الحاسب والإنترنت. كما أفهم أن أي مخالفة لهذه السياسة يعد تصرفًا لا مسؤولاً وقد يعد جريمة. وفي حال ارتكبت أية مخالفة، فإن جميع الخدمات الممنوحة لي قد يتم إلغاؤها، وقد يتخذ ضدي إجراءات نظامية مناسبة تحددها الجامعة.

المادة (1) السياسات والإجراءات الخاصة بالصيانة والدعم

الصيانة الدورية

- تتم عمليات صيانة الأعطال التي تسبب انقطاعا كاملاً أو جزئياً في الخدمة في عطلة نهاية الأسبوع أو بعد ساعات الدوام الرسمي.
- إشعار جميع المستخدمين ذوي العلاقة أن النظام لن يعمل بسبب عملية الصيانة على أن يكون ذلك قبل الصيانة بما لا يقل عن 48 ساعة، إلا في الحالات الطارئة التي تتم فيها الصيانة بشكل عاجل وغير مبرمج.
- الإشعار السابق يكون عبر البريد الإلكتروني الجامعي أو رسائل الجوال أو كليهما.

الدعم

- الدعم التقني للمستخدمين هو خدمة مقدمة من قبل عمادة تقنية المعلومات.
- تقدم طلبات الصيانة والدعم من خلال المنافذ التي تحددها عمادة تقنية المعلومات، سواء كانت من خلال طلبات ورقية أو إلكترونية أو برامج أو منصات إلكترونية خاصة أو من خلال بوابة الجامعة.

- تتوفر خدمة الدعم التقني للمستخدمين خلال أيام وساعات العمل الرسمي.
- تتم الاستجابة لطلبات الدعم حسب الأولوية، ويراعى عند ترتيب الأولوية درجة خطورة الطلب والموقع الوظيفي لمقدم الطلب، مع احتفاظ العمادة بالحق في تحديد الأولويات وترتيب الاستجابة.
- تصنف طلبات الصيانة الواردة حسب الأولوية الى أربعة أنواع هي:
  - **حرجة:** وتعني أن الوضع حرج لمقدم الطلب، كأن يكون هناك توقف للعمل ولا يوجد حل متاح، فتتم الاستجابة مباشرة.
  - **عالية:** الميزات الهامة غير متوفرة، لكن العمل يمكن أن يستمر على نحو معين والحل متاح، فتتم الاستجابة خلال مدة لا تتجاوز يوم عمل واحد.
  - **متوسطة:** وهذا يعني أن المنتج لا يعمل بالشكل الذي صمم من أجله مما أدى إلى فقد طفيف في الخدمة، فتتم الاستجابة في مدة لا تتجاوز 3 أيام عمل.
  - **منخفض:** وهذا يعني أنه لا يوجد أي فقد في الخدمة وقد يكون الطلب بغرض الحصول على بعض الملفات أو المعلومات أو تحسين المنتج، فتتم الاستجابة في مدة لا تتجاوز السبعة أيام عمل.
- تحدد عمادة تقنية المعلومات آلية تقديم الدعم الفني المناسب حسب ما تقتضيه طبيعة المشكلة، إما من خلال مشاغل العمادة أو من خلال المشاغل المتنقلة أو عن بُعد من خلال الإنترنت او الهاتف.

المادة (2) كلمة المرور

تعد كلمات المرور من أهم خطوط الحماية لحسابات المستخدمين على الأنظمة والخدمات التقنية المستخدمة في بيئة العمل الجامعي. وقد ينتج عن استخدام كلمات المرور الضعيفة او التي لا تتماشى مع معايير الأمان اختراقات أمنية على أصول المعلومات الخاصة بالجامعة؛ ولذلك كان لزاماً على كافة مستخدمي الحسابات المخصصة للوصول الى تلك الأصول الالتزام بمعايير كلمات المرور كما تقع عليهم مسؤولية اتخاذ الإجراءات والاحتياطات اللازمة لحماية كلمات المرور الخاصة بحساباتهم أو بالحسابات المسند إدارتها إليهم.

سياسة إدارة كلمات المرور للمستخدم

تعتبر المعايير التالية هي الحد الأدنى المقبول لاي من كلمات المرور الخاصة بحسابات المستخدمين على أي من مصادر التقنية أو أصول المعلومات في الجامعة:

- أن لا يقل طول كلمة المرور عن 10 خانات للمستخدم و 15 خانة لمديري الأنظمة.
- أن تحتوي على مزيج من الحروف الكبيرة والصغيرة والأرقام والرموز الخاصة.

مثال لكلمة مرور: r$cYv4m@3j8

- يتم تغيير كلمة المرور كل 45 يوم لمديري أنظمة التشغيل.
- شفرة (كود) التحقق الثنائي المرسل إلى هاتف المستخدم مكون من 6 خانات.
- الوقت المسموح به لإدخال كود التحقق الثنائي قبل انتهاء صلاحيته هو 120 ثانية.
- يتم تجميد الحساب بعد خمسة محاولات دخول فاشلة.

السياسات التنفيذية والإجراءات لتعيين كلمة المرور

- يقوم مدير النظام بتفعيل خيار تعيين كلمة مرور عند إنشاء حساب جديد.
- يقوم مدير النظام بتفعيل خيار تغيير كلمة المرور عند الدخول، وذلك عند استجابته لطلبات فقدان كلمة المرور الواردة من المستخدمين.
- يجب ألا تكون كلمة المرور فارغة، ولا تكون مشابهة لاسم المستخدم، ولا تكون معتمدة على معلومات شخصية مسجلة في النظام، مثل اسم المستخدم، هويته، أو مسماة الوظيفي.
- أن لا تكون من آخر 10 كلمات مرور تم استخدامها مسبقا.
- يحظر على المستخدمين إفشاء كلمة المرور لأي شخص كان بما في ذلك موظفي عمادة تقنية المعلومات، ولدى موظفي قسم أنظمة التشغيل في العمادة إمكانية توفير الدعم للمستخدمين دون الحاجة للكشف عن كلمات المرور الخاصة بهم.
- يحظر على المستخدمين كتابة كلمة المرور الخاصة بهم أو الاحتفاظ بها بطريقة غير آمنة وفي الحالات التي يضطر فيها المستخدم لتدوين كلمة المرور الخاصة به؛ فعليه الاحتفاظ بها في موقع آمن، كما يجب اتلافها بشكل آمن عندما تنتفي الحاجة لذلك.
- تجنب استخدام نفس كلمة المرور لحسابات مختلفة.

الإجراءات المتبعة في حال الاستخدام غير المشروع لكلمة المرور

- في حال الاستخدام الغير مشروع لكلمة المرور مثل كتابة كلمة المرور بشكل خاطئ عدة مرات أو محاولة تخمينها لحساب معين يتم تجميد الحساب كلياً ولن يتم إعادة تفعيل الحساب إلا عن طريق مسؤول المجال.
- عدد المحاولات المسموح به استخدام كلمة مرور خاطئة قبل تجميد الحساب بشكل تلقائي هو 5 مرات.
- يتم إعادة ضبط عدد مرات السماح بإدخال كلمة المرور بشكل خاطئ بعد

60 دقيقة من إدخال أول كلمة مرور خاطئة.

- في حال تجميد الحساب رغم عدم إدخال كلمة مرور خاطئة من قبل صاحب الحساب يجب عليه إشعار موظفي تقنية المعلومات بأسرع وقت.

المادة (3) البريد الإلكتروني

هذه السياسة هي وصف الاستخدامات المسموح بها للبريد الإلكتروني للجامعة. ولا يقصد بها أن تحل محل سياسات الجامعة الأخرى، بل ينبغي أن تقرأ بالاقتران معها. وتتضمن سياسة تقنية المعلومات تفاصيل ذات صلة باستخدام البريد الإلكتروني.

ويساعد الامتثال لهذه السياسة الجامعة على تحقيق هدفين:

- تحسين بيئة الاتصال بين منسوبي الجامعة .
- الحد من تعريض بيانات الجامعة المرسلة عبر البريد الإلكتروني لأي مخاطر.

تطبق هذه السياسة على كافة المستخدمين لأنظمة الجامعة الإلكترونية والزائرين ومن هم في حكمهم من موظفي الشركات الذين يقدمون خدمات للجامعة.

مستخدمو حسابات البريد الإلكتروني

تهدف خدمات البريد الإلكتروني الجامعي إلى تمكين أعضاء هيئة التدريس والموظفين من تسيير أعمال الجامعة بشكل سلس. ويسمح بالاستخدام الشخصي للبريد الإلكتروني شريطة ألا يؤثر ذلك على جودة الأداء أو يقلل من كفاءة شبكات الجامعة، وألا يتعارض مع السياسات الواردة في هذا الدليل أو سياسات الجامعة الأخرى .

توفر الجامعة حاليًا كذلك خدمة البريد الإلكتروني لجميع طلبة الجامعة ويخضع استخدامهم لتلك الخدمة للائحة سلوك الطلاب كما يخضع لسياسة العمادة لتقنية المعلومات، على وجه الخصوص سياسة الاستخدام المقبول.

لا يجوز تحويل (Forward) أي بريد إلكتروني للجامعة أو محتواه إلا للغايات المصرح بها للعمل الرسمي وبعد اتخاذ الاحتياطات الأمنية المناسبة الموضحة في بند السرية والأمان التالي.

السرية والأمان

يجب أن تخضع جميع رسائل البريد الإلكتروني التي تحتوي على معلومات محمية ومصنفة ذات حساسية عالية إلى الاحتياطات الأمنية المناسبة مثل التشفير والحماية بكلمات مرور قوية واستخدام الـ VPN حسب ما تقتضيه الحاجة. وعلى المستخدم ألا يسمح لأحد بالوصول إلى بريده الإلكتروني أو إعطاء كلمات المرور لآخرين.

على المستخدمين أن يدركوا بأن كلمة المرور المرتبطة بحساب البريد الإلكتروني قد تستخدم لتوثيق الهوية في الخدمات الإلكترونية الجامعية، ولذلك فإن المحافظة على سريه كلمة المرور وعدم إتاحتها للآخرين هو نوع من حماية الهوية والخصوصية الشخصية.

الاحتفاظ بمحتوى البريد الإلكتروني

ينبغي على المستخدم أن يتجنب الاحتفاظ بأعداد كبيرة من رسائل ومرفقات البريد الإلكتروني (سواء في صندوق الوارد، أو المرسلة، أو المحذوفة ، أو المجلدات الشخصية) لفترات طويلة من الزمن. إن صندوق البريد الإلكتروني ليس المكان المناسب للاحتفاظ بسجلات الجامعة وينصح دائمًا بإزالة السجلات الموجودة في البريد الإلكتروني أو نقلها إلى وسائط تخزين إلكترونية أخرى .

سياسة البريد الإلكتروني

البريد الإلكتروني الجامعي هو أحد قنوات الاتصال الرسمية المعتمدة في الجامعة ويحمل الحُجّيَّة القانونية، ولذلك:

- يتم رفع طلب الحصول على بريد إلكتروني جامعي من خلال نظام الدعم الفني وبموافقة صاحب الصلاحية.
- يتم إنشاء البريد الإلكتروني الجامعي للمستخدم وفق الآتي: الاسم الأول متبوعاً بنقطة، يليه الاسم الأخير مضافاً له امتداد نطاق الجامعة: **@nbu.edu.sa**
- يجب على منسوبي الجامعة استخدام خدمة البريد الإلكتروني الجامعي في التعاملات الرسمية، وعدم استخدام خدمات البريد الإلكتروني المجاني مثل **Yahoo، Gmail، Hotmail**. ...إلخ.
- لا يُسمح للمستخدمين باستخدام البريد الإلكتروني لأغراض غير لائقة أو غير قانونية، ولا يُسمح إطلاقًا بإرسال رسائل قد تسبب ضرراً للجامعة أو تؤدي إلى تشويه صورتها أو الإساءة إلى سمعتها.
- يحظر مشاركة كلمات المرور.
- يحظر على المستخدمين نشر أو إعادة إرسال رسائل البريد الإلكتروني لأغراض شخصية أو تجارية أو دينية أو سياسية أو غيرها من المحظورات.
- يحظر على المستخدمين المشاركة في نشر رسائل البريد الإلكتروني لأغراض جمع التبرعات والأنشطة الخيرية.
- يجب تذييل جميع رسائل البريد الإلكتروني الصادر من الجامعة بنص إخلاء المسؤولية التالي: " المعلومات في هذا البريد وجميع الملفات المرفقة به تخص المرسل إليه. وقد تحتوي على بيانات ذات خصوصية وسرية. والاطلاع على هذا البريد أو قراءته من الغير أمر غير مصرح به كما يمنع نسخها أو إرسالها. فإذا استلمت الرسالة عن طريق الخطأ الرجاء الاتصال بـ **it@nbu.edu.sa**"
- على المستخدم الحذر عند إعادة توجيه أي بريد إلكتروني، وعدم توجيه البريد الإلكتروني غير المرغوب فيه والإعلانات التجارية والبريد العشوائي.
- لا يُسمح للمستخدمين بإرسال أو الرد أو توجيه رسائل البريد الإلكتروني ذو المحتوى السري أو التي تنتهك حقوق الملكية الفكرية.

- يحظر على المستخدمين إرسال أو الرد أو توجيه رسائل البريد الإلكتروني التي قد تحتوي على مرفقات مصابة بالفيروسات أو أي برمجيات ضارة.
- على المستخدمين الحذر وعدم فتح رسائل البريد الإلكتروني غير المرغوب فيها والتأكد من حذفها من النظام.
- يحظر على المستخدمين استخدام نظام البريد الإلكتروني للجامعة لانتحال صفة شخص آخر.
- يحظر على المستخدمين استخدام نظام البريد الإلكتروني الخاص بشخص أخر.
- على المستخدمين عدم تسجيل أو مشاركة عنوان البريد الإلكتروني الخاص بالجامعة في المواقع الإلكترونية لغير أغراض العمل.
- على المستخدمين عدم استخدام خاصية إعادة التوجيه التلقائي إلى أو من عناوين البريد الإلكتروني الخارجي.
- عند استخدام البريد الإلكتروني في الهاتف النقال مثل الهواتف الذكية، يراعى تزويده بميزة قفل الأمان التلقائي وكلمة المرور في حالة عدم استخدام الهاتف.
- يجب أن تتوافق كافة أنواع التواصل التي يرسلها أعضاء الجامعة من خلال نظام البريد الإلكتروني مع جميع سياسات الجامعة، ولا يجوز الإفصاح عن أية معلومات سرية تعود ملكيتها للجامعة.

سياسة حذف الحسابات وصناديق البريد الإلكتروني

عند تلقي إشـــعار المغادرة النهائية لأي من المســـتخدمين في الجامعة، تقوم عمادة تقنية المعلومات باتخاذ بعض الإجراءات النظامية حسب التصنيف التالي:

المتعاقدون مع الجامعة عن طريق الشركات:

- يتم إبطال كافة التطبيقات والخدمات وفقًا للتاريخ المحدد من قبل إدارة الموارد البشرية في الجامعة.
- يُحذف حساب المجال وصندوق البريد الإلكتروني الخاص بالمستخدم المنتهي عقده.

أعضاء هيئة التدريس والموظفين:

- يتم إبطال كافة التطبيقات والخدمات في المجال وفقًا للتاريخ المحدد من قبل إدارة الموارد البشرية في الجامعة.
- يحتفظ عضو هيئة التدريس أو الموظف الذي انتهت خدماته أو المحال على التقاعد بالبريد الإلكتروني ولا يتم إبطاله. ويمكنه الاستمرار باستخدام نظام البريد الإلكتروني الخاص به في الجامعة.

الخريجون:

- يتم إبطال كافة التطبيقات والخدمات في المجال وفقًا للتاريخ المحدد من قبل وحدة الخريجين في الجامعة.
- يحتفظ الخريج بالبريد الإلكتروني ولا يتم إبطاله، ويمكنه الاستمرار باستخدام نظام البريد الإلكتروني الخاص به في الجامعة.
- يحتفظ الخريج بحق الدخول الى بياناته / بياناتها الأكاديمية، بصلاحيات محددة من عمادة القبول والتسجيل.

المادة (4) سياسة استخدام الهاتف الشبكي

التواصل عبر خدمة الهاتف الشبكي من خلال جامعة الحدود الشمالية يعد ميزة، ولذا يجب على المستخدمين الحاصلين على هذا الامتياز الالتزام على نحو صارم بالإرشادات التي تتعلق بالاستخدام المناسب للمكالمات. ويتعرض المستخدمون الذين يخالفون الأحكام المنصوص عليها في هذه الوثيقة لإجراءات نظامية. قد تشمل فقدان الخدمة. وبالإضافة لذلك فإن أي استخدام غير ملائم قد يعتبر جريمة تؤدي إلى تطبيق الإجراءات ذات الصلة المعمول بها في المملكة العربية السعودية على مرتكبيها.

خدمة الاتصال الخارجي وتحويل المكالمات إلى الجوال

تقتصر هذه الخدمة على موافقة صاحب الصلاحية معالي رئيس الجامعة.

الاستقالة أو النقل الخارجي

- على الموظف الذي قبلت استقالته أو نقله الخارجي المبادرة بتسليم جهاز الهاتف الشبكي للموظف الجديد وإبلاغ العمادة ببيانات الموظف الذي سيستلمه أو إعادة الجهاز لعمادة تقنية المعلومات.
- تقوم إدارة البث المرئي والهاتف الشبكي في عمادة تقنية المعلومات بتحديث دليل الهاتف الشبكي مرة واحدة كل ستة شهور

طلبات الدعم الفني

- تكون كافة طلبات الدعم الفني من خلال النظام الإلكتروني (ادعمني)، ولا ينظر لأي طلبات تتم من خلال وسائل أخرى.
- في حالات الضرورة - مثل أن يكون النظام الإلكتروني لا يعمل- يتم تقديم الطلب بالبريد الإلكتروني الجامعي، ويوجه مباشرة إلى المشرف على الإدارة.
- إن الاستجابة لأي طلب بأي طريقة خلاف ما ذكر أعلاه تعد مخالفة توجب المُسائَلة القانونية لكافة الأطراف.
- يتم الرجوع الى السياسات والإجراءات الخاصة بالدعم والصيانة لتحديد أولوية الرد على طلبات الدعم .

المادة (5): إنشاء أنظمة تقنية المعلومات من قبل العمادة

- تقوم الجهة المستفيدة في الجامعة بتقديم طلب على نظام معاملتي وفق النموذج المعد لذلك، ومن ثم تقوم العمادة بدراسة الطلب وتحليله والرد على الجهة بالموافقة من عدمها مع ذكر المبررات إن وجدت في مدة لا تتجاوز الأسبوعين من تاريخ استلامه.
- عمادة تقنية المعلومات هي الجهة المخولة بتحديد المصادر والتجهيزات التي تدعم النظام المطلوب إنشاؤه (كأن يكون برمجة محلية أو شراء من المصدر أو استئجار أو أية طريقة أخرى تراها العمادة مناسبة).
- ستقوم عمادة تقنية المعلومات بإدراج طلب النظام على قائمة انتظار بموجب نظام معد خصيصاً يراعي الأولويات في التنفيذ.
- يجوز إشراك الجهة الطالبة بالاطلاع على مراحل تصميم وتنفيذ وفحص واستلام النظام المعلوماتي المطلوب، بحيث يتم تلافي الأخطاء المحتملة بشكل مبكر وقبل الانتهاء من إعداده بشكل نهائي.
- بعد اكتمال النظام واختباره، يتم تسليمه إلى الجهة الطالبة بشكل رسمي، وذلك بعد إجراء تدريب مناسب تُقَدره عمادة تقنية المعلومات لأفراد من الجهة المستفيدة.
- يمكن تزويد الجهة المستفيدة بنسخة من (دليل المستخدم) باللغتين العربية والإنجليزية (إن وجدتا)، وتعود حقوق تصميم وتنفيذ وملكية النظام إلى عمادة تقنية المعلومات.
- يتم إدراج أيقونة أو رمز يسمى (حول النظام) يحتوي أسماء فريق العمل من مبرمجين مصممين وكل من شارك في إعداد النظام من الرؤساء المباشرين وذلك حفظاً للحقوق.

- بعد تسليم النظام للجهة المستفيدة، تعطى هذه الجهة فترة تجريبية لا تزيد عن الشهر للتكيف مع النظام الجديد وإجراء التعديلات اللازمة – إن وجدت – شرط أن لا تؤثر على جوهر النظام الأصلي.
- بعد انتهاء الفترة التجريبية، لا يسمح بإجراء أية تعديلات على النظام مهما كانت ويستثنى من ذلك التعديلات الأمنية أو الوظيفية التي قد تؤثر على عمل النظام.
- يتم تجميع طلبات التعديلات، إلى حين إصدار نسخة جديدة مُحدَّثة من النظام – إذا توفرت الأسباب الكافية – بعد مرور سنة على إطلاق النسخة السابقة.

المادة (6): مركز البيانات

سياسات العتاد التابع لمركز البيانات

تطبق السياسات التالية على جميع الأجهزة والمعدات والأدوات والمصادر الموجودة في مركز البيانات.

- تقدم طلبات التركيب أو التغيير أو الصيانة لأي من مصادر التقنية قبل وقت كافٍ لا يقل عن 12 ساعة قبل الموعد المطلوب لتنفيذ الخدمة.
- يقوم الموظف المختص أو مزودو الأجهزة والخدمات بتعبئة نموذج دخول وخروج المعدات لجميع الخدمات تركيباً أو تغييراً أو صيانةً، ولا يُسمح لهم بالدخول دون إكمال النموذج.
- يقوم الموظف المختص أو مزودو الاجهزة والخدمات بفحص وتجهيز المعدات في غرفة خاصة قبل تركيبها، أو تغييرها، أو صيانتها.
- على مدير مركز البيانات ضمان تسجيل جميع المعدات في نظام جرد مركز البيانات، وهو المسؤول عن توفير بيانات تفصيلية عن جميع المعدات الموجودة، وتحديث النظام بشكل مستمر.

تشمل البيانات التفصيلية للمعدات -ولا تقتصر- على ما يلي:

- **أجهزة النظام:**

وصـفاً كاملاً لمكونات الجهاز، بما في ذلك المورد، الإصـدار، رقم الإصـدار، الرقم التسلسلي، وسائط التخزين الفرعية، النوع وغير ذلك.

- **برامج النظام:**

وصـفاً كاملاً للبرامج الموجودة على الجهاز، بما في ذلك مورد نظام التشـغيل، الإصدار، انتهاء الرخصة وغيرها من مكونات البرامج الرئيسية على النظام.

- **وظيفة النظام:**

وصفاً كاملاً لوظيفة النظام.

- **استعادة النظام:**

الإجراءات الدقيقة لبدء التشـغيل والإغلاق والمعلومات الخاصـة المتعلقة بالوقوع المفاجئ للمعدات وحالات الطوارئ الأخرى.

- يقوم مدير مركز البيانات وموظفوه بإدخال بيانات الصـيانة الدورية للمعدات التشـغيلية للمركز، ويتم ذلك ورقياً على بطاقات الصيانة، وإلكترونياً على نظام الصيانة.
- يزود مركز البيانات عمادة تقنية المعلومات بتقرير شـهري عن الإنجاز والتحديات، وتقرير شامل كل ستة شهور.
- يزود مركز البيانات عمادة تقنية المعلومات بصـلاحيات الدخول على جميع أنظمة المراقبة لمركز البيانات.
- على مدير مركز البيانات التأكد من عمل نظام المراقبة بشـكل مسـتمر (أربعاً وعشـرون سـاعة ولمدة سـبع أيام في الأسـبوع)، والتأكد من تفعيل خاصـية الإنذار في حالة أي خطر كامن على عمل المركز.
- يمتثل المركز لمعايير السـلامة الكاملة المنصـوص عليها في قوانين المملكة العربية السـعودية ذات الصلة، ووفقا للمعاير الدولية.
- ينبغي التأكد من جاهزية مصـادر تزويد الطاقة البديلة والطارئة مثل وحدات تزويد الطاقة **UPS** ومولدات الكهرباء **Generators** وأية أنظمة طوارئ أخرى.

- تجري عمليات التأكد من جاهزية مصـادر الطاقة البديلة والطارئة بشـكل دوري وبموجب خطة طوارئ خاصة (أسبوعية وشهرية ونصف سنوية وسنوية) وتوثق في سجلات خاصة.

إجراءات الزوار

أي شخص ليس موظفًا في مركز البيانات، يعتبر زائراً ويُراعى ما يلي:

- ينبغي أن تتم جدولة الزيارات بالتنسـيق مع وكيل العمادة أو من ينيبه قبل وقتٍ كافٍ لا يقل عن 24 ساعة من الموعد للزيارة.
- لن يسمح لأي شخص بالدخول إلى مركز البيانات بدون نموذج تصريح الدخول.
- يقتصر دخول الزوار لمبنى مركز البيانات على المدخل الرئيسي .
- سـيطلب من الزائر أن يوثق حضـوره للمركز وعليه أن يكتب اسـمه ومسـماه الوظيفي والغرض من الزيارة ووقتها، ووقت الخروج.
- سيكون الزائر مصحوباً بأحد موظفي المركز في جميع الأوقات.
- ينبغي على الزائر ارتداء شارة زائر في جميع الأوقات.
- على الزائر تجنب لمس المعدات أو التجهيزات التي تنتمي إلى إدارات أخرى.
- يمنع التصوير بكافة أنواعه (الفيديو والرقمي والفوتوغرافي وغيره) داخل مركز البيانات.
- انتهاك أي من هذه الضـوابط السـابقة قد يؤدي إلى إبطال تصـريح الدخول إلى المركز، وايقاع العقوبة المناسبة بمن تهاون في ذلك أو سمح به.

المادة (7): البوابة الإلكترونية للجامعة

قيود الاستخدام

باستخدامك للبوابة الإلكترونية لجامعة الحدود الشمالية، تُقر بالامتناع عما يلي:

- استخدام البوابة لأغراض غير لائقة أو غير نظامية.
- التورط في – أو تسهيل – تبادل الملفات غير المصرح به لمحتويات يملكها طرف ثالث، ويشمل ذلك النشر والإتاحة والتحميل والتنزيل والتوزيع غير المصرح بأي شكل لمحتويات تابعة لطرف ثالث.
- استخدام البوابة بأية طريقة لأغراض تجارية أو تحقيق أرباح.
- تحميل ملفات على البوابة تحتوي على أي برمجيات خبيثة أو التي قد تُلحق ضرراً بالأجهزة او المعدات.
- نشر أو توزيع أو تعميم مواد أو معلومات تنطوي على تشويه سمعة لأي طرف، أو انتهاكاً للأنظمة ويدخل في ذلك أي محتوى غير مقبول دينياً أو اجتماعياً أو كان مخالفاً للآداب العامة.
- الانخراط في نقاشات لمواضيع وعناوين غير ملائمة أو فاضحة أو عدائية أو بذيئة أو غير قانونية.

- الاشـــتراك من خلال البوابة في أنشـــطة غير مشـــروعة أو تنتهك أي من الأنظمة المرعية في المملكة العربية السعودية.
- القيام بأي نشـــاط من شـــأنه اعتراض -أو محاولة اعتراض- التشـــغيل الصـــحيح للبوابة، ويدخل في ذلك القيام بأي إجراء يفرض حملاً غير مناســـب على البنية التحتية لبوابة الجامعة.
- الإساءة للآخرين أو ابتزازاهم أو الاستهزاء بهم بأي شكل من الأشكال.

مدير البوابة

- هو الشـــخص المعني بتطبيق الاقتراحات والتوصـــيات ســـواء كانت تنفيذية أو إجرائي أو تطويرية على موقع الجامعة على شبكة الإنترنت.
- يكون مسؤولاً مباشـراً عن متابعة التزام الشـركة/الشـركات المتعاقد معها لتشـغيل وصـيانة البوابة وتنفيذ جميع الشروط المنصوص عليها في كراسة العقد.
- اقتراح الحقائب التدريبية وإعدادها بشكل دوري على جميع المستويات.
- متابعة ما هو جديد من تطورات تقنية تخص البوابة وتقديم تقارير لإدارة العمادة.
- يحق لمدير البوابة تفويض صـــلاحياته لمن ينوب عنه بعد موافقة إدارة العمادة، ويكون التفويض خطياً وموثقاً.
- لمدير البوابة أو من ينوب عنه الحق بإيقاف أو إعاقة أي ارتباط من أي موقع يحتوي على مواد تخالف السياسة العامة لاستخدام البوابة.
- مدير البوابة هو المسؤول عن منح الصلاحيات الدخول عليها.

مديرو البوابة الفرعيون

- يُعينون من قبل وكلاء الجامعة، أو العمداء، أو مديري الإدارات بقرارات إدارية.
- يملأ النموذج الخاص بتقنية المعلومات بأسماء المديرين الفرعيين ويصادق عليه من مسؤول الجهة المباشر، ويمنح الصلاحيات بناءً على هذا.
- على كل إدارة تسمية اثنين من المدراء الفرعيين على الأقل.
- تقتصر صلاحيات المدير الفرعي على إضافة/حذف/تعديل المحتوى الخاص بإداراته باللغة الرسمية المعتمدة (العربية والإنجليزية) وكذلك إنشاء الصفحات وإضافة الأخبار.
- لا يحق للمديرين الفرعيين التغيير في تصميم الصفحات، ويتحملون المسؤولية في حال حصول ذلك.
- يتلزم المديرون الفرعيون بحضور كافة الدورات التدريبية المقدمة من العمادة.
- في حال انتقال او استقالة أي مدير فرعي تبلغ العمادة بشكل فوري لإيقاف صلاحيته على البوابة.
- أمن اسم المستخدم وكلمة المرور لمدير فرعي هي ضمن مسئولياته.
- عند إضافة أي روابط على البوابة فيجب ألا تتعارض مع أهداف وسياسات البوابة أو تُعرضها للخطر.
- يمنع منعًا باتًا إنشاء أية روابط إلكترونية خاصة بالمديرين الفرعيين أو عرض أي منها في صفحات البوابة.
- يخضع المديرون الفرعيون للمساءلة النظامية في حال انتهاكهم لما نصت عليه الوثيقة وتُبطل صلاحياتهم.

المحتوى

- على المديرين الفرعيين مسؤولية التأكد من أن يكون المحتوى ذا قيمة تخدم الجامعة والمجتمع المحلي والدولي.
- يلتزم المديرون الفرعيون بعدم الإضافة أو الحذف او التعديل على المحتوى الثابت والبيانات الأساسية في البوابة (الرؤية، والرسالة، والأهداف، والهيكل التنظيمي، ومنسوبو اللجنة وسيرهم الذاتية وبيانات التواصل معهم، والإدارات التابعة ومهامها، وبيانات التواصل).
- تعتبر الأخبار محتوى متغير، تتحمل الإدارة مسؤولية إضافته وعليها مراعاة الدقة دائماً.
- تعتبر الخطط الدراسية، ووصف المقررات، والخطط المستقبلية والمشاريع المقترحة محتوى متغير أيضاً، تتحمل الإدارة مسؤولية إضافته.
- لا يجوز رفع محتوى على لبوابة الا بعد أن يتم تدقيقه لغوياً وترجمته – عند الحاجة – بشكل صحيح واعتماده من قبل المدير الفرعي للبوابة صاحبة المحتوى.
- كل من يخالف هذه السياسة يعرض نفسه للمساءلة النظامية.

الصيانة والتشغيل

- تقوم وحدة الأصـول بفحص التراخيص الخاصـة بأنظمة تشـغيل البوابة بشـكل دوري، وإخطار الجهة المسؤولة عن الترخيص قبل انتهاء التراخيص بتسعة أشهر.
- يقوم العميد أو المشـرف على العمادة بإخطار الجهات المسـؤولة (وكيل الكلية أو الإدارة المالية أو الجهة المستفيدة) داخل الجامعة بمتطلبات تجديد الترخيص قبل ستة أشهر من انتهاء الرخصة.
- على الإدارات المختلفة وكافة المسـتخدمين إبلاغ عمادة تقنية المعلومات عن المشـكلات التشـغيلية أو الوظيفية التي تواجههم عند اسـتخدام البوابة، أو الاختراقات والحوادث الأمنية السيبرانية التي تتعرض لها البوابة.
- على العمادة العمل على نقل المعرفة من الشـركات المشـغلة للبوابة إن وجدت إلى الجهات ذات العلاقة في الجامعة.
- يجب أخذ موافقة مجلس العمادة بالإجماع قبل إجراء تعديلات جوهرية على البوابة.
- على العمادة إعداد تقرير سـنوي عن جودة عمل البوابة، يتضـمن إحصـائيات تتعلق بالاستخدام والاستفادة من البوابة، عدد المواد الجديدة، مشاريع التطوير للبوابة، وكمية الأعطال ونسبة ما تم إصلاحه منها.. وغيره.

النشر على البوابة

- تخضع كافة المواد المنشورة على بوابة الجامعة للسياسة العامة للنشر في الجامعة.
- تخضـع المواد المنشـورة إلى تحديد عمر افتراضـي للمادة المنشـورة، بحيث تكون إما مادة دائمة الصلاحية أو محددة بوقت معين.
- تخضع المواد المنشورة إلى تحديد مكان النشر المناسب، فقد تكون على الصفحة الرئيسة أو في صفحات فرعية.

- تحدد الجهة طالبة النشـر الفئة المسـتهدفة من النشـر بحيث يتم توجيه المادة المنشـورة للفئات المستهدفة.

- النشر وإدارة المحتوى عبر موقع جامعة الحدود الشمالية أو الشاشات الإعلانية او خدمات الرسـائل النصـية يعد ميزة، ولذا يجب على المسـتخدمين الحاصـلين على هذه الميزة الالتزام وبشـكل صـارم بالإرشـادات التي تتعلق بالاسـتخدام المناسـب لموارد المعلومات. ويتعرض المسـتخدمون الذين يخالفون الأحكام المنصـوص عليها في هذه الوثيقة لإجراءات نظامية تشمل فقدان الخدمة. وبالإضافة لذلك فإن أي استخدام غير ملائم أو مخالف للسياسات العامة قد يُصنف جريمة معلوماتية تؤدي إلى تطبيق الإجراءات ذات الصلة المعمول بها في المملكة العربية السعودية على مرتكبيها.

المادة (8): سياسات إدارة المشاريع

- يلتزم مكتب إدارة المشاريع بإعداد دراسات جدوى (**Business Case**) للمشاريع قبل عرضها واعتمادها من إدارة العمادة بمشاركة الراعي الرسمي (**Business Sponsor**).
- يلزم اعتماد دراسة الجدوى من صاحب الصلاحية قبل البدء في المشروع، ثم تعيين مدير للمشروع ومنحه الصلاحيات اللازمة للبدء في إعداد وثيقة ميثاق المشروع (**Project Charter**) واعتمادها من صاحب الصلاحية.
- يتم تحديد ميزانية المشروع ومصادر التمويل (**Source Of Fund**) من بنود الميزانية بالتنسيق مع إدارتي المالية والمشتريات بالجامعة واعتماده من صاحب الصلاحية.
- بمجرد تحديد نطاق عمل مشروع، يتم إنشاء لجنة إشرافية وأخرى فنية له للبدء في عمليات التخطيط للمشروع، واعتماد الخطط التنفيذية من صاحب الصلاحية.
- تقوم اللجنة الإشرافية للمشروع باعتماد خطط الإدارة والاتصالات والمخاطر والجودة الخاصة بالمشروع.
- يلتزم مكتب إدارة المشاريع بالتنسيق الكامل مع مكتب/لجنة البنية المؤسسية (الجهة التي تقود عملية التحول الرقمي بالجامعة).
- يلتزم المكتب أيضاً بالاحترافية العالية في إدارة المشاريع باعتماد منهجية **PMI** لإدارة جميع مراحل المشروع من البداية حتى الإغلاق.
- يتم إعداد قائمة معايير تحقيق الجودة المطلوبة وفقًا لمتطلبات كفاءة المشاريع.
- الالتزام بتقديم تقارير دورية لسير المشروع تشمل (الجدول الزمني ونطاق العمل والميزانية والمخاطر).
- وثائق قبول الأعمال المعتمدة من اللجنة الفنية، ضرورة قبل الشروع في عمليات الإغلاق لاي مرحلة او مخرج من مخرجات المشروع.

- عمليات إغلاق المشاريع تتم بالتنسيق مع إدارة المشاريع وتقرها اللجنة الإشرافية لكل مشروع.
- تم وضع مصفوفة ومسارات ونقاط ومستويات التصعيد مع بداية التخطيط لكل مشروع للجوء إليها عند مواجهة مشكلات مع تحديد اتفاقية مستوى الخدمة وزمن الاستجابة قبل التصعيد.
- تشمل عمليات الإغلاق إعداد خطة انتقال المشروع إلى مرحلة التشغيل (**Operation mode**) وتسليمه للجهة الفنية مع إعداد خطة تدريب وتأهيل ونقل معرفة.
- في حال كان المشروع خارجياً:
  - فإن المقاول يقوم بتعيين مدير للمشروع والتنصيص عليه في وثيقة التأسيس. وتبقى لمكتب إدارة المشاريع الصلاحيات في تعميد أو رفض مدير المشروع إن كان لا يستجيب لمتطلبات المشروع.
  - يضع مكتب إدارة المشاريع على ذمة المقاول نماذج خاصة بكل عمليات إدارة المشاريع من البدء إلى الإغلاق كما يتم تحديد عدد الاجتماعات وتواريخها والتقارير الدورية التي يقوم المقاول بإرسالها لمكتب إدارة المشاريع ضمن خطط المشروع.

المادة (9): السرية

يُقصد بالألفاظ والعبارات الآتية المعاني المبينة أمامها:

المعلومات	أي بيانات شفوية أو مكتوبة أو سجلات أو إحصاءات أو وثائق مكتوبة أو مصورة أو مسجلة أو مخزنة إلكترونياً أو بأي طريقة أخرى وتقع تحت إدارة العمادة أو ولايتها.
وعاء المعلومات/ الوعاء	مكان تخزين المعلومات مثل: الانظمة الإلكترونية، قرص صلب /مدمج، نسخة ورقية، وسائل سمعية وبصرية وغيرها من الوسائط المعتمدة لغايات تبيان المعلومات.
تصنيف المعلومات	تحديد مستوى الحساسية المناسب للمعلومات التي يتم انشاؤها أو تغييرها أو نقلها او تعديلها أو حفظها على أية وسائل كانت وبأية تقنيات ممكنة، اعتماداً على المخاطر المترتبة عن الاطلاع والاستخدام غير المشروع لتلك المعلومات.
مالك المعلومة	الجهة المسؤولة عن استخدام/التفويض باستخدام المعلومات.
الطالب/ طالب المعلومات	الشخص الطبيعي أو الاعتباري من منسوبي الجامعة الذي يتقدم بطلب للحصول على المعلومات إذا كانت له مصلحة مشروعة أو سبب مشروع.
الجهات الخارجية	أي جهة تتعامل معها الجامعة بحكم طبيعة عملها.
البريد الرسمي	هو آلية تسليم المعاملات الورقية أو المغلفات بطريقة تضمن إيصاله إلى الشخص /الوحدة التنظيمية /الجهة المعنية.
السجل الخاص	السجل الذي يوثق استلام وتسليم البريد الرسمي.

البيانات الشخصية	أي معلومات يتم جمعها وتسجيلها بتنسيق يسمح بالتعرف على شخص ما وتحديد هويته بشكل مباشر أو غير مباشر بما في ذلك البيانات المتعلقة بالحالة الشخصية أو الجسدية أو الشكلية أو الذهنية أو الاقتصادية أو الدينية.

تصنيف المعلومات

بند (1):

تطبق هذه التعليمات على كافة الوحدات التنظيمية واللجان الدائمة والمؤقتة في الجامعة.

بند (2):

يتم تصنيف المعلومات منذ لحظة انشائها أو استلامها بغض النظر عن الوعاء الذي يحوي هذه المعلومات او بيئة العمل المستخدمة / المتداول فيها تلك المعلومات، ويتم تحديد مدة سريان التصنيف لهذه المعلومات وفقاً لتقدير مالكي المعلومات، وفقاً لمستويات التصنيف التالية مع مراعاة التشريعات النافذة في المملكة بهذا الخصوص:

- **المستوى الرابع – معلومات متاحة/ عادية**

هي معلومات لا يؤثر الإفصاح عنها على خصوصية أو أمن الجامعة أو أي من المتعاملين معه مثل الموظفين والعملاء والشركاء والجهات الخارجية، ولا تؤدي إلى إيذاء أي من المصالح السياسية أو الاقتصادية أو غيرها من مصالح الجامعة، وتكون عادة متاحة للنشر عبر وسائل الاتصال والإعلام، بالطرق الإلكترونية، أو الشفوية، أو المكتوبة.

- يتطلب هذا المستوى من التصنيف توفير الضوابط الأمنية التي تساعد على حماية البيانات من الضياع او التعديل غير المصرح به.
- من الأمثلة على المعلومات التي من المحتمل أن تقع ضمن هذا المستوى من التصنيف: المعلومات المنشورة ضمن المطبوعات وصفحات الإنترنت المتاحة للعموم.
- لا توجد صلاحيات أو تحديدات للاطلاع على هذا النوع من المعلومات.
- يجب ضمان جودة وصحة المعلومات الواقعة ضمن هذه الفئة واستمرار تحديثها ونشرها.

- **المستوى الثالث - معلومات غير متاحة / خاصة**

هي معلومات معدة للاستخدام الرسمي، والذي يؤدي الكشف أو الإفصاح غير المخول به إلى أي من التهديدات التالية:

- تعريض خصوصية وأمن الجامعة أو أي من المتعاملين معه للخطر.
- إيذاء محدود لمصالح الجامعة.
- يتطلب هذا المستوى من التصنيف توفير مستوى متوسط من الضوابط الأمنية التي تساعد على حماية البيانات من الضياع او التعديل أو الاطلاع غير المصرح به.
- من الأمثلة على المعلومات التي من المحتمل أن تقع ضمن هذا المستوى من التصنيف: البريد الإلكتروني غير المشّفر، والتعاميم والمذكرات الداخلية.

- **المستوى الثاني- معلومات غير متاحة/ حساسة**

هي معلومات معدّة للاستخدام الرسمي المحدود، والذي يؤدي الكشف أو الإفصاح غير المخول به إلى أحد أو بعض التهديدات التالية:

- تعريض أمن وخصوصية الجامعة والمتعاملين معه للخطر.
- أضرار مادية أو معنوية للجامعة أو المتعاملين معها.
- التأثير على سمعة الجامعة.
- أضرار على المصلحة العامة للدولة أو الوزارة أو الجامعة أو مصالح الأفراد

- يتطلب هذا المستوى من التصنيف توفير مستوى مرتفع من الضوابط الأمنية التي تساعد على حماية البيانات من الضياع او التعديل أو الاطلاع غير المصرح به.
- من الأمثلة على المعلومات التي من المحتمل أن تقع ضمن هذا المستوى من التصنيف: الحسابات المصرفية، بيانات الطلاب والموظفين، خطط العمل التنفيذية، وثائق العطاءات التي لم يتم طرحها بعد، والمعلومات المستثناة من الإفصاح عن المعلومات العامة والداخلية.
- يتم تصنيف البيانات الشخصية على أنها "حساسة " ما لم تحدد التعليمات النافذة في الجامعة غير ذلك.

- **المستوى الأول – معلومات غير متاحة / سرية**
- هي المعلومات التي تعتبر غاية في الأهمية للجامعة والتي يؤدي الكشف أو الإفصاح غير المخول به إلى أحد أو بعض التهديدات التالية:
- تعرض أمن الجامعة وخصوصيتها والمتعاملين معها للخطر الشديد.
- تهديد الأمن الوطني أو حياة الأشخاص أو الصحة العامة.
- أضرار مادية أو معنوية شديدة للجامعة أو المتعاملين معها.
- الإضرار بأصول الدولة أو الجامعة وممتلكاتها.
- تعريض أمن الدولة أو الجامعة للخطر.
- التأثير على سمعة الجامعة.
- يتطلب هذا المستوى من التصنيف توفير مستوى عالي من الضوابط الأمنية التي تساعد على حماية البيانات من الضياع او التعديل أو الاطلاع غير المصرح به.
- من الأمثلة على المعلومات التي من المحتمل أن تقع ضمن هذا المستوى من التصنيف: التحقيقات الجارية، ومعلومات تتعلق بأمن الدولة، والمعلومات ذات الطبيعة الخاصة التي تحددها الجامعة.

بند (3):

يكون المسؤول الأول في الوحدات التنظيمية مالكة المعلومات بموجب هذه التعليمات مخولاً (اطلاع فقط، الاطلاع والمشاركة، الاطلاع والتعديل، الاطلاع والتعديل والمشاركة) على المعلومات الواقعة ضمن المستويين الأول والثاني ومسؤولاً عن تحديد الأشخاص/الجهات المخولة بالاطلاع على هذه المعلومات.

بند (4):

يجب على الوحدات التنظيمية مالكة المعلومات أن تراعي ما أمكن عدم اطلاع أي من العاملين لصالح الجامعة على هذه المعلومات في حال كانت هذه المعلومات تتعلق بشخص/جهة تربطه به صلة قرابة من الدرجة الاولى أو في حال كان هناك احتمالية تعارض في المصالح نتيجة اطلاعه عليها، وفي حال اطلاعه عليها أو احتمالية اطلاعه يجب على العامل لصالح الجامعة الإفصاح عن ذلك خطياً.

بند (5):

تكون مسؤولية تصنيف المعلومات وصلاحية تعديل التصنيف، لمالكي المعلومات، ويتم ذلك بموجب "نموذج تصنيف/تعديل تصنيف المعلومات" المعتمد لهذه الغاية.

بند (6):

يتم تصنيف المعلومات التي تخص الجامعة بناءً على اختبار درجة الخطر أو المصلحة العامة، كما يجب على مالكي المعلومات اجراء مراجعة دورية لمستويات تصنيف البيانات التي تمتلكها وتعديلها عند اللزوم وفقا لتغير درجة الخطر أو المصلحة العامة سواء برفع درجة التصنيف أو تخفيضها، بموجب النموذج المعتمد لهذه الغاية.

بند (7):

على مالك البيانات إدراج وصف واضح للبيانات يتم تضمينه لقائمة المعلومات السرية أو الحساسة بهدف تحديد مستوى التصنيف المناسب وتعليل ذلك وفقا لمنهجية واضحة وشفافة.

بند (8):

أي وثائق مملوكة للجامعة، مثل تلك التي مرّ عليها فترات طويلة ولم يتم تصنيفها قبل تطبيق هذه التعليمات تصنف كمعلومات من المستوى الثالث - معلومات غير متاحة / خاصة، ما لم تقرر الجهة مالكة المعلومات تغيير مستوى التصنيف لها فور استخدامها أو ظهور الحاجة اليها.

بند (9):

تصنف المعلومات التي تخص جهات خارجية وتكون محفوظة لدى الجامعة ضمن المستوى الثاني – معلومات غير متاحة / حساسة ويتم اتباع إجراءات إدارة المعلومات الواردة في الفصل الرابع من هذه التعليمات و/أو التعليمات ذات العلاقة بالحفظ الأمين بغض النظر عن وعاء المعلومات المخزنة فيه.

بند(10):

يحق للمسؤول الأول في الوحدة التنظيمية أو من ينوب عنه طلب تعديل تصنيف معلوماته وطلب التعديل على قائمة المعلومات "السري أو الحساس" دون الإخلال بمضمون هذه التعليمات.

بند (11):

تتم عملية تصنيف/تعديل تصنيف المعلومات وفق الآلية التالية:

- يتم التقدم بطلب إلى عمادة تقنية المعلومات لتصنيف/تعديل تصنيف المعلومات موقعة اصولياً من المسؤول الأول في الوحدة التنظيمية مالكة المعلومات، مبيناً فيها الأسباب والمخاطر التي دعت إلى تصنيفها بهذا المستوى أو تعديل مستوى تصنيفها معززاً بنموذج "تصنيف/تعديل تصنيف المعلومات" المعد لهذه الغاية.
- يقوم القسم المعني في أمن المعلومات في العمادة بمراجعة تصنيف/تعديل تصنيف المعلومات وفقاً لمخاطر أمن المعلومات وتزويد الوحدة التنظيمية مالكة المعلومات بالتوصيات حول التصنيف لغايات اعتماد أو عدم اعتماد التصنيف الوارد.
- اعتماد نماذج تصنيف/تعديل تصنيف المعلومات من قبل مالك المعلومات ومن ثم اعتمادها من قبل وكيل الجامعة المشرف على مالك المعلومات.
- تقوم عمادة تقنية المعلومات بتجميع قائمة المعلومات السرية أو الحساسة من كافة الوحدات التنظيمية ومن ثم رفعها إلى معالي رئيس الجامعة لغرض الاعتماد.

بند (12):

عند استلام معلومات غير مصنفة من قبل الجهة المرسلة، وتبين للجهة المستلمة ضرورة تصنيفها كمعلومات حساسة/سرية، فيقع على عاتق الوحدة التنظيمية المستلمة لها التعامل معها وفقًا لمستوى التصنيف الملائم بغض النظر عن وعاء المعلومات الذي يحتويها، على أن يتم إبلاغ مالك المعلومات ليقوم بتصنيفها في حال كانت الجهة المرسلة داخلية.

إدارة المعلومات

بند(13):

على كافة الوحدات التنظيمية الالتزام بإجراءات التعامل مع المعلومات المصنفة اعتماداً على وعاء المعلومات ومستوى تصنيفها بما يضمن أمن وحماية هذه المعلومات وفقاً للإجراءات التالية:

- **المستوى الرابع - معلومات متاحة/ عادية ضمن وعاء إلكتروني:**
  - الحفظ: يتم بشكل غير مشفر.
  - التداول: يتم على شكل معلومات غير مشفرة.
  - الاتلاف: يتم بواسطة الحذف.

- **المستوى الثالث - معلومات غيرمتاحة / خاصة ضمن وعاء إلكتروني:**
  - الحفظ: يتم حفظها بطريقة تضمن خصوصيتها وعدم الوصول غير المصرح به من خلال تطبيق إجراءات التحكم بالوصول كقوائم السماح والمنع بالوصول.
  - التداول: يمكن تداولها على شكل معلومات غير مشفرة بطريقة تضمن خصوصيتها وعدم الوصول غير المصرح به.
  - الإتلاف: يتم من خلال حذف البيانات عن وسائط التخزين.

- **المستوى الثاني - معلومات غيرمتاحة / حساسة ضمن وعاء إلكتروني:**
  - الحفظ: يتم حفظ هذه المعلومات بشكل مُشَّفر مع التأكد من تأمين الحماية المادية من الوصول المادي غير المصرح به لوعاء المعلومات، وتكون الوحدة التنظيمية مالكة المعلومات مسؤولة عن تحديد آلية ومكان حفظ هذه المعلومات والتخويل باستخدامها والوصول إليها.
  - التداول: يتم تداولها بشكل مشفر.
  - الإتلاف: يتم إتلافها بالاستئصال في حال الحاجة لإعادة استخدام وعاء المعلومات كوسائط التخزين الإلكترونية داخل الجامعة، وفي حال عدم الحاجة لإعادة استخدام الوعاء يتم استخدام طرق التحطيم المادي مثل (التكسير/التقطيع/التهشيم/الطحن/العجن/الحرق) وتوثيق عملية الإتلاف أصولياً.

- **المستوى الأول - معلومات غير متاحة / سرية ضمن وعاء إلكتروني:**

  - الحفظ: يتم حفظ هذه المعلومات بشكل مشفر مع التأكد من تأمين الحماية المادية من الوصول المادي غير المصرح به لوعاء المعلومات، وتكون الوحدة التنظيمية مالكة المعلومات مسؤولة عن تحديد آلية ومكان حفظ هذه المعلومات والتخويل باستخدامها و/أو الوصول إليها.
  - التداول: يتم تداولها بشكل مشفر باليد وعدم استخدام الشبكة او التداول الإلكتروني ويستثنى منها معلومات الأنظمة المؤتمتة.
  - الإتلاف: يتم إتلافها بالاستئصال في حال الحاجة لإعادة استخدام وعاء المعلومات كوسائط التخزين الالكترونية داخل الجامعة، وفي حال عدم الحاجة لإعادة استخدام الوعاء يتم استخدام طرق التحطيم المادي مثل (التكسير/التقطيع/التهشيم/الطحن/العجن/الحرق)، ويتم توثيق عملية الاتلاف أصولياً.

التعامل مع طلبات الحصول على المعلومات

بند(14):

تتولى مختلف الوحدات التنظيمية استقبال/التعامل مع طلبات الحصول على المعلومات الواردة من الجهات التي يوجد للجامعة تعامل رسمي معها وفقاً للتشريعات النافذة والتعليمات التطبيقية لهذه الوحدات وذلك كلٍ وفق اختصاصه ووفق الآليات المعتمدة بهذا الخصوص.

على كافة الوحدات التنظيمية الراغبة بالاطلاع على معلومات مصنفة تقع ضمن أي من المستويين الأول أو الثاني (سرية أو حساسة) لازمة لإكمال اعمالها الرسمية، الحصول على موافقة خطية من وكيل الجامعة المسؤول عن الوحدة التنظيمية المالكة لهذه المعلومات، ما لم تنص التعليمات النافذة على جواز ذلك.

بند (15):

يتم استقبال طلبات الحصول على المعلومات الواردة من غير الجهات المذكورة في البند (14) باستخدام النموذج المعتمد لهذه الغاية من خلال الموقع الإلكتروني للجامعة على شبكة الإنترنت.

بند (16):

تكون عملية استقبال طلبات الحصول على المعلومات والرد عليها وفق النظام وحسب الإجراءات التالية:

1. يقوم طالب المعلومات بتعبئة النموذج الالكتروني المعتمد معززاً بنسخة إلكترونية عن وثائق إثبات الشخصية معززاً بالموافقات الرسمية.
2. يتم بشكل آلي تخصيص رقم لطلب الحصول على المعلومات الإلكتروني وتخزينه على قاعدة بيانات خاصة بالموضوع وخاضعة للحماية اللازمة بما يضمن عدم وجود صلاحية تعديل أو إلغاء للبيانات المخزنة على هذه القاعدة.
3. يتم إعلام صاحب الطلب بشكل آلي عن رقم الطلب الخاص به مباشرة فور الانتهاء من تقديمه للطلب.
4. تقوم الجهة المسؤولة في عمادة تقنية المعلومات بالاستعلام يومياً خلال أيام العمل الرسمي عن طلبات الحصول على المعلومات الواردة للجامعة من خلال الموقع وتحميل وتجميع نماذج الطلبات المتوفرة عليه.
5. تقوم عمادة تقنية المعلومات بإرسال نموذج طلب الحصول على المعلومات إلى الوحدة التنظيمية مالكة المعلومات خلال مدة أقصاها يومي عمل من تاريخ استلامها له مع التأكد من توقيع المعنيين في الوحدة التنظيمية بالاستلام.
6. تقوم الوحدة التنظيمية مالكة المعلومات بتدوين شروحاتها على النموذج حول مدى توفر المعلومات المطلوبة في الجامعة أو عدم توفرها خلال مدة لا تتجاوز أسبوعًا.
7. في حال توفر المعلومات تعمل الوحدة التنظيمية مالكة المعلومات على تحديد إمكانية تزويد الطالب بها استناداً إلى مستوى تصنيفها المعتمد، بالإضافة الى التعليمات التطبيقية لحفظ الوثائق في المستودعات الأمينة والعادية ولدى دوائر الجامعة وفروعه ومكاتبه وإتلافها سارية المفعول بالإضافة إلى اية طلبات سابقة بخصوص المعلومات المطلوبة، وإجراء التالي بناء على ذلك:
    - في حالة وجود الإمكانية لتزويد المعلومات يقوم مالك المعلومات بإعداد المطلوب ضمن وعاء معلومات معين وفق النموذج، وتسليمها إلى العمادة خلال مدة أسبوع من تاريخه.

- في حال كانت المعلومات المطلوبة مصنفة ضمن أي من المستويين الأول أو الثاني (سري أو حساس) يتم الرد بعدم الموافقة على تزويد طالب المعلومات بها مع ذكر الأسباب ضمن الخانة المخصصة لذلك في النموذج وإعادة نموذج طلب الحصول على المعلومات إلى العمادة خلال مدة أسبوع من تاريخه.
- في حال كانت المعلومات متلفة يتم تدوين ذلك على النموذج.
- في حال وجود مبررات تستدعي عدم الموافقة على تزويد طالب المعلومات بها غير ما ورد سابقاً (مستوى التصنيف، أو الإتلاف) يتم توضيح ذلك في النموذج.

8. تقوم العمادة خلال يومي عمل من رد الوحدة التنظيمية على الطلب بإبلاغ الطالب برد الوحدة التنظيمية مالكة المعلومات وفق التالي:
   - في حال الموافقة؛ تقوم العمادة بالتحقق من شخصية الطالب وإثبات ذلك بالمعززات،
   - في حال عدم الموافقة؛ يتم إعلام الطالب بذلك وتزويده بصورة من النموذج مبين عليه أسباب عدم الموافقة بعد التأكد من شخصية الطالب واثبات ذلك بالمعززات.

بند (17):

يتم الرد على طلبات الحصول على المعلومات التي تم استقبالها بشكل ورقي أو بشكل إلكتروني سواء بالموافقة أو الرفض خلال فترة 30 يومًا تحسب من اليوم التالي لتاريخ تقديم الطلب، وفي حال عدم مراجعة طالب المعلومة للجامعة أو المفوض عنه وتجاوزت فترة التأخير (30) يومًا أخرى يعتبر الطلب ملغيًا تلقائيًا ويعاد وعاء المعلومات المطلوبة إلى الوحدة التنظيمية مالكة المعلومات.

بند (18):

بالإضافة إلى ما ورد سابقاً تتولى العمادة المهام التالية:

- تعيين شخص في العمادة مسؤولًا عن متابعة الطلبات التي ترد عبر رابط طلبات الحصول على المعلومات من خلال الموقع الإلكتروني للجامعة على شبكة الإنترنت.

- الاحتفاظ بنسخ من طلبات الحصول على المعلومات وبسجل لمتابعة الطلبات الواردة للجامعة، وتحدد مدة الاحتفاظ بنسخ الطلبات والسجل وفقاً للتعليمات التطبيقية لحفظ الوثائق في المستودعات الأمينة والعادية ولدى دوائر الجامعة وفروعه ومكاتبه وإتلافها النافذة، ويتم إنشاء سجل خاص بطلبات الحصول على المعلومة بحيث تكون الطلبات بأرقام تسلسلية بغض النظر عن صيغة النموذج ورقيًا كان أو الكترونيًا.

بند (19):

يتولى القسم الاحتفاظ بنسخ عن طلبات الحصول على المعلومات التي ترد بشكل ورقي وبسجل تسليم الطلبات، وتحدد مدة الاحتفاظ بنسخ الطلبات والسجل وفقاً للتعليمات التطبيقية لحفظ الوثائق في المستودعات الأمينة والعادية ولدى دوائر الجامعة وفروعه ومكاتبه واتلافها النافذة.

بند (20):

- يتم نشر آلية تقديم طلبات الحصول على المعلومات على الموقع الخارجي للجامعة وفي حال ورود طلبات للحصول على المعلومات من قنوات خارج إطار الآلية المنشورة تُعاد هذه الطلبات إلى مرسليها مع الرد بضرورة الالتزام بالآلية.
- يجب على القسم توفير السبل والآليات المناسبة بما يضمن مراعاة طالبي المعلومات من ذوي الإعاقة أو الفئات التي تعاني من فقدان بعض الحواس وكذا فئة الأميين.

بند (21):

تنطبق الآلية الوارد ذكرها سابقاً على العاملين في الجامعة بصفتهم الشخصية وذلك بحالة طلبهم للمعلومات التي تخص أعمال الجامعة.

أحكام عامة

بند (22):

يحظر إخراج المعلومات المصنفة ضمن أي من المستويين الأول و الثاني من الجامعة ما لم تكن الضـرورة قد اقتضـت ذلك وعلى أن تكون مقرونة بموافقة معالي رئيس الجامعة أو من ينوب عنه، ويمنع الاحتفاظ بها في المسـاكن والاماكن العامة كما يحظر طباعتها أو نسـخها خارج الجامعة.

بند (23):

تُطبق التعليمات في البنود أعلاه مع مراعاة نظامي الموظفين والمستخدمين والسياسات الأمنية في الجامعة والأنظمة والتعليمات الأخرى ذات العلاقة.

المادة (10): الشبكات و الآمن

تلتزم عمادة تقنية المعلومات بما يلي:

- تتم التحديثات لجميع مكونات البنية التحتية للشـبكة **Switches, Routers, assess point, firewall, and ect**.. كل ما تتطلب الامر، أو أن وجود أصدرا جديد.
- تكون التحديثات مطابقة لإعدادات الموصي بها من قبل الشركة الأم.
- لا تزيد الفترة بين التحديثات عن ستة شهور.
- تضمن العمادة أفضل الممارسات التقنية في مجال الشبكات.
- مراقبة الشبكة ومسحها لتأكد من عدم وجود ثغرات مرة كل شهر أو عند الطلب من إدارة العمادة أو وحدة الأمن السيبراني.
- يتم تأمين مواقع الموزعات والمحولات وترقيمها وتوثيقها وفقا لمعايير الجودة.
- يتم تحديث خريطة الشـبكة كل شـهرين، وتزويد وحدة التطوير بالعمادة بأحدث المخططات.
- حجب مواقع الإنترنت غير المتلائمة مع بيئة الجامعة، كما سـيتم حظر البروتوكولات الخاصة بالمواقع التالية:
  - الإعلانات والإطارات المنبثقة.
  - المواقع التي تحتوي على مواد إباحية أو تروج للممنوعات.
  - المواقع الخاصة بالمقامرة.

- مواقع الهاكرز أو التي تحتوي على مواد وأدوات الاختراق .
- مواقع وبرامج التحميل السريع.
- مواقع وبرامج التجسس.
- المواقع التي تقوم بإرسال بريد يحتوي على روابط الغش والاحتيال.
- المواقع التي تحث على التعصب والعنف بكافة صوره.

- جميع الأجهزة الموجودة داخل شبكة الجامعة يجب أن تكون مضافة على المجال (نطاق الجامعة)، وأي جهاز لم تتم إضافته سوف يتم فصل الشبكة عنه.
- توفير شبكة عالية الحماية للمستخدمين سواء كانت شبكات داخلية أو شبكات عمومية للمنافذ الأمنة فقط.
- المراقبة وتدقيق حجم بيانات الشبكة وذلك لضمان المحافظة على جودة الاتصال.
- الدخول للخدمة يجب أن يكون محميًا من خلال وسائل التحكم بالاتصال مثل تطبيقات الويب وجدار الحماية. سيتم تحديث برامج الحماية حال صدور التحديث، أو عند طلب ذلك من العمادة أو وحدة الأمن السيبراني.
- يتم الإشراف على تركيب معدات الشبكة في مركز البيانات أو مواقع الجامعة من قبل وحدة الشبكات.
- وضع وتفعيل خطط وأنظمة إدارة الكوارث.

العمادة (11): VPN

- يتم تقديم طلب الحصول على VPN من صاحب الصلاحية في العمادة من خلال النموذج المعتمد.
- يخضع الطلب لمعيار الاستخدام المقبول والاستخدام الفعال.
- صلاحية VPN الممنوحة تعتبر سرية للغاية ويقع على عاتق الأشخاص المخولين المصرح لهم من قبل العمادة التأكد عدم مشاركة الخدمة مع أي شخص.
- على الجهاز المتصل بـ VPN أن يكون مزود برنامج حماية من الفيروسات.
- يتم أيقاف حساب VPN إذا لم يتم استخدامه لمدة سبعة أيام، وفي حال الرغبة في تجديده يجب إشعار العمادة بمدة لا تقل عن سبعة أيام قبل انتهاء صلاحية الحساب.
- يتم قطع خدمة VPN بعد ثلاثين دقيقة من الخمول في الاستخدام.
- أي نشاط مشبوه قد يؤدي إلى انقطاع الخدمة والمساءلة النظامية.

المادة (12): قواعد البيانات والنسخ الاحتياطي و الخوادم.

- العمادة مسؤولة عن أعمال الصيانة والدعم لقواعد البيانات.
- يجب تجنب عملية النسخ الاحتياطي اليدوية التي تعتمد على المستخدم النهائي. وأن تتم العملية بشكل تلقائي.
- تحدد مدة الاحتفاظ بالنسخ بناءً على أهمية النظام، على أن لا تقل الفترة عن ثلاثة شهور.
- يجب الاحتفاظ بنسخ سنوية ونصف سنوية.
- يجب أن تشفر ملفات النسخ الاحتياطية بمفتاح تشفير لا يقل عن **256 bit** .
- يجب استخدام التخزين السحابي -إن وجد- بأقصى حدوده، لتوفير المساحات وتفعيل إدارة الكوارث.
- يتم تحديد جدول النسخ الاحتياطي اليومي، الاسبوعي، الشهري، السنوي حسب أولوية وحساسية الHنظمة وتُخطر إدارة العمادة بذلك.
- يجب على كل الأقسام أن تحفظ نسخة احتياطية لخوادمهم في حال أي فشل في معدات الخادم وتتحمل مسؤولة فقدان البيانات.
- بتم اتباع السياسات الموصي بها من شركة مايكروسوفت فيما يخص **Active Directory**، وفق آخر أصدار، وبما يشمل جميع الخواص (**Centralized management , resource, Exchange, Domain-based, Group Policy, ... etc**).

- يتم اتباع السياسات الموصي بها من مايكروسوفت فيما يخص DNS، وفق اخر أصدار.
- تكون خدمة الاستضافة بالمشاركة في مركز البيانات المتواجد داخل حرم الجامعة الرئيس، بعد الحصول على موافقة عمادة تقنية المعلومات.
- طالب خدمة الاستضافة بالمشاركة علية تقديم الطلب حسب النموذج الخاص بذلك، مع كتابة أسباب مقنعة لطلبه وتوضيح مواصفات الخادم، وتحتفظ العمادة بحق رفض الطلب.
- تضمن وحدة الخوادم وقواعد البيانات الاستخدام الامثل للخوادم، كما تضمن تحديثها وصيانتها بشكل دوري.
- توقف خدمة الاستضافة في حال مخالفة السياسات، أو عدم وجود نشاط فعال لمدة ستة شهور على سيرفر الاستضافة.
- جميع بيانات النسخ الاحتياطي، وملكية الأنظمة والبرمجيات، و الاحتفاظ بالبيانات، و الاحتفاظ بالنسخ، واسترجاع البيانات، و وصف المدة الزمنية للاحتفاظ بها، والنسخ الاحتياطية من البرمجيات يجب أن تكون موضحة بشكل تفصيلي.
- استرجاع البيانات من النسخ الاحتياطية يتم بعد:
  - الاختراقات والهجمات السيبرانية.
  - تلف أو حذف أو تعديل الملفات.
  - عندما تطلب النسخ الاحتياطية المؤرشفة.
  - عند طلب البرمجيات والأنظمة على أن يتم من خلال نظام ادعمني وبموافقة إدارة للعمادة.

العادة (13): سياسة أمن تقنية المعلومات

توفر هذه السياسة إرشادات لحماية واستخدام أصول وموارد تقنية المعلومات داخل العمادة لضمان سلامة وسرية البيانات والأصول.

الأمن المادي

- بالنسبة لجميع الخوادم وأجهزة الشبكة وأصول الشبكة الأخرى، يجب تراعى معدات السلامة في أماكن تواجدها، وتكون منطقة تواجدها ذات تهوية مناسبة ووصول متاح لموظفي العمادة، وأن تراعى التدابير الأمنية مثل لوحة المفاتيح والقفل وما إلى ذلك.
- تقع على عاتق قسم الشبكات وأمن المعلومات مسؤولية ضمان اتباع هذا المطلب في جميع الأوقات. ويلتزم أي من منسوبي الجامعة بالإخطار الفوري في حالة حدوث خرق، وعلى كافة منسوبي الجامعة إبلاغ العمادة عن أية حوادث أمنية تتعرض لها أجهزة الحاسب التي بحوزتهم لحظة اكتشاف حدوثها، بما فيها الحوادث الأمنية السيبرانية و/أو الحوادث الأمنية المادية (مثل حالات السرقة و الضياع و الأعطال التي قد تتعرض لها الاجهزة).
- مسؤولية أمن وسلامة الاجهزة الشخصية (جهاز مكتبي، جهاز محمول، أيباد، وخلافه) تقع على عاتق مستلمها.
- في حال الإضرار المتعمد سوف تطلب العمادة التعويض المادي، والمسائلة القانونية لمسبب الضرر.

أمن المعلومات

- تتولى وحدة قواعد البيانات والسيرفرات إجراء النسخ الاحتياطي لجميع بيانات الجامعة سواء الحساسة أو القيمة أو الحرجة، وتوفير قائمة مرجعية لإدارة العمادة لجميع البيانات التي تم نسخها.
- القائمة المرجعية تشمل بيانات تفصيلية عن (الفترات بين النسخ، مكان حفظها داخل الجامعة أو خارجها أو على السحابة، درجة اهميتها،).
- تقع على عاتق وحدة قواعد البيانات والسيرفرات تثبيت وتحديث برنامج مكافحة فيروسات في جميع المعدات التقنية التي لها اتصال بالإنترنت.
- جميع المعلومات المستخدمة في العمادة تلتزم بقوانين الخصوصية ومتطلبات السرية الخاصة بالعمادة والرجوع إلى سياسة السرية.

الوصول إلى التقنية

- كل شخص من منسوبي الجامعة يحمل رمز تعريف فريد للوصول إلى الخدمات التقنية للعمادة، ويكون تعيين كلمة مرور مسؤولية الشخصية.
- يتم اتباع سياسات كلمة المرور عند تعينها.
- تقع على عاتق وحدة قواعد البيانات والسيرفرات مسؤول عن إصدار رمز التعريف وكلمة المرور الأولية لجميع منسوبي الجامعة.

المادة (14): إدارة الأصول

تهدف هذه السياسة إلى وضع الاجراءات والمنهجيات لإدارة الأصول التقنية.

- أن كل من المعدات التقنية والبرمجيات والمعلومات والخدمات هي اصول تقنية للعمادة.
- إدارة وتوثيق وصيانة وتحديث الأصول التقنية مسؤولية على عمادة تقنية المعلومات.
- تتولى العمادة مهمة توفير نظام أمن لإدارة الأصول.
- نظام إدارة الأصول يجب أن يحتوي على البيانات التفصيلية والتعريفية للأصول، ووصفها ومكانها وتصنيفها وقيمتها وترقيمها ومالكها.
- المعلومات الموجودة في قاعدة الأصول هي معلومات ذات سرية عالية. يجب عدم تسليمها أو الافصاح عنها للجهات الخارجية أو الشركات دون موافقة إدارة العمادة.
- تتولى إدارة الأصول جميع اتفاقيات الخدمة، وتوثيق الصيانة والتراخيص.
- تلتزم إدارة الاصول بجميع سياسات عمادة تقنية المعلومات وتقوم بالتنسيق مع جميع وحدات العمادة.

المادة (15): إدارة الحوادث الأمنية واستمرارية العمل

توفر هذه السياسة إرشادات لإدارة الطوارئ لجميع المعدات التقنيات داخل العمادة.

- تتولى كل وحدة داخل العمادة وضع خطة طوارئ في حال حدوث فشل لجميع أو لأحد الأنظمة أو الخدمات المقدمة، سواءً في معداتها أو برمجياتها.
- تزود إدارة العمادة بالخطة من تاريخ إقرار السياسة وتحدث بشكل سنوي على الاقل.
- تشمل الخطة معلومات التواصل التفصيلية للأشخاص أو الشركات (معلومات الاتصال للمعنيين عن كل خدمة سواء كانوا جهات داخلية أو خارجية).
- تشمل الخطة الوصف التفصيلي للإجراءات المتخذة ومدة الاستجابة المتوقعة.
- تقع على عاتق كل وحدة اختبار خطة الطوارئ بشكل دوري، وتقديم تقرير مفصل حول جدواها.
- تشمل الخطة آلية التبليغ الفوري عن الأخطار، واجراءات التصعيد.

المادة (16): سياسة إدارة واستخدام الأنظمة

أن نجاح عمادة تقنية المعلومات يعتمد بشكل أساسي على الالتزام بالتشريعات المشار إليها في وثيقة السياسات لتقنية المعلومات، وعلى سرية المعلومات غير المعلنة، ويشمل ذلك بيانات الدخول وقواعد البيانات والمعلومات الخاصة بالبحث والتطوير والإنتاج والتسويق وإدارة الأنظمة واستخدامها والمجالات الأخرى.

وحرصا من عمادة تقنية المعلومات على تنظيم العلاقة بين (وكالات وكليات وعمادات وإدارات) الجامعة من جهة وبين عمادة تقنية المعلومات، فقد تم تحديد سياسة إدارة واستخدام أنظمة المعلومات في جامعة الحدود الشمالية وفقًا لما يلي: -

- على مالك النظام أن يلتزم بسياسة الاستخدام المقبول والفعال والمشار إليها في فقرة السياسات العامة للأنظمة المدارة من قبله.
- تخضع كافة أنظمة المعلومات لسياسة النسخ الاحتياطي المتبعة في عمادة تقنية المعلومات وحسب سياسة النسخ الاحتياطي المشارة اليها في المادة (12).
- تخضع كافة أنظمة المعلومات في الجامعة لسياسة أمن المعلومات كما ورد في المادة (9) من سياسات عمادة تقنية المعلومات وذلك لضمان السرية الكاملة للأنظمة.
    - تخضع جميع أنظمة المعلومات في الجامعة لمتطلبات الحوكمة والتدقيق والتصنيف والمراقبة وكافة المتطلبات التي تطلبها الجهات الحكومية والرقابية في المملكة مثل متطلبات الأمن السيبراني ومتطلبات هيئة الحكومة الرقمية ومتطلبات ديوان المحاسبة وهيئة الرقابة ومكافحة الفساد (نزاهة) وغيرها من الجهات الرقابية والتنفيذية الأخرى، مع الالتزام بما يلي:

- وضع قواعد التحقق من صحة البيانات **Validation Rules** لتحديد مجال قبول البيانات في الحقول المستخدمة مثل (قيمة الحقل العُليا والدنيا والقيم خارج النطاق وغيرها).
- التحقق من مطابقة البيانات المدخلة للشكل المطلوب، مثل (التأكد من عدم وجود حروف غير صالحة متناقضة) في حقل البيانات.
- تحديد الحقول المهمة وتمييزها بإشارات خاصة تدل عليها إلزامية حقل البيانات.
- التأكد من توافق البيانات المدخلة وعدم تعارضها مع القوانين واللوائح والتشريعات.
- مراقبة أداء الأنظمة إما بالطرق المؤتمتة أو الطرق الأخرى لضمان حماية الأنظمة من الهجمات الشائعة أو الأخطاء البشرية مثل (الهجمات السيرانية أو تجاوز سعات التخزين وغيرها).
- استخدام أدوات مساعده **Assistant Tools** أخرى للتحقق من صحة البيانات المدخلة والتأكد من استكمالها ومعالجتها بالشكل الصحيح.

- تخضع كافة أنظمة المعلومات لنظام صلاحيات الدخول والاستخدام حسب ما تقتضيه المصلحة بالتنسيق بين الجهة المستفيدة وعمادة تقنية المعلومات، وضمن الضوابط التالية:

- لا يتم منح صلاحية دخول واستخدام لأي نظام معلومات إلا بموجب طلب رسمي موقع من الرئيس المباشر في الجهة المستفيدة وبعد موافقة عميد تقنية المعلومات.
- تخصص نماذج خاصة لطلب صلاحيات الدخول والاستخدام ويشمل نموذج المعلومات:

1- بيانات طالب الصلاحية (الاسم، رقم السجل، الايميل، مكان العمل، الصفة الوظيفية، رقم الهاتف).

2- نوع الطلب (جديد، اعادة تفعيل، حجب أو تعديل صلاحية).

3- مستوى الصلاحية (بيئة تجريبية، بيئة النظام الحقيقة).

4- تاريخ تفعيل الدخول وتاريخ انهاء الصلاحيات.

5- مستوى الوصول (مستوى قواعد البيانات او مستوى التطبيقات، أو مستوى وظائف النظام).

6- طبيعة العمل (حذف ، تعديل، إدخال، إنشاء ، إنشاء صفحات، صلاحيات تعديل كود، وخلافه).

7- مصادقة من المسؤول المباشر على طلب الصلاحية.

- تعتبر أي صلاحية ممنوحة دون استيفاء نموذج إنشاء الصلاحية ومراحله الإجرائية ومصادق عليه، صلاحيه غير نظامية ويتحمل المسؤولية القانونية كل من يستخدم النظام دون موافقة رسمية.
- يمنع التواصل المباشر من الجهة المستفيدة مع موظفي عمادة تقنية المعلومات المسؤولين عن إنشاء الصلاحيات أو إدارتها أو قواعد البيانات، وأي تواصل بغير القنوات الرسمية يعتبر مخالفة نظامية ومحاولة للانحراف عن التعليمات.
- أي طلب للتغيير على إجراءات سير عمل النظام أو إضافة خصائص جديدة للنظام أو تعديلها أو حذفها، يجب أن تتم بطلب خطي من مالك النظام وبإشراف عمادة تقنية المعلومات.
- يحتفظ مالك النظام بسجل طلبات الدخول ويتم مراجعته كل ثلاثة شهور بتنسيق مع عمادة تقنية المعلومات.
- إذا حدث تغير مفاجئ على النظام، مثل تغير موقع استضافة النظام أو تغير مشغل النظام فإنه يجب مراجعه سجل الصلاحيات فوراً للقيام بالإجراءات الاحترازية لضمان عدم دخول غير المخولين للنظام.
- يجب على مالك النظام الاحتفاظ بما يلي:

a. سجلات الدخول والخروج الناجحة والفاشلة.

b. إعادة تشغيل وإيقاف تشغيل النظام الناجح والفاشل.

c. تغيرات سياسات الأمان الناجحة والفاشلة.

d. إدارة المستخدم والمجموعة الناجحة والفاشلة.

e. الدخول إلى الملفات الناجح والفاشل.

f. استخدام حقوق المستخدم الناجح والفاشل.

- يحق لعمادة تقنية المعلومات طلب تقرير من مالك النظام يوضح السلوك غير الطبيعي للنظام، وعلى مالكه تسليم التقرير خلال مدة لا تتجاوز 24 ساعة من تاريخ طلبه، ويشمل السلوك غير الطبيعي للنظام الآتي:

1- الحمل الزائد على النظام.

2- زيادة عدد العمليات قيد التشغيل.

3- الزيادة المفاجئة لاستخدام وحدة المعالجة المركزية.

4- خلق اتصالات غير عادية أو قطعها.

5- إنذارات من الجدران النارية.

6- محاولات الدخول المتكررة.

7- الدخول عبر منافذ غير اعتيادية.

- تحتفظ عمادة تقنية المعلومات بكل من السجلات التالية:

1- سجلات كشف التسلل إلى النظام.

2- سجلات الجدار الناري.

3- سجلات حساب المستخدم.

4- سجلات مسح الشبكة.

5- سجلات أمان التطبيق.

6- سجلات الأمان.

- تلتزم عمادة تقنية المعلومات برفع تقرير سنوي إلى مالك النظام حيال وضع النظام من حيث الحسابات النشطة والصلاحيات الممنوحة لها، طلبات التغيير على إجراءات سير عمل النظام وكل ما يستجد من اجراءات قد تقع عليه، على أن تقوم الجهة المالكة للنظام بالرد على أي

ملاحظة حيال التقرير خلال سبعة أيام عمل من تاريخ إرساله، وفي حال عدم الرد تعتبر موافقة من الجهة المالكة على كل ما ورد فيه.

- تطبق السياسات على كافة الأنظمة التي يتم إنشاؤها داخل عمادة تقنية المعلومات أيضا.
- يقوم مالك النظام بتعبئة المعلومات العامة عن النظام والبيانات الإحصائية باللغتين العربية و الانجليزية على نظام حصر الخدمات، انسجامًا مع بنود الخطة الاستراتيجية للجامعة، وتحقيقًا لمتطلبات هيئة الحوكة الرقمية وبرنامج (يُسر).

فريق العمل

رئيس الفريق

الدكتور / سلطان بن صالح الخليوي
عميد تقنية المعلومات

محرر الوثيقة

الدكتور / محمود أحمد البواليز

مراجع داخلي

الدكتور / شهرين بن أزوان نذير

مراجع خارجي

الدكتور / أحمد العمري

دليل السياسات والاجراءات لعمادة تقنية المعلومات