المملكة العربية السعودية
وزارة التعليم
جامعة الحدود الشمالية

جامعة الحدود الشمالية
NORTHERN BORDER UNIVERSITY
إدارة تقنية المعلومات

Kingdom of Saudi Arabia
Ministry of Education
Northern Border University

دليل السياسات والإجراءات
لإدارة تقنيـة المعلومـات

الإصدار الثالث
2024م - 1446هـ

المحتويات

الملاحـق

- الملحق 1

  سياسة حماية البيانات الشخصية

- الملحق 2

  سياسة التخزين والاستبقاء

- المحلق 3

  طلب الحصول على VPN

- الملحق 4

  نموذج طلب مشروع

- الملحق 5

  تصريح دخول لمركز البيانات

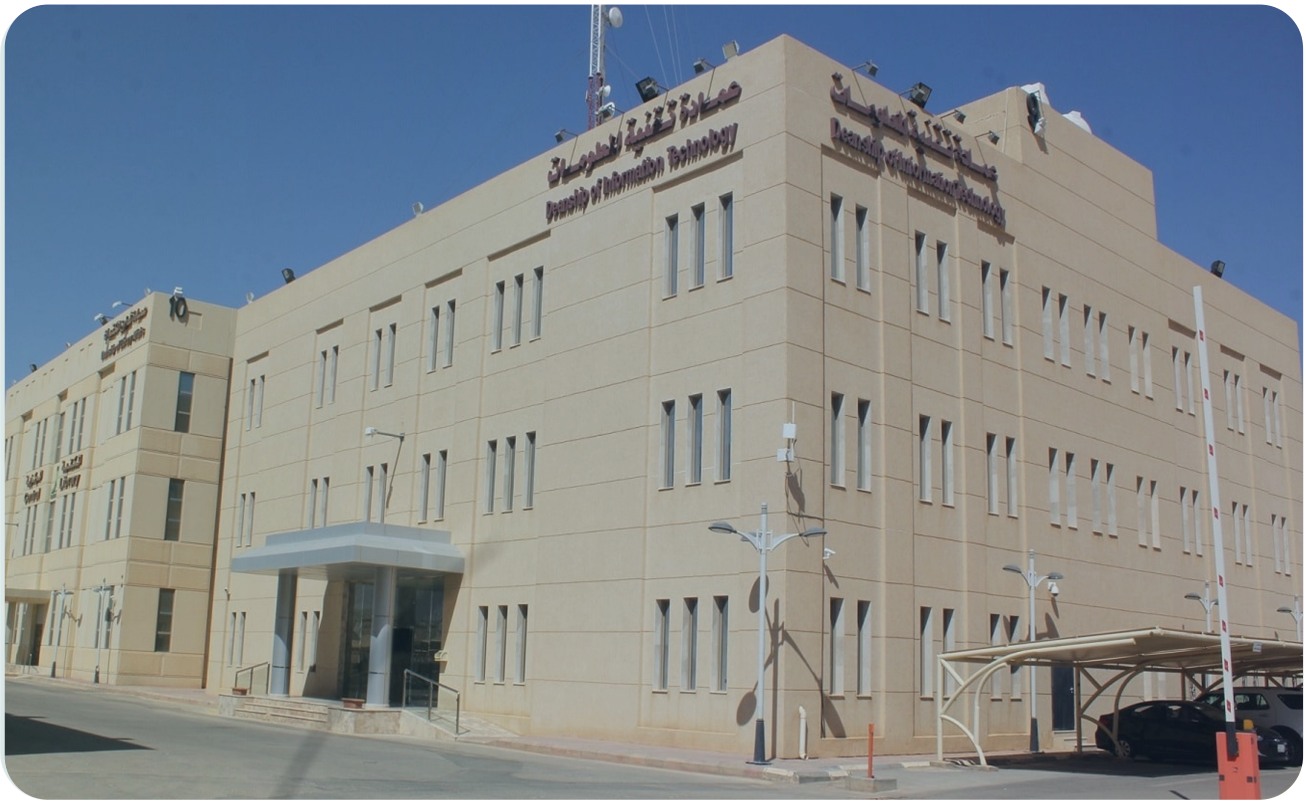
- الملحق 6

  نموذج طلب صلاحية على البوابة

- الملحق 7

  سياسة إدارة المحتوى

بسم الله الرحمن الرحيم



عمادة تقنية المعلومات

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

الرؤية

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

الرسالة

العمل بروح الفريق الواحد والتفاني 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 المبنية بجانبها مالم يقتض السياق خلاف ذلك:

السياسات	هي حزمة القواعد والقوانين التي تنظم علاقة المستخدمين والإدارة داخل المؤسسة.
الجامعة	جامعة الحدود الشمالية في عرعر وفروعها في شطري الطلاب والطالبات.
الإدارة	إدارة تقنية المعلومات في الجامعة.
الاجهزة المدعومة	الأجهزة الالكترونية 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 وكذلك موظفي الشركات التي تتعامل مع الجامعة ممن له صلاحية الدخول على شبكة الجامعة او أجهزتها أو أجهزة قاعات التدريس وأجهزة المعامل.
البوابة	بوابة الدخول على الموقع الالكتروني 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. وإدارة 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 جميعا الالتزام بما جاء في هذه الوثيقة عند استخدام أو التعامل مع أصول المعلومات الخاصة بالجامعة.

السياسات العامة:

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 جميعا الالتزام بما جاء في هذه الوثيقة عند استخدام أو التعامل مع أصول المعلومات الخاصة بالجامعة.

الاستخدام المقبول

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

مستوى الأمان

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

الاستخدام غير المناسب

بعد استخدام مصادر التقنية التي توفرها الجامعة لأية أغراض تخالف الأنظمة والقوانين والأعراف المجتمعية والقيم الإسلامية استخداما غير مناسب، ويشمل ذلك ولا يقتصر على إعداد أو تحميل أو تنزيل أو نشر محتويات تتضمن عنفا أو تهديداً أو تضليلا أو فكراً متطرفا، أو غير ذلك من المواد المجرمة معلوماتياً، ويدخل في ذلك أيضا اتخاذ أي خطوات من شأنها أن تنتهك حقوق الملكية الفكرية لأي طرف كما يدخل في الاستخدام غير المناسب توظيف موارد الجامعة التقنية لآية 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 الأنظمة الجامعة التقنية أو التحايل عليها.

الامتثال من جانب المستخدم

جميع المواد والبنود والشروط المنصوص عليها في هذه الوثيقة تمثل اتفاقا بين جميع الأطراف، ويجب أن تصنف وتفسر طبقاً 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 أصل من أصول التقنية، ويقع على عاتق مالكي الأصول حمايتها وجردها وتزويد إدارة الأصول بالعمادة ببيانات تلك الأصول بشكل دوري، وتخضع الجميع السياسات الواردة بالدليل.

التعهد

أنا أفهم وأتعهد بالالتزام بسياسة استخدام الحاسب والإنترنت كما أفهم أن أي مخالفة. لهذه السياسة بعد 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.

أحكام عامة:

1. تكون مرجعية تفسير النصوص الواردة في هذه السياسة من اختصاص إدارة تقنية المعلومات.
2. أي سياسات لم يرد بها نص في هذه السياسة تكون من اختصاص هيئة الحكومة الرقمية.
3. أي تعديلات أو إضافات على هذه السياسة تخضع لموافقة اللجنة الدائمة للتعاملات الالكترونية.
4. يتم تعديل أو اصدار نسخ محدثة من السياسات مرة واحدة كل سنة على الأقل أو إذا لزم الأمر.

المادة (1) السياسات والإجراءات الخاصة بالصيانة والدعم

أ- الصيانة الدوريـــة

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

ب- الدعـم

1. الدعم التقني للمستخدمين هو خدمة مقدمة من قبل إدارة تقنية المعلومات.
2. تقدم طلبات الصيانة والدعم من خلال المنافذ التي تحددها إدارة تقنية المعلومات، سواء كانت من خلال طلبات ورقية أو الكترونية أو برامج أو منصات الكترونية خاصة أو من خلال البوابة الالكترونية.
3. تتوفر خدمة الدعم التقني للمستخدمين خلال ايام وساعات العمل الرسمي.
4. تتم الاستجابة لطلبات الدعم حسب الأولويات، ويراعى عند ترتيب الأولوية درجة خطورة الطلب والموقع الوظيفي لمقدم الطلب، مع احتفاظ الإدارة بالحق في تحديد الأولويات وترتيب الاستجابة.
5. تصنف طلبات الصيانة الواردة حسب الاولوية الى أربعة أنواع هي:
   - **حرجة:** وتعني أن الوضع حرجة للمقدم الطلب كأن يكون هناك توقف للعمل ولا يوجد حل متاح. فتتم الاستجابة مباشرة.
   - **عالية:** الميزات الهامة غير متوفرة، لكن العمل يمكن ان يستمر على نحو معين والحل متاح. وتتم الاستجابة خلال مدة لا تتجاوز يوم عمل واحد.
   - **متوسطة:** وهذا يعني ان المنتج لا يعمل بالشكل الذي صمم من أجله مما أدى الى فقد طفيف في الخدمة. فتتم الاستجابة في مدة لا تتجاوز 3 أيام عمل
   - **منخفضة:** وهذا يعني انه لا يوجد أي فقد في الخدمة وقد يكون الطلب بغرض الحصول على بعض الملفات او المعلومات او تحسين المنتج. فتتم الاستجابة في مدة لا تتجاوز سبعة أيام عمل.
6. تحدد إدارة تقنية المعلومات آلية تقديم الدعم الفني المناسب حسب ما تقتضيه طبيعة المشكلة، إما من خلال مشاغل الإدارة أو من خلال المشاغل المتنقلة أو عن بُعد من خلال الإنترنت او الهاتف.

المادة (2) السياسات والإجراءات الخاصة بإدارة الحسابات

أولاً: كلمة المرور

تعد كلمات المرور من اهم خطوط الحماية لحسابات المستخدمين على الأنظمة والخدمات التقنية العاملة في بيئة الجامعة. وقد ينتج عن استخدام كلمة المرور الضعيفة او التي لا تتماشى مع أفضل معايير الأمان اختراقات أمنية على أصول المعلومات الخاصة بالجامعة؛ ولذلك كان لزاماً على كافة مستخدمي الحسابات المخصصة للوصول الى أصول المعلومات في الجامعة الالتزام بمعايير كلمات المرور وتقع عليهم مسؤولية اتخاذ الإجراءات اللازمة لاختيار كلمات المرور الخاصة بحساباتهم او بتلك الحسابات المسندة ادارتها إليهم.

أ- 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:

راجع ملحق سياسة حماية البيانات الشخصية المادة الخامسة الفقرة رقم (10).

1. ألا يقل طول كلمة المرور عن 10 خانات للمستخدم و15خانة لمدريي الانظمة.
2. ان تحتوي على مزيج من الحروف الكبيرة والصغيرة والأرقام والرموز الخاصة مثلاً: r$cYv4m@3j8
3. يتم تغير كلمة المرور كل 45 يوم لمدراء انظمة التشغيل.
4. شفرة (كود) التحقق الثنائي المرسل الى هاتف المستخدم مكون من 6 خانات.
5. الوقت المسموح به لدخال كود التحقق الثنائي قبل انتهاء صلاحيته هو 2 دقائق.
6. يتم تجميد الحساب لمدة 15 دقيقة بعد خمس محاولات دخول فاشلة.

ب- السياسات التنفيذية والإجراءات لتعيين كلمة المرور:

راجع ملحق سياسة حماية البيانات الشخصية المادة الخامسة الفقرة رقم (7) والفقرة رقم (10).

1. يقوم مدير النظام بتفعيل خيار تعيين كلمة مرور عند إنشاء حساب جديد.
2. يتم تفعيل خيار تغيير كلمة المرور عند الدخول عن طريق كود التحقق الثنائي، وذلك استجابة لطلبات فقدان كلمة المرور الواردة من المستخدمين .
3. يجب الا تكون كلمة المرور فارغة، والا تكون مشابهة لاسم المستخدم، والا تكون معتمدة على معلومات شخصية مسجلة في النظام، مثل اسم المستخدم، هويته او مسماه الوظيفي.

4. ألا تكون من آخر 5 كلمات مرور تم استخدامها مسبقا.
5. يحظر على المستخدمين إفشاء كلمة المرور لأي شخص بما في ذلك موظفي إدارة تقنية المعلومات، الطلاب، أعضاء هيئة التدريس والموظفين. ولدى موظفي قسم أنظمة التشغيل في الإدارة القدرة على توفير الدعم للمستخدمين دون الحاجة للكشف عن كلمات المرور الخاصة بهم.
6. 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 بشك آمن عندما تنتفي الحاجة لذلك.
7. تجنب استخدام نفس كلمة المرور لحسابات مختلفة.
8. على مستخدمين الحسابات العادية تغيير كلمة المرور كل 90 يوماً.
9. على مستخدمين الحسابات الحساسة تغيير كلمة المرور كل 45 يوماً.

ج- الإجراءات المتبعة في حال الاستخدام غير المشروع لكلمة المرور:

راجع ملحق سياسة حماية البيانات الشخصية المادة الخامسة الفقرة رقم (4) و الفقرة رقم (11)..

1. في حال استخدام غير المشروع 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.
2. عدد المحاولات المسموح بها لاستخدام كلمة مرور خاطئة قبل تجميد الحساب بشكل تلقائي هي 5 مرات.
3. يتم إعادة ضبط عدد مرات السماح بإدخال كلمة المرور بشكل خاطئ بعد 60 دقيقة من إدخال أول كلمة مرور خاطئة.
4. في حال تجميد الحساب رغم عدم إدخال كلمة مرور خاطئة من قبل صاحب الحساب يجب عليه إشعار موظفي تقنية المعلومات بأسرع وقت.

ثانياً: 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 الالكتروني لأي خطر.

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

أ- مستخدمو حساب البريد الالكتروني:

راجع ملحق سياسة حماية البيانات الشخصية المادة الخامسة الفقرة رقم (7) و الفقرة رقم (11)..

- توفر الجامعة حالياً البريد الإلكتروني في المقام الأول إلى تمكين أعضاء هيئة التدريس والموظفين من تسيير أعمال الجامعة بشكل سلس. ويسمح بالاستخدام الشخصي للبريد الإلكتروني، شريطة ألا يؤثر الاستخدام الشخصي جودة الأداء، أو يقلل كفاءة شبكات الجامعة، والا يتعارض مع السياسات الواردة في هذا الدليل أو سياسات الجامعة الأخرى.
- تقدم الجامعة حاليا خدمات البريد الإلكتروني لجميع طلبة الجامعة. ويخضع استخدام لتلك الخدمة للائحة سلوك الطلاب، كما يخضع لسياسة الإدارة لتقنية المعلومات، وسياسة الجامعة للاستخدام المقبول.
- لا يجوز تحويل (Forward) أي بريد الإلكتروني للجامعة أو محتواه إلا ّللغايات المصرح بها للعمل الرسمي وبعد اتخاذ الاحتياطات الأمنية المناسبة الموضحة بند السرية والآمان.

ب- السرية والأمان:

راجع ملحق سياسة حماية البيانات الشخصية المادة الخامسة الفقرة رقم (12).

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

ج- الاحتفاظ بمحتوى البريد الإلكتروني:

راجع ملحق سياسة حماية البيانات الشخصية المادة الخامسة الفقرة رقم (9).

- 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 حيث إن صندوق البريد الإلكتروني ليس المكان المناسب للاحتفاظ بسجلات الجامعة.
- إن البريد الالكتروني ليس المكان المناسب للاحتفاظ بسجلات الجامعة وينصح دائماً بإزالة السجلات الموجودة في البريد الإلكتروني أو نقلها إلى وسائط تخزين إلكترونية أخرى.

د- سياسة البريد الإلكتروني:

البريد الإلكتروني الجامعي هو أحد قنوات التواصل الرسمية المعتمدة في الجامعة ويحمل الحُجيّة القانونية ولذلك:

راجع ملحق سياسة حماية البيانات الشخصية المادة الخامسة الفقرة رقم (12).

1. يتم رفع طلب الحصول على البريد الإلكتروني من خلال نظام الدعم الفني وبموافقة صاحب الصلاحية.
2. يتم أنشاء البريد الإلكتروني الجامعي للمستخدم وفق الاتي: الاسم الأول متبوعاً بنقطة يليه الاسم الأخير (في حال التشابه إضافة الحرف الأول من الاسم الثاني) مضافاً له امتداد نطاق الجامعة @nbu.edu.sa.
3. يجب على منسوبي الجامعة استخدام خدمات البريد الإلكتروني الجامعي في التعاملات الرسمية، ويمنع استخدام خدمات البريد الإلكتروني المجاني مثل Yahoo, Gmail و... .Hotmailإلخ.
4. لا يسمح للمستخدمين باستخدام البريد الالكتروني لأغراض غير لائقة او غير قانونية، ولا يسمح إطلاقا بإرسال رسائل قد تسبب ضررا للجامعة او تؤدي الى تشويه صورتها أو الإساءة الى سمعتها.
5. يحضر مشاركة كلمة المرور.
6. يحظر على المستخدمين نشر او إعادة ارسال رسائل البريد الإلكتروني لأغراض شخصية، أو تجارية، أو دينية، أو سياسية، او غيرها من المحظورات.
7. يحظر على المستخدمين إرسال أو الرد أو توجيه رسائل البريد الإلكتروني التي تحتوي على مرفقات مصابة بالفيروسات أو أي برمجيات ضارة.
8. على المستخدمين الحذر وعدم فتح رسائل البريد الإلكتروني غير المرغوب فيها، مع حذفها من النظام.

9. يحظر على المستخدمين استخدام نظام البريد الإلكتروني للجامعة لانتحال صفة شخص آخر.
10. يحظر على المستخدمين استخدام نظام البريد الإلكتروني الخاص بشخص أخر.
11. على المستخدمين عدم تسجيل أو مشاركة عنوان البريد الإلكتروني الخاص بالجامعة في المواقع الإلكترونية لغير أغراض العمل.
12. يحظر على المستخدمين المشاركة في نشر رسائل البريد الإلكتروني لأغراض جمع التبرعات والأنشطة خيرية.
13. يجب تذييل جميع رسائل البريد الإلكتروني الصادر من الجامعة بنص إخلاء المسؤولية التالي:

إخلاء المسؤولية: تمثل هذه الرسالة وما تحويه من مرفقات (إن وجدت) وثيقة سرية قد تحتوي على معلومات محمية بموجب القانون، إذا لم تكن الشخص المعني بهذه الرسالة فيجب عليك تنبيه المرسل بخطأ وصولها إليك، وحذف الرسالة ومرفقاتها (إن وجدت)، ولا يجوز لك نسخ أي جزء من هذه الرسالة ومرفقاتها (إن وجدت) أو توزيعها، أو البوح بمحتوياتها، أو استعمالها لأي غرض؛ علماً بأن محتوى هذه الرسالة ومرفقاتها (ان وجدت) تعبر عن رأي المرسل وليس بالضرورة رأي جامعة الحدود الشمالية ، ولا تتحمل الجامعة أي مسئولية عن الأضرار الناتجة عن هذا البريد الإلكتروني ومحتوياته.

14. على المستخدم الحذر عند إعادة توجيه أي بريد إلكتروني، وعدم توجيه البريد الإلكتروني غير المرغوب فيه والإعلانات التجارية والبريد العشوائي.
15. لا يُسمح للمستخدمين بإرسال أو الرد أو توجيه رسائل البريد الإلكتروني ذو المحتوى السري أو التي تنتهك حقوق الملكية الفكرية.
16. على المستخدمين عدم استخدام خاصية إعادة التوجيه التلقائي إلى أو من عناوين البريد الإلكتروني الخارجي.
17. عند استخدام البريد الإلكتروني في الهاتف النقال مثل الهواتف الذكية، يراعى تزويده بميزة قفل الأمان التلقائي وكلمة المرور في حالة عدم استخدام الهاتف.
18. 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.

هـ- سياسة حذف الحسابات وصناديق البريد الإلكتروني:

عند تلقي إشعار المغادرة النهائية لأي من المستخدمين في الجامعة، تقوم "إدارة تقنية المعلومات" باتخاذ الإجراءات النظامية حسب التصنيف التالي:

راجع ملحق سياسة حماية البيانات الشخصية المادة الخامسة الفقرة رقم (9).

المتعاقدون مع الجامعة عن طريق الشركات

1. يتم إبطال كافة التطبيقات والخدمات -ما لم يستدع الأمر الاحتفاظ بنسخة من البريد لمدة معينة- وفقا للتاريخ المحدد من قبل إدارة الموارد البشرية في الجامعة.
2. يُحذف حساب المجال وصندوق البريد الإلكتروني الخاص بالمستخدم المنتهي عقده.

أعضاء هيئة التدريس والموظفين

1. يتم إبطال كافة التطبيقات والخدمات وفقا للتاريخ المحدد من قبل إدارة الموارد البشرية في الجامعة.
2. يحتفظ عضو هيئة التدريس أو الموظف السعودي الذي انتهت خدماته أو المحال على التقاعد بالبريد الإلكتروني ولا يتم إبطاله. ويمكنه الاستمرار باستخدام نظام البريد الإلكتروني الخاص به في الجامعة.
3. يحفظ البريد الالكتروني الخاص بعضو هيئة التدريس أو الموظف غير السعودي بعد إزالة كل ما يؤدي إلى معرفة صاحبها على وجه التحديد
4. وفق الضوابط التي تحددها اللوائح. وذلك حسب الحالتين الآتيتين:

- إذا توافر مسوغ نظامي يوجب الاحتفاظ بها مدة محُددة، وفي هذه الحالة يجُرى إتلافها بعد انتهاء هذه المدة أو انتهاء الغرض من جمعها، أيهما أطول.
- إذا كانت البيانات الشخصية متصلة اتصالاً وثيقاً بقضية منظورة أمام جهة قضائية وكان الاحتفاظ بها مطلوباً لهذا الغرض، وفي هذه الحالة يتم إتلافها بعد استكمال الإجراءات القضائية الخاصة بالقضية.

الخريجون

1. يتم إبطال كافة التطبيقات والخدمات وفقا للتاريخ المحدد من قبل وحدة الخريجيين في الجامعة
2. يحتفظ الخريج بالبريد الإلكتروني ولا يتم إبطاله، ويمكنه الاستمرار باستخدام نظام البريد الإلكتروني الخاص به في الجامعة.
3. يحتفظ الطالب بحق الدخول الى بياناته / بياناتها الأكاديمية، بصلاحية المحددة من إدارة القبول والتسجيل.

المادة (3) سياسة استخدام الهاتف الشبكي

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.

أ- خدمة الاتصال الخارجي وتحويل المكالمات إلى الجوال:

تقتصر هذه الخدمة على موافقة صاحب الصلاحية معالي رئيس الجامعة.

ب- الاستقالة أو النقل الخارجي:

1. على الموظف الذي قبلت استقالته او نقله الخارجي المبادرة بتسليم جهاز الهاتف الشبكي للموظف الجديد وابلاغ الإدارة ببيانات الموظف الذي سيستلمه أو إعادة الجهاز لإدارة تقنية المعلومات.
2. تقوم ادارة البث المرئي والهاتف الشبكي في إدارة تقنية المعلومات بتحديث دليل الهاتف الشبكي مرة واحدة كل ستة شهور.

ج- طلبات الدعم الفني:

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

المادة (4) سياسة إنشاء أنظمة تقنية المعلومات

أنظمة تقنية المعلومات:

إنشاء أنظمة تقنية المعلومات من قبل الإدارة:

1. تقوم الجهات المستفيدة في الجامعة بتقديم طلب على وفق النموذج -مرفق النموذج ملحق رقم (4) المعد لذلك، ومن ثم تقوم الإدارة بدراسة الطلب وتحليله والرد على الجهة بالموافقة من عدمها مع ذكر المبررات ان وجدت في مدة لا تتجاوز أسبوعين من تاريخ استلامه.
2. إدارة تقنية المعلومات هي الجهة المخولة بتحديد المصادر والتجهيزات التي تدعم النظام المطلوب أنشاءه (كأن يكون برمجة محلية أو شراء من المصدر أو استئجار أو أية طريقة أخرى تراها الإدارة مناسبة).
3. ستقوم إدارة تقنية المعلومات بإدراج طلب النظام وبإشراف مكتب البنية المؤسسية- قبل البدء بباقي الاجراءات على قائمة الانتظار بموجب نظام معد خصيصاً يراعي الأولويات في التنفيذ.
4. 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.
5. بعد اكتمال النظام واختباره، يتم تسليمه إلى الجهة الطالبة بشكل رسمي، وذلك بعد إجراء تدريب مناسب تُقدره إدارة تقنية المعلومات لأفراد من الجهة المستفيدة.
6. يتم تزويد الجهة المستفيدة بنسخة من (دليل المستخدم) باللغتين العربية والانجليزية -إن وجدتا-، وتعود حقوق تصميم وتنفيذ وملكية النظام إلى إدارة تقنية المعلومات.
7. يتم إدراج أيقونة أو رمز يسمى (حول النظام) يحتوي أسماء فريق العمل من مبرمجين ومصممين من شارك في النظام مع الرؤساء المباشرين وذلك حفظاً للحقوق.
8. بعد تسليم النظام للجهة المستفيدة، تعطى هذه الجهة فترة تجريبية لا تزيد عن الشهر للتكيف مع النظام الجديد وإجراء التعديلات اللازمة -ان وجدت- شرط الا تؤثر على جوهر النظام الأصلي.
9. بعد انتهاء الفترة التجريبية، لا يسمح بإجراء أية تعديلات على النظام مهما كانت ويستثنى من ذلك التعديلات الأمنية أو الوظيفية التي تؤثر على عمل النظام
10. يتم تجميع طلبات التعديلات، لغايات اصدار نسخة جديدة محُدثّة من النظام إن كان الأمر يستدعي ذلك بعد مرور سنة على إطلاق النسخة السابقة

المادة (5) مركز البيانات

مركز البيانات:

أ- سياسات العتاد التابع لمركز البيانات:

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

راجع سياسات التخزين والاستبقاء الفقرة رقم (8) و (9).

1. تقدم طلبات التركيب أو التغيير أو الصيانة لأي من مصادر التقنية قبل وقت كاف لا يقل عن 12 ساعة قبل الموعد المطلوب لتنفيذ الخدمة .
2. يقوم الموظف المختص أو مزودو الاجهزة والخدمات بتعبئة نموذج دخول وخروج المعدات لجميع المعدات تركيباً، أو تغييراً، أو صيانةَ، ولا يسمح لهم بالدخول دون إكمال النموذج.
3. يقوم الموظف المختص أو مزودو الاجهزة والخدمات بفحص وتجهيز المعدات في غرفة خاصة قبل تركيبها، أو تغييرها، أو صيانتها.
4. على مدير مركز البيانات ضمان تسجيل جميع المعدات في نظام جرد مركز البيانات، وهو المسؤول عن توفير بيانات تفصيلية لجميع المعدات الموجودة، وتحديث النظام بشكل مستمر.
5. تشمل البيانات التفصيلية للمعدات – ولا تقتصر - ما يلي:
   - **أجهزة النظام:** وصف كامل لمكونات الجهاز، بما في ذلك المورد، الإصدار، رقم الإصدار، الرقم التسلسلي وسائط التخزين الفرعية، النوع، الخ.
   - **برامج النظام:** وصف كاملاً للبرامج الموجودة على الجهاز، بما في ذلك مورد نظام التشغيل، الإصدار، انتهاء الرخصة وغيرها من مكونات البرامج الرئيسية على النظام
   - **وظيفة النظام:** وصف كامل لوظيفة النظام.
   - **استعادة النظام:** الإجراءات الدقيقة لبدء التشغيل والاغلاق والمعلومات الخاصة المتعلقة بالوقوع المفاجئ للمعدة والوقوع المفاجئ للمعدات وحالات الطوارئ الأخرى.
6. يقوم مدير مركز البيانات وموظفيه بإدخال بيانات الصيانة الدورية للمعدات التشغيلية للمركز، ويتم ذلك ورقيًا على بطاقات الصيانة، والكترونيًا على نظام الصيانة.
7. يزود مركز البيانات إدارة تقنية المعلومات بتقرير شهري عن الانجاز والتحديات، وتقرير شامل كل ستة شهور.

8. يزود مركز البيانات إدارة تقنية المعلومات بصلاحيات دخول على جميع أنظمة المراقبة لمركز البيانات.
9. على مدير مركز البيانات التأكد من عمل نظام المراقبة بشكل مستمر (أربع وعشرون ساعة ولمدة سبع أيام في الأسبوع)، والتأكد من تفعيل خاصية الانذار في حالة اي خطر كامن على عمل المركز
10. يمتثل المركز لمعايير السلامة الكاملة المنصوص عليها في قوانين المملكة العربية السعودية ذات الصلة، ووفقا للمعايير الدولية.
11. ينبغي التأكد من جاهزية مصادر تزويد الطاقة البديلة والطارئة مثل وحدات تزويد الطاقة UPS ومولدات الكهرباء Generatorsوأية أنظمة طوارئ أخرى.
12. تجري عمليات التأكد من جاهزية مصادر الطاقة البديلة والطارئة بشكل دوري وبموجب خطة طوارئ خاصة (أسبوعية وشهرية ونصف سنوية وسنوية) وتوثق في سجلات خاصة.

ب- إجراءات الزوار:

(أي شخص ليس موظفاً في مركز البيانات، يعتبر زائر ويجب أن يراعي التالي):

1. ينبغي ان تتم جدولة الزيارات بالتنسيق مع وكيل الإدارة أو من ينيبه قبل وقت كاف لا يقل عن 24 ساعة عن موعد الزيارة.
2. لن يسمح لأي شخص بالدخول إلى مركز البيانات بدون نموذج تصريح الدخول. مرفق النموذج -ملحق رقم 5.
3. يقتصر دخول الزوار لمركز البيانات من المدخل الرئيسي فقط.
4. سيطلب من الزائر أن يوثق حضوره للمركز وعليه أن يكتب اسمه ومسماه الوظيفي والغرض من الزيارة ووقتها، ووقت الخروج.
5. سيكون الزائر مصحوباً أحد موظفي المركز في جميع الأوقات.
6. ينبغي على الزائر ارتداء شارة زائر في جميع الأوقات.
7. على الزائر تجنب لمس المعدات أو التجهيزات التي تنتمي إلى إدارات أخرى.
8. يمنع التصوير بكافة أنواعه (الفيديو والرقمي والفوتوغرافي وغيره) داخل مركز البيانات.

في حال انتهاك أي من هذه الضوابط السابقة سيؤدي إلى إبطال تصريح الدخول إلى المركز، وايقاع العقوبة المناسبة بمن تهاون في ذلك وسمح به.

المادة (6) البوابة الالكترونية للجامعة

البوابة الإلكترونية للجامعة:

أ- قيود الاستخدام:

باستخدامك لبوابة جامعة الحدود الشمالية، تقر بالامتناع عما يلي:

1. استخدام البوابة لأغراض غير لائقة أو غير نظامية.
2. التورط في - أو تسهيل - تبادل الملفات غير المصرح بها لمحتويات يملكها طرف ثالث، ويشمل لك النشر والإتاحة والتحميل والتنزيل والتوزيع غير المصرح به بأي شكل لمحتويات تابعة لطرف ثالث.
3. استخدام البوابة بأية طريقة لأغراض تجارية أو تحقيق أرباح.
4. تحميل ملفات على البوابة تحتوي على برمجيات خبيثة أو التي تلحق ضرراً بالأجهزة أو المعدات.
5. نشر، أو توزيع، أو تعميم مواد، أو معلومات تنطوي على تشويه سمعة لأي طرف أو انتهاكا للأنظمة ويدخل ذلك في أي محتوى غير مقبول دينياً أو اجتماعيًا أو كان مخالفاً للآداب العامة.
6. الانخراط في نقاشات لمواضيع وعناوين غير ملائمة، أو فاضحة، أو عدائية، أو بذيئة، أو غير قانونية.
7. الاشتراك من خلال البوابة في أنشطة غير مشروعة أو تنتهك أي من الأنظمة المرعية في المملكة العربية السعودية.
8. القيام بأي نشاط من شأنه اعتراض -أو محاولة اعتراض- التشغيل الصحيح للبوابة ويدخل في ذلك القيام بأي إجراء يفرض حملاً غير مناسب على البنية التحتية لبوابة الجامعة.
9. الإساءة للآخرين أو ابتزازهم أو الاستهزاء بهم بأي شكل من الأشكال.

ب- مدير البوابة:

1. هو الشخص المعني بتطبيق الاقتراحات والتوصيات سواء كانت تنفذيه، أو إجرائية، أو تطويرية على موقع الجامعة على شبكة الانترنت. (أو محتوى)
2. يكون مسؤولاً مباشراً عن التزام الشركة/الشركات المتعاقد معها لتشغيل وصيانة البوابة وتنفيذ جميع الشروط المنصوص عليها في كراسة العقد.

3. اقتراح الحقائب التدريبية وإعدادها بشكل دوري على جميع المستويات.
4. متابعة ما هو جديد من تطورات تقنية تخص البوابة وتقديم تقارير لإدارة الإدارة .
5. يحق لمدير البوابة تفويض صلاحياته لمن ينوب عنه، بعد موافقة إدارة الإدارة ويكون التفويض خطياً وموثقاً.
6. لمدير البوابة او من ينوب عنه الحق بإيقاف وإعاقة أي ارتباط من أي موقع يحتوي على مواد تخالف السياسة العامة لاستخدام البوابة.
7. مدير البوابة هو المسؤول عن منح الصلاحيات الدخول على البوابة. مرفق النموذج رقم 6.

ج- مديرو البوابة الفرعيون:

1. يُعينون من قبل وكلاء الجامعة، أو العمداء، أو مدراء الإدارات بقرارات إدارية.
2. يملأ النموذج الخاص بتقنية المعلومات بأسماء المدراء الفرعيين ويصادق عليه من مسؤول الجهة المباشر، ويمنح الصلاحيات بناء على هذا.
3. على كل إدارة تسمية أثنين من المدراء الفرعيين على الأقل.
4. تقتصر صلاحيات المدير الفرعي على إضافة/حذف/تعديل المحتوى الخاص بإداراته باللغات الرسمية المعتمدة (العربية والإنجليزية) وكذلك إنشاء الصفحات وإضافة الأخبار.
5. لا يحق للمدراء الفرعيين التغيير في تصميم الصفحات، ويتحملون المسؤولية في حال حصول ذلك.
6. يلتزم المدراء الفرعيون بحضور كافة الدورات التدريبية المقدمة من الإدارة.
7. في حال انتقال او استقالة أي مدير فرعي تبلغ الإدارة بشكل فوري لإيقاف صلاحيته على البوابة.
8. أمن اسم المستخدم وكلمة المرور لمدير فرعي هي من ضمن مسؤولياته.
9. عند إضافة اي روابط على البوابة فيجب ان لا تتعارض مع أهداف وسياسات البوابة أو تعرضها للخطر.
10. يمنع منعا باتا إنشاء أية روابط إلكترونية خاصة بالمدراء الفرعيين أو عرض أي منها في صفحات البوابة.
11. يخضع المدراء الفرعيون للمساءلة النظامية في حال انتهاكهم لما نصت عليه الوثيقة وتبطل صلاحياتهم.

د- المحتوى:

مرفق النموذج رقم (7)

1. على المدراء الفرعيين مسؤولية التأكد من أن يكون المحتوى ذا قيمة تخدم الجامعة والمجتمع المحلي والدولي.
2. يلتزم المدراء الفرعيين بعدم الإضافة او 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).
3. تعتبر الأخبار محتوى متغير تتحمل الإدارة مسؤولية إضافته، وأن تتحرى الدقة دائماً.
4. تعتبر الخطط الدراسية، ووصف المقررات، والخطط المستقبلية والمشاريع المقترحة محتوى متغير أيضاً، تتحمل الإدارة مسؤولية إضافته.
5. 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.
6. كل من يخالف هذه السياسة يعرض نفسه للمساءلة النظامية.

هـ- الصيانة والتشغيل:

1. تقوم وحدة الاصول بفحص التراخيص الخاصة بأنظمة تشغيل البوابة بشكل دوري، وإخطار الجهة المسؤولة عن الترخيص قبل انتهاء التراخيص بتسعة أشهر.
2. يقوم العميد أو المشرف على الإدارة بإخطار الجهات المسؤولة (وكيل الكلية أو الإدارة المالية أو الجهة المستفيدة) داخل الجامعة بمتطلبات تجديد الترخيص قبل ستة شهور من انتهاء الرخصة.
3. على الإدارات المختلفة وكافة المستخدمين ابلاغ إدارة تقنية المعلومات عن المشكلات التشغيلية او الوظيفية التي تواجههم عند استخدام البوابة، أو الاختراقات والحوادث الأمنية السيبرانية التي تتعرض لها البوابة.
4. على الإدارة نقل المعرفة من الشركات المشغلة للبوابة إن وجدت إلى الجهات ذات العلاقة بالجامعة.
5. يجب اخذ موافقة مجلس الإدارة بالإجماع قبل اجراء تعديلات جوهرية على البوابة.

6. على الإدارة اعداد تقرير سنوي عن جودة عمل البوابة، يتضمن احصائيات تتعلق بالاستخدام والاستفادة من البوابة، عدد المواد الجديدة، مشاريع التطوير للبوابة، وكمية الأعطال ونسبة ما تم إصلاحه منها.. وغيره.

و- النشر على البوابة:

مرفق النموذج رقم (7)

1. تخضع كافة المواد المنشورة على بوابة الجامعة للسياسة العامة للنشر في الجامعة.
2. تخضع المواد المنشورة إلى تحديد عمر افتراضي للمادة المنشورة، بحيث تكون إما مادة دائمة الصلاحية أو محددة بوقت معين.
3. تخضع المواد المنشورة إلى تحديد مكان النشر المناسب، فقد تكون على الصفحة الرئيسة او في صفحات فرعية.
4. تحدد الجهة طالبة النشر الفئة المستهدفة من النشر بحيث يتم توجيه المادة المنشورة للفئات المستهدفة.

المادة (7) سياسة إدارة المشاريع

سياسات إدارة المشاريع:

سياسات إدارة المشاريع

1. يلتـزم مكتـب إدارة المشـاريع بإعـداد دراسـات جـدوى(Business Case) للمشـاريع قبـل عرضـها واعتمادها من ادارة الإدارة بمشاركة الراعي الرسمي(Business Sponsor).
2. يلزم اعتماد دراسة الجدوى من صاحب الصلاحية قبل البدء في المشروع، ثم تعيين مدير المشروع ومنحه الصلاحيات اللازمة للبدء في إعداد وثيقة ميثاق المشروع(Project Charter) واعتمادها من صاحب الصلاحية في الجهة الطالبة قبل البدء في إجراءات طرح المشروع.
3. يتم تحديد التكلفة التقديرية للمشاريع قبل طرح كراسة المواصفات
4. بمجرد تحديد نطاق عمل المشروع، يتم إنشاء لجنة إشرافية وأخرى فنية له للبدء في عمليات التخطيط للمشروع، واعتماد الخطط التنفيذية من صاحب الصلاحية.
5. تقوم اللجنة الإشرافية للمشروع باعتماد خطط إدارة الاتصالات والمخاطر والجودة الخاصة بالمشروع.
6. يلتزم مكتب إدارة المشاريع بالتنسيق الكامل مع مكتب/لجنة البنية المؤسسية (الجهة التي تقود عملية التحول الرقمي بالجامعة).
7. يلتزم المكتب أيضا بالاحترافية العالية في إدارة المشاريع باعتماد منهجية PMI لإدارة جميع مراحل المشروع من البداية حتى الإغلاق.
8. يتم إعداد قائمة معايير تحقيق الجودة المطلوبة وفقا لمتطلبات كفاءة المشاريع.
9. الالتـزام بتقـديم تقـارير دوريـة لسـير المشـروع تشـمل (الجـدول الزمنـي ونطـاق العمـل والميزانيـة والمخاطر).
10. وثائق قبول الأعمال المعتمدة من اللجنة الفنية، ضرورة قبل الشروع في عمليات الإغلاق لاي مرحلة او مخرج من مخرجات المشروع.
11. عمليات إغلاق المشاريع تتم بالتنسيق مع إدارة المشاريع وتقرها اللجنة الإشرافية لكل مشروع.
12. تم وضع مصفوفة، ومسارات، ونقاط، ومستويات التصعيد مع بداية التخطيط لكل مشروع للجوء اليها عند مواجهة المشاكل مع تحديد اتفاقية مستوى الخدمة وزمن الاستجابة قبل التصعيد.

13.تشـمل عمليـات الإغـلاق إعـداد خطـة انتقـال المشـروع إلـى مرحلـة التشـغيل (Operation Mode) وتسليمه للجهة الفنية مع إعداد خطة تدريب وتأهيل ونقل المعرفة.

14.في حال كان المشروع خارجياً:

- فإن المقاول يقوم بتعيين مدير للمشروع والتنصيص عليه فـي وثيقـة التأسـيس. وتبقـى لمكتـب إدارة المشاريع الصلاحيات في تعميد أو رفض مدير المشروع إذا كان لا يستجيب لمتطلبات المشروع.
- يضع مكتب إدارة المشاريع على ذمة المقاول نماذج خاصة بكل عمليات إدارة المشاريع من البدء إلى الإغلاق كما يتم تحديـد عـدد الاجتماعـات وتواريخهـا والتقـارير الدوريـة التـي يقـوم المقـاول بإرسـالها لمكتب إدارة المشاريع ضمن خطط المشروع.

المادة (8) الشبكات والأمن

الشبكات والأمن:

1. تتم التحديثات لجميع مكونات البنية التحتية للشبكة Switches, Routers, assess point, firewall, and etc. كل ما تتطلب الامر، أو أن وجد اصدار جديد.
2. تكون التحديثات مطابقة لإعدادات الموصى بها من قبل الشركة الأم ووحدة الأمن السيبراني.
3. لا تزيد الفترة بين التحديثات عن ستة أشهر أو توصيات الشركة.
4. تضمن الإدارة أفضل الممارسات التقنية في مجال الشبكات.
5. مراقبة الشبكة ومسحها لتأكد من عدم وجود ثغرات مرة كل شهر أو عند الطلب من إدارة الإدارة أو وحدة الأمن السيبراني.
6. يتم تأمين مواقع الموزعات، والمحولات وترقيمها وتوثيقها وفقا لمعايير الجودة.
7. يتم تحديث خريطة الشبكة كل شهرين، وتزويد وحدة التطوير بالإدارة بأحدث المخططات.
8. حجب مواقع الانترنت غير المتلائمة مع بيئة الجامعة، وسوف يتم حظر البروتوكولات الخاصة بالمواقع التالية:

- الإعلانات والإطارات المنبثقة.
- المواقع التي تحث على التعصب والعنف بكافة صوره.
- المواقع الخاصة بالمقامرة.
- المواقع التي تحتوي على مواقع إباحية أو تروج للمنوعات
- مواقع وبرامج التحميل السريع.
- مواقع الهاكرز أو التي تحتوي على مواد وأدوات اختراق.
- مواقع وبرامج التجسس.
- المواقع التي تقوم بإرسال بريد يحتوي على روابط الغش والاحتيال.

9. جميع الأجهزة الموجودة داخل شبكة الجامعة يجب أن تكون مضافة على المجال (نطاق الجامعة) ، أي جهاز لم يتم إضافته للمجال سوف يتم فصل الشبكة عنه.
10. توفير شبكة عالية الحماية للمستخدمين سواء كانت شبكات داخلية أو شبكات عمومية للمنافذ الأمنة فقط.
11. المراقبة وتدقيق حجم بيانات الشبكة وذلك لضمان المحافظة على جودة الاتصال.
12. الدخول للخدمة يجب أن يكون محمي من خلال وسائل التحكم بالاتصال مثل تطبيقات الويب وجدار الحماية. يتم تحديث برامج الحماية حال صدور التحديث، أو عند الطلب من إدارة الإدارة أو وحدة الأمن السيبراني.
13. يتم الاشراف على تركيب معدات الشبكة في مركز البيانات أو مواقع الجامعة من قبل وحدة الشبكات.
14. وضع وتفعيل خطط وانظمة إدارة الكوارث.

المادة (9) الشبكة الخصوصية الافتراضية VPN

الشبكة الخصوصية الافتراضية VPN:

1. يتم تقديم طلب الحصول على VPN من صاحب الصلاحية في الإدارة من خلال النموذج المعتمد.
   مرفق النموذج ملحق رقم 3
2. يخضع الطلب لمعيار الاستخدام المقبول والاستخدام الفعال.
3. صلاحية VPN الممنوحة تعتبر سرية للغاية ويقع على عاتق الأشخاص المخولين المصرح لهم من قبل الإدارة التأكد عدم مشاركة الخدمة مع أي شخص.
4. على الجهاز المتصل بـ VPN أن يكون مزود برنامج حماية للفيروسات.
5. يتم أيقاف حساب VPN إذا لم يتم استخدامه تسعون يوماً، وفي حال الرغبة في تجديد الحساب يجب إشعار الإدارة بمدة لا تقل عن ثلاثون يوماً قبل انتهاء صلاحية الحساب.
6. يتم قطع خدمة VPN بعد ثلاثون دقيقة من الخمول في الاستخدام.
7. أي نشاط مشبوه يؤدي إلى انقطاع الخدمة والمسالة النظامية.

المادة (10) قواعد البيانات والنسخ الاحتياطي والخوادم

قواعد البيانات والنسخ الاحتياطي والخوادم:

راجع سياسة التخزين والاستبقاء الفقرة رقم (8) و (9).

1. الإدارة مسؤولة عن اعمال الصيانة والدعم لقواعد البيانات.
2. يجب تجنب عملية النسخ الاحتياطي اليدوية التي تعتمد على المستخدم النهائي. وأن تتم العملية بشكل تلقائي.
3. تحدد مدة الاحتفاظ بالنسخ بناء على أهمية النظام، على ألا تقل الفترة عن ثلاثة شهور.
4. يجب الاحتفاظ بنسخ سنوية او نصف سنوية.
5. يجب أن تشفر ملفات النسخ الاحتياطية بمفتاح تشفير لا يقل عن 256bit.
6. يجب استخدام التخزين السحابي أن وجد بأقصى حدوده، لتوفير المساحات، وتفعيل إدارة الكوارث.
7. يتم تحديد جدول النسخ الاحتياطي اليومي، الاسبوعي، الشهري، السنوي حسب أولوية وحساسية الانظمة وتخطر إدارة الإدارة بذلك.
8. يتم اتباع السياسات الموصى بها من مايكروسوفت بما يخص Active Directory، وفق اخر اصدار، وبما يشمل جميع الخواص Centralized management, resource, Exchange, Domain-based, (Group Policy, ... etc.).
9. يتم اتباع السياسات الموصى بها من مايكروسوفت بما يخص DNS، وفق اخر اصدار.
10. تكون خدمة الاستضافة بالمشاركة في مركز البيانات المتواجد داخل حرم الجامعة الرئيس، بعد الحصول على موافقة إدارة التقنية.
11. طالب خدمة الاستضافة بالمشاركة علية تقديم الطلب حسب النموذج الخاص بذلك مع كتابة أسباب مقنعة لطلبه وتوضيح مواصفات الخادم ،وتحتفظ الإدارة بحق رفض الطلب.
12. تضمن وحدة الخوادم وقواعد البيانات الاستخدام الامثل للخوادم، كما تضمن تحديثها وصيانتها بشكل دوري.

13. توقف خدمة الاستضافة في حال مخالفة السياسات، أو عدم وجود نشاط فعال لمدة ستة أشهر على سيرفر الاستضافة.
14. جميع بيانات النسخ الاحتياطي، وملكية الانظمة والبرمجيات، والاحتفاظ بالبيانات، والاحتفاظ بالنسخ، واسترجاع البيانات، ووصف المدة الزمنية للاحتفاظ بالبيانات، والنسخ الاحتياطية من البرمجيات يجب أن تكون موضحة بشكل تفصيلي.
15. استرجاع البيانات من النسخ الاحتياطية يتم بعد:
    - الاختراقات والهجمات السيبرانية.
    - تلف أو حذف أو تعديل الملفات.
    - عندما تطلب النسخ الاحتياطية المؤرشفة.
    - عند طلب البرمجيات والانظمة على ان يتم من خلال نظام أدعمني وبموافقة إدارة الإدارة.
    - عند تعطل أجهزة الخوادم (Hardware, Software)

المادة (11) سياسة أمن تقنية المعلومات

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

أ- الأمن المادي:

1. بالنسبة لجميع الخوادم وأجهزة الشبكة وأصول الشبكة الأخرى، يجب تراعى معدات السلامة في اماكن تواجدها، وتكون منطقة تواجدها ذات تهوية مناسبة ووصول متاح لموظفي الإدارة، وأن تراعى التدابير الأمنية مثل لوحة المفاتيح والقفل وما إلى ذلك.
2. 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 الإدارة 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 أو الضياع والأعطال التي قد تتعرض لها الاجهزة).
3. مسؤولية أمن وسلامة الاجهزة الشخصية (جهاز مكتبي، جهاز محمول، أيباد، وخلافه) تقع على عاتق مستلمها.
4. في حال الاضرار والمتعمد سوف تطلب الإدارة التعويض المادي، والمسائلة القانونية لمسبب الضرر.

ب- أمن المعلومات:

راجع ملحق سياسة حماية البيانات الشخصية المادة الخامسة الفقرة رقم (10) - راجع سياسة التخزين والاستبقاء الفقرة رقم (9).

1. تتولى وحدة إدارة البنية التحتية إجراء النسخ الاحتياطي لجميع بيانات الجامعة سواء الحساسة أو القيمة أو الحرجة، وتوفير قائمة مرجعية لإدارة الإدارة لجميع البيانات التي تم نسخها.
2. القائمة المرجعية تشمل بيانات تفصيلية عن (الفترات بين النسخ، مكان حفظها داخل الجامعة أو خارجها أو على السحابة، درجة اهميتها،).
3. تقع على عاتق إدارة البنية التحتية تثبيت وتحديث برنامج مكافحة فيروسات في جميع المعدات التقنية التي لها اتصال بالإنترنت.

4. جميع المعلومات المستخدمة في الإدارة تلتزم بقوانين الخصوصية ومتطلبات السرية الخاصة بالإدارة. الرجوع إلى سياسة السرية.

ج- الوصول إلى التقنية:

1. كل شخص من منسوبي الجامعة يحمل رمز تعريف فريد للوصول إلى الخدمات التقنية للإدارة، ويكون تعيين كلمة مرور مسؤولية الشخصية. (راجع ملحق سياسية حماية البيانات الشخصية المادة الخامسة الفقرة رقم (7) والفقرة رقم (10) ورقم (11)).
2. يتم اتباع سياسات كلمة المرور عند تعينها. راجع سياسة تعيين كلمة المرور.
3. تقع على عاتق إدارة البنية التحتية مسؤولية إصدار رمز التعريف وكلمة المرور الأولية لجميع منسوبي الجامعة. (راجع ملحق سياسية حماية البيانات الشخصية المادة الخامسة الفقرة رقم (7)).

المادة (12) إدارة الأصول

تهدف السياسة إلى وضع الإجراءات والمنهجيات لإدارة الأصول التقنية.

إدارة الأصول:

1. أن كل المعدات التقنية والبرمجيات والمعلومات والخدمات هي أصول تقنية للإدارة.
2. إدارة، وتوثيق، وصيانة الأصول التقنية مسؤولية إدارة تقنية المعلومات.
3. تتولى الإدارة توفير نظام أمن لإدارة الأصول.
4. نظام إدارة الأصول يجب أن يحتوي على البيانات التفصيلية والتعريفية للأصول، ووصفها، ومكانها، وتصنيفها، وقيمتها، وترقيمها، ومالكها.
5. المعلومات الموجودة في قاعدة الاصول هي معلومات ذات سرية عالية. يجب عدم تسليمها أو الافصاح عنها للجهات الخارجية أو الشركات الا بموافقة الإدارة.
6. تتولى إدارة الأصول جميع اتفاقيات الخدمة، وتوثيق الصيانة والتراخيص.
7. تلتزم إدارة الاصول بجميع سياسات إدارة تقنية المعلومات، وتقوم بتنسيق مع جميع وحدات الإدارة.
8. تفعيل إجراءات وعمليات إدارة الأصول .

المادة (13) إدارة الحوادث الأمنية واستمرارية العمل

توفر هذه السياسة إرشادات لإدارة الطوارئ لجميع المعدات والتقنيات داخل الإدارة.

إدارة الحوادث الأمنية واستمرارية العمل:

1. تتولى كل وحدة داخل الإدارة وضع خطة طوارئ في حال حدوث فشل لجميع أو لاحد الأنظمة او الخدمات المقدمة، سوى في معداتها أو برمجيتها.
2. تزود الإدارة بالخطة من تاريخ اقرار السياسة وتحدث بشكل سنوي على الاقل.
3. تشمل الخطة معلومات التواصل التفصيلية للأشخاص او الشركات (معلومات الاتصال للمعنيين عن كل خدمة سواء كانوا جهات داخلية او خارجية).
4. تشمل الخطة الوصف التفصيلي للإجراءات المتخذة ومدة الاستجابة المتوقعة.
5. تقع على عاتق كل وحدة اختبار خطة الطوارئ بشكل دوري، وتقديم تقرير مفصل حول جدواها.
6. تشمل الخطة الية التبليغ الفوري عن الاخطار، واجراءات التصعيد.

المادة (14) سياسة إدارة واستخدام الأنظمة

أن نجاح إدارة تقنية المعلومات يعتمد بشكل اساسي على الالتزام بالتشريعات المشار اليها في وثيقة السياسات لتقنية المعلومات، وعلى سرية المعلومات غير المعلنة، ويشمل ذلك بيانات الدخول وقواعد البيانات والمعلومات الخاصة بالبحث والتطوير والإنتاج والتسويق وإدارة الانظمة واستخدامها والمجالات الاخرى. وحرصاً من إدارة تقنية المعلومات على تنظيم العلاقة بين (وكالات وكليات وعمادات وادارات) الجامعة من جهة وبين إدارة تقنية المعلومات، فقد تم تحديد سياسة إدارة واستخدام أنظمة المعلومات في جامعة الحدود الشمالية وفقاً لما يلي:

سياسة إدارة واستخدام الأنظمة:

1. على مالك النظام أن يلتزم بسياسة الاستخدام المقبول والفعال والمشار اليها في فقرة السياسات العامة للأنظمة المدارة من قبله.
2. تخضع كافة أنظمة المعلومات لسياسة النسخ الاحتياطي المتبعة في إدارة تقنية المعلومات وحسب سياسة النسخ الاحتياطي المشارة اليها في المادة (12). (راجع سياسة التخزين والاستبقاء الفقرة رقم (8) و (9)).
3. تخضع كافة أنظمة المعلومات في الجامعة لسياسة أمن المعلومات كما ورد في المادة (9) من سياسات إدارة 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 النزاهة 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 السيبرانية أو تجاوز سعات التخزين وغيرها).
- استخدام أدوات مساعده Assistants Tools أخرى للتحقق من صحة البيانات المدخلة والتأكد من استكمال البيانات المدخلة ومعالجتها بالشكل الصحيح.

4. تخضع كافة أنظمة المعلومات لنظام صلاحيات الدخول والاستخدام حسب ما تقتضيه المصلحة بالتنسيق ما بين الجهة المستفيدة وإدارة تقنية المعلومات وضمن الضوابط التالية:

a. لا يتم منح صلاحية دخول واستخدام لأي نظام معلومات الا بموجب طلب رسمي موقع من الرئيس المباشر في الجهة المستفيدة وبعد موافقة عميد تقنية المعلومات.

b. تخصص نماذج خاصة لطلب صلاحيات الدخول والاستخدام ويشمل نموذج المعلومات التالية:

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، ادخال، انشاء ، انشاء صفحات، صلاحيات تعديل كود، وخلافه).
7. مصادقة من المسؤول المباشر على طلب الصلاحية.

a. تعتبر اي صلاحية ممنوحة دون استيفاء نموذج انشاء الصلاحية ومراحله الإجرائية ومصادق عليه صلاحيه غير نظامية، ويتحمل المسؤولية القانونية كل من يستخدم النظام دون موافقة رسمية.

b. يمنع التواصل المباشر من الجهة المستفيدة مع موظفي إدارة تقنية المعلومات المسؤولين عن انشاء الصلاحيات أو إدارتها أو قواعد البيانات، وأي تواصل بغير القنوات الرسمية يعتبر مخالفة نظامية ومحاولة للالتفاف على التعليمات

c. أي طلب للتغيير على إجراءات سير عمل النظام او أي إضافة خصائص جديدة للنظام أو تعديلها أو حذفها، يجب ان تتم بطلب خطي من مالك النظام وبإشراف إدارة تقنية المعلومات.

d. يحتفظ مالك النظام بسجل طلبات الدخول ويتم مراجعته كل ثلاثة شهور بالتنسيق مع إدارة تقنية المعلومات.

e. إذا حدث تغير مفاجئ على النظام، مثل تغير موقع استضافة النظام أو تغير مشغل النظام فإنه يتوجب مراجعه سجل الصلاحيات فوراً للقيام بالإجراءات الاحترازية لضمان عدم دخول غير المخولين للنظام.

f. يجب على مالك النظام الاحتفاظ بما يلي:

f. يجب على مالك النظام الاحتفاظ بما يلي:

- سجلات الدخول والخروج الناجحة والفاشلة.
- إعادة تشغيل وإيقاف تشغيل النظام الناجح والفاشل.
- تغيرات سياسات الأمان الناجحة والفاشلة.
- إدارة المستخدم والمجموعة الناجحة والفاشلة.
- الدخول إلى الملفات الناجح والفاشل.
- استخدام حقوق المستخدم الناجح والفاشل.

5. يحق لإدارة تقنية المعلومات طلب تقرير من مالك النظام يوضح السلوك غير الطبيعي للنظام، وعلى مالكه تسليم التقرير بمدة لا تتجاوز 24 ساعة من تاريخ طلبه، ويشمل السلوك غير الطبيعي لنظام كل من:

- الحمل الزائد على النظام.
- زيادة عدد العمليات قيد التشغيل.
- الزيادة المفاجئة لاستخدام وحدة المعالجة المركزية.
- خلق اتصالات غير عادية أو قطعها.
- انذارات من الجدران النارية.
- محاولات الدخول المتكررة.
- الدخول عبر منافذ غير اعتيادية.

6. تحتفظ إدارة تقنية المعلومات بكل من السجلات التالية:

- سجلات كشف التسلل إلى النظام.
- سجلات الجدار الناري.
- سجلات حساب المستخدم.
- سجلات مسح الشبكة.
- سجلات أمان التطبيق.
- سجلات الأمان.

7. تلتزم إدارة تقنية المعلومات برفع تقرير سنوي الى مالك النظام حيال وضع النظام من حيث الحسابات النشطة والصلاحيات الممنوحة لها، طلبات التغير على إجراءات سير عمل النظام وكل ما يستجد من اجراءات قد تقع عليه، على ان تقوم الجهة المالكة للنظام بالرد على اي ملاحظة حيال التقرير خلال سبعة ايام عمل من تاريخ ارساله. وفي حال عدم الرد تعتبر موافقة الجهة المالكة لكل ما ورد فيه.
8. تطبق السياسات على كافة الأنظمة التي يتم إنشاؤها داخل إدارة تقنية المعلومات ايضا.
9. يقوم مالك النظام بتعبئة المعلومات العامة عن النظام والبيانات الاحصائية باللغة العربية واللغة الانجليزية على نظام حصر الخدمات، انسجاماً مع بنود الخطة الاستراتيجية، وتحقيق لمتطلبات هيئة الحكومة الرقمية.

سياسة حماية البيانات الشخصية

1. اعتماد وضبط الوثيقة

1.1 اعتماد الوثيقة

الإعداد والمراجعة			
الاسم	المسمى الوظيفي	الدور	التوقيع / التاريخ
المصادقة والاعتماد			
الاسم	المسمى الوظيفي	الدور	التوقيع / التاريخ

1.2 الاصدارات

الإصدار والتاريخ	أعده وراجعه	اعتمده	التغيير

1. المادة الأولى: الغرض والنطاق

تهدف هذه السياسة إلى الحرص على أن تكون الجامعة ملتزمة بالتشريعات والضوابط المتعلقة بحماية البيانات الشخصية الصادرة من الجهات المختصة، وعلى أن يكون التعامل مع البيانات الشخصية داخل الجامعة منضبطا مع تلك التشريعات والضوابط بما يضمن حماية خصوصية الأفراد أصحاب البيانات وتوفير حقوقهم المكفولة لهم. كما تهدف هذه السياسة إلى تنظيم عملية جمع البيانات الشخصية ومعالجتها ومشاركتها والحفاظ عليها . وتنطبق أحكام هذه السياسة على جميع منسوبي الجامعة، الذين يقومون كليا أو جزئيا بمعالجة البيانات الشخصية. ويلتزم جميع منسوبي الجامعة بهذه السياسة بمن فيهم الأطراف الخارجية التي تتعامل مع البيانات التي تملكها الجامعة وأي مخالفة لهذه السياسة يترتب عليها تطبيق الأنظمة واللوائح المتعلقة بذلك.

2. المادة الثانية: التعريف بالمصطلحات العامة:

- **البيانات الشخصية:** كل بيان مهما كان مصدره أو شكله من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعله قابلا للتعرف عليه بصفة مباشرة أو غير مباشرة عند دمجه مع بيانات أخرى، ويشمل ذلك - على سبيل المثال ال الحصر الاسم ، وأرقام الهويات الشخصية، والعناوين وأرقام الحسابات البنكية والبطاقات الائتمانية، أو صور المستخدم الثابتة أو المتحركة، والأرقام الوظيفية والأرقام الجامعية، وغير ذلك من البيانات ذات الطابع الشخصي.
- **معالجة البيانات الشخصية:** جميع العمليات التي تجرى على البيانات الشخصية بأي وسيلة كانت يدوية أو آلية، وتشمل هذه العمليات - على سبيل المثال - جمع البيانات ونقلها وحفظها وتخزينها ومشاركتها وإتلافها وتحليلها واست خراج أنماطها والاستنتاج منها وربطها مع بيانات أخرى.
- **الإفصاح عن البيانات الشخصية:** تمكين أي شخص عدا جهة التحكم بالجامعة من الحصول على البيانات الشخصية أو استعمالها أو الاطلاع عليها بأي وسيلة ولأي غرض.
- **إشعار الخصوصية:** إشعار خارجي موجه للأفراد يوضح محتوى البيانات الشخصية، ووسائل جمعها والغرض من معالجتها، وكيفية استخدامها، والجهات التي سيتم مشاركة هذه البيانات معها وفترة الاحتفاظ بها وآلية التخلص منها.

- **الموافقة الصريحة**: موافقة مكتوبة أو إلكترونية تكون صريحة ومحددة وصادرة بإرادة حرة ومطلقة من صاحب البيانات تدل على قبوله لمعالجة بياناته الشخصية.
- **الموافقة الضمنية:** موافقة لا يتم منحها صراحة من قبل صاحب ت ضمنياً عن طريق أفعال الشخص ووقائع وظروف البيانات، ولكنها منح الموقف، كتوقيع العقود أو الموافقة على الشروط والأحكام.

3. المادة الثالثة : مبادئ حماية البيانات الشخصية:

عند التعامل مع البيانات الشخصية يجب مراعاة المبادئ التالية:

والتي حددتها السياسات المعتمدة من الجهات التنظيمية وعلى مكتب إدارة البيانات التأكد من الالتزام بهذه المبادئ:

1. **المسؤولية:** يقوم مكتب إدارة البيانات بتحديد وتوثيق سياسات وإجراءات الخصوصية الخاصة بالجامعة واعتمادها من قبل رئيس الجامعة أو من يفوضه، ونشرها إلى جميع من تنطبق عليه
2. **الشفافية:** يقوم مكتب إدارة البيانات بالتنسيق مع الجهات المختصة بإعداد إشعار عن سياسات وإجراءات الخصوصية الخاصة بالجامعة، يحدد فيه الأغراض التي من أجلها تمت معالجة البيانات الشخصية وذلك بصورة محددة وواضحة وصريحة
3. **الاختيار والموافقة:** يتم تحديد جميع الخيارات المتاحة لصاحب البيانات الشخصية والحصول على موافقته الضمنية أو الصريحة فيما يتعلق بجمع بيانات واستخدامها أو الإفصاح عنها.
4. **الحد من جمع البيانات:** يقتصر جمع البيانات الشخصية على الحد الأدنى من البيانات الذي يمكن من تحقيق الأغراض المحددة في إشعار الخصوصية .
5. **الحد من استخدام البيانات والاحتفاظ بها والتخلص منها:** تقتصر معالجة البيانات الشخصية على الأغراض المحددة في إشعار الخصوصية والتي من أجلها قدم صاحب البيانات موافقته الضمنية أو الصريحة، ويتم تقييد الاحتفاظ بها طالما كان ذلك ضروريا لتحقيق الأغراض المحددة أولما تقتضيه الأنظمة واللوائح والسياسات المعمول بها في المملكة وإتلافها بطريقة آمنة تمنع التسرب، أو الفقدان، أو الاختلاس أو إساءة الاستخدام، أو الوصول غير المصرح.

4. المادة الرابعة : حقوق صاحب البيانات:

1. يتمتع صاحب البيانات بحقوق تتعلق ببياناته الشخصية والطريقة التي تتعامل بها الجامعة مع هذه البيانات، ويجب الحرص على الالتزام بتوفير هذه الحقوق لصاحب البيانات
2. الحق في العلم ويشمل ذلك إشعار صاحب البيانات بالأساس النظامي أو الاحتياج الفعلي لجمع بياناته الشخصية، والغرض من ذلك، وألا تعالج بياناته الحقا بصورة تتنافى مع الغرض الذي جمعت من أجله والذي وافق عليه مسبقا سواء كانت الموافقة صريحة أو ضمنية .
3. لصاحب البيانات الحق في الرجوع عن موافقته على معالجة بياناته الشخصية - في أي وقت - مالم تكن هناك أغراض مشروعة تتطلب عكس ذلك.
4. الحق في الوصول إلى بياناته الشخصية لصاحب البيانات الحق في الوصول إلى بياناته الشخصية لدى الجامعة، وذلك للاطلاع عليها، وطلب تصحيحها، أو إتمامها، أو تحديثها، والحصول على نسخة منها بصيغة واضحة.

5. المادة الخامسة: السياسة:

1. **المسؤولية:** يكون مكتب إدارة البيانات مسؤولا عن إعداد وتطبيق السياسات والإجراءات المتعلقة بحماية البيانات الشخصية، ويكون رئيس الجامعة أو من يفوضه - مسؤولا عن الموافقة عليها واعتماده.
2. **تقييم المخاطر :** يتم تقييم المخاطر والآثار المحتملة لأنشطة معالجة البيانات الشخصية وعرض نتائج التقييم على رئيس الجامعة أو من يفوضه - لتحديد مستوى قبول المخاطر وإقرارها.
3. **تحديث ومراجعة العقود:** يقوم المركز - بعد التنسيق مع الجهات ذات العلاقة - بمراجعة وتحديث العقود واتفاقيات مستوى الخدمة والتشغيل بما يتوافق مع سياسات وإجراءات الخصوصية المعتمدة داخل الجامعة.
4. **الانتهاكات:** يتم اعداد وتوثيق الإجراءات اللازمة لإدارة ومعالجة انتهاكات الخصوصية وتحديد المهام والمسؤوليات المتعلقة بفريق العمل المختص، والحالات التي يتم بها إشعار الجهة التنظيمية والمكتب حسب التسلسل الإداري - بناءً على قياس شدة الأثر.

5. **تعزيز الوعي:** يقوم مكتب إدارة البيانات وبعد التنسيق مع الجهات ذات الاختصاص بإعداد برامج توعوية لتعزيز ثقافة الخصوصية ورفع مستوى الوعي وفقا لسياسات وإجراءات الخصوصية المعتمدة من الإدارة العليا للجامعة

6. **الشفافية:**

a. يتم إشعار صاحب البيانات بطريقة ملائمة وقت جمع البيانات بالغرض والأساس النظامي والاحتياج الفعلي والوسائل والطرق المستخدمة لجمع ومعالجة ومشاركة البيانات الشخصية وكذلك التدابير الأمنية لضمان حماية الخصوصية حسب الأنظمة واللوائح والسياسات المعمول بها في المملكة .
b. يتم إشعار صاحب البيانات عن المصادر الأخرى التي يتم استخدامها في حال تم جمع بيانات إضافية بطريقة غير مباشرة من جهات أخرى .

7. **الاختيار والموافقة:**

1. يتم تزويد صاحب البيانات بالخيارات المتاحة فيما يتعلق بمعالجة البيانات الشخصية والآلية المستخدمة لممارسة هذه الخيارات.
2. يتم أخذ موافقة صاحب البيانات على معالجة البيانات الشخصية بعد تحديد نوع الموافقة صريحة أو ضمنية بناء على طبيعة البيانات وطرق جمعها.

8. **الحد من جمع البيانات واستخدامها:**

1. يكون الغرض من جمع البيانات متوافقا مع الأنظمة والسياسات واللوائح المعمول بها في المملكة وذا عالقة مباشرة بنشاط الجامعة
2. يكون محتوى البيانات مقتصرا على الحد الأدنى من البيانات اللازمة لتحقيق الغرض من جمعها
3. يتم تقييد جمع البيانات على المحتوى المعد سلفا الموضح في النقطة السابقة ويكون بطريقة عادلة ومباشرة وواضحة وآمنة وخالية من أساليب الخداع أو التضليل
4. يقتصر استخدام البيانات على الغرض الذي جمعت من أجله.

9. **الاحتفاظ بالبيانات والتخلص منها :**

1. يقوم مكتب إدارة البيانات بإعداد وتوثيق سياسة وإجراءات الاحتفاظ بالبيانات وفقا للأغراض المحددة والأنظمة والتشريعات ذات العلاقة.

2. تقوم الجامعة بتخزين البيانات الشخصية ومعالجتها داخل الحدود الجغرافية للمملكة، ولا تجوز معالجتها خارج المملكة إلا بعد حصول الجامعة على موافقة كتابية من الجهة التنظيمية، بعد تنسيق الجهة التنظيمية مع المكتب
3. يقوم المركز بالتنسيق مع الجهات ذات العلاقة بإعداد وتوثيق سياسة وإجراءات التخلص من البيانات التالفة بطريقة آمنة تمنع فقدانها أو إساءة استخدامها أو الوصول غير المصرح به إليها وتشمل البيانات التشغيلية المؤرشفة، والنسخ الاحتياطية وذلك وفقا لما يصدر من الهيئة الوطنية للأمن السيبراني
4. تقوم الجامعة بتضمين أحكام سياستي الاحتفاظ والتخلص من البيانات في العقود في حال إسناد هذه المهام إلى جهات معالجة أخرى.

10. الوصول إلى البيانات:

1. يقوم مكتب إدارة البيانات - بعد التنسيق مع الجهات ذات العلاقة بتحديد وتوفير الوسائل التي عن طريقها يمكن لصاحب البيانات الوصول إلى بياناته الشخصية وذلك لمراجعتها وتحديثها.
2. يقوم المركز - بعد التنسيق مع الجهات ذات العلاقة بالتحقق من هوية الأفراد قبل منحهم الوصول إلى بياناتهم الشخصية وفقا للضوابط المعتمدة من قبل الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.

11. مشاركة البيانات مع جهات أخرى

1. يحظر مشاركة البيانات الشخصية مع جهات أخرى إلا وفقا للأغراض المحددة بعد موافقة صاحب البيانات ووفقا للأنظمة واللوائح والسياسات، تزُودّ الجهات الأخرى بسياسات وإجراءات الخصوصية المتبعة على أن يتم تضمينها في العقود والاتفاقيات .
2. يتم إشعار أصحاب البيانات وتؤخذ الموافقة منهم في حال مشاركة البيانات مع جهات أخرى لاستخدامها في غير الأغراض المحددة . يقوم مكتب إدارة البيانات بأخذ موافقة مكتب إدارة البيانات الوطنية – NDMO بعد التنسيق مع الجهة التنظيمية - قبل مشاركة البيانات الشخصية مع جهات أخرى خارج المملكة .

12. جودة البيانات وحمايتها

1. يقوم مكتب إدارة البيانات بالتنسيق مع الجهات ذات العلاقة بإعداد وتوثيق الإجراءات اللازمة لضمان دقة البيانات الشخصية واكتمالها وحداثتها وارتباطها بالغرض الذي وضعت من أجله .
2. يتم استخدام الضوابط الإدارية والتدابير التقنية المعتمدة في سياسات الجامعة لأمن المعلومات لضمان حماية البيانات الشخصية ومنها على سبيل المثال لا الحصر:

- منح صلاحيات الوصول إلى البيانات وفقا لمهام العاملين ومسؤولياتهم لتجنب تداخل الاختصاص وتلافي تشتيت المسؤوليات .
- تطبيق الإجراءات الإدارية والتدابير التقنية التي توثق مراحل معالجة البيانات وتوفر إمكانية تحديد المستخدم المسؤول عن كل مرحلة من هذه المراحل (سجلات الاستخدام).
- توقيع العاملين الذين يباشرون عمليات معالجة البيانات على تعهد للمحافظة على البيانات وعدم الإفصاح عنها إلا وفقا للسياسات والإجراءات والأنظمة والتشريعات .
- اختيار العاملين الذين يباشرون عمليات معالجة البيانات ممن يتصفون بالأمانة والمسؤولية ووفقا لطبيعة وحساسية البيانات وسياسة الوصول المعتمدة من الجامعة .
- استخدم التدابير الأمنية المناسبة - كالتشفير - لأمن البيانات الشخصية وحمايتها بما يتناسب مع طبيعتها وحساسيتها والوسائط المستخدمة لنقلها وتخزينها وفقا لما يصدر من الهيئة الوطنية لألمن السيبراني والجهات ذات الاختصاص.
- يكون مكتب إدارة البيانات مسؤولا عن مراقبة الامتثال لسياسات وإجراءات الخصوصية بشكل دوري ويتم عرضها على رئيس الجامعة أو من يفوضه - كما يتم تحديد وتوثيق الإجراءات التصحيحية التي سيتم اتخاذها في حال عدم الامتثال وإشعار الجهة التنظيمية والمكتب حسب التسلسل التنظيمي.

6. المادة السادسة: أحكام عامة:

- يجب إبلاغ الجهات التنظيمية فورا ودون تأخير وبما ال يتجاوز ٧٢ ساعة من وقوع أو اكتشاف أي حادثة تسريب للبيانات الشخصية وفقا لآليات والإجراءات التي تحددها الجهات التنظيمية.
- يجب على الجامعة عند تعاقدها مع جهات المعالجة أن تتحقق بشكل دوري من امتثال جهات المعالجة لهذه السياسة وفقا لآليات والإجراءات التي تحددها الجهات التنظيمية، على أن يشمل ذلك أي تعاقدات الحقة تقوم بها جهات المعالجة.

سياسة التخزين والاستبقاء

1. اعتماد وضبط الوثيقة

1.1 اعتماد الوثيقة

الإعداد والمراجعة			
الاسم	المسمى الوظيفي	الدور	التوقيع / التاريخ
المصادقة والاعتماد			
الاسم	المسمى الوظيفي	الدور	التوقيع / التاريخ

1.2 الاصدارات

الإصدار والتاريخ	أعده وراجعه	اعتمده	التغيير

2. المقدمة

تمثل البيانات التي تنتجها الجهات الحكومية أو تتلقاها أو تتعامل معها أصولا وطنية يمكن أن تساهم في تحسين الأداء والإنتاجية وتسهيل تقديم الخدمات العامة عن طريق دعم العمليات الفعالة لإدارة البيانات واتخاذ القرارات الإستراتيجية واستشراف المستقبل تحقيق أعلى مستويات المسؤولية والشفافية.

ولضمان الاستفادة القصوى من هذه البيانات التي تشكل جزءاً مهماً من الأصول الوطنية، فلابد من تعزيز مبادئ تعريف شروط التخزين وحماية البيانات في حالات الكوارث الطبيعية والتأكد من إمكانية استعادتها وتحديد فترات استبقاء البيانات بناء على نوعها ومستوى تصنيفها وقيمتها في الأعمال والمتطلبات القانونية.

3. الهدف

تهدف هذه السياسة إلى وضع القواعد الأساسية لإدارة عمليات البيانات من حيث التخزين والاستبقاء والتخلص منها والتي يجب اتباعها في الجامعة لضمان سلامة هذه العمليات واستدامة البيانات.

4. نطاق العمل

تنطبق سياسة التخزين والاستبقاء على كافة أنواع أجهزة تخزين البيانات بما في ذلك الأقراص الصلبة الداخلية والخارجية ووسائط التخزين المتصلة بشبكة التخزين ووسائط التخزين على الأشرطة ومحركات الذاكرة السريعة القابلة للإزالة وبيانات الأعمال على الهواتف النقالة وأجهزة المساعدة الرقمية الشخصية والأقراص المرنة والأقراص المدمجة وشبكة الإنترنت الداخلية والمواقع الإلكترونية وغيرها

5. التعريفات

الجامعة	جامعة الحدود الشمالية
مكتب إدارة البيانات	مكتب إدارة البيانات في الجامعة
لجنة إدارة وحوكمة البيانات	تمثل اللجنة كافة قطاعات الجامعة وتعمل على إدارة المبادرات المتعلقة بإدارة وحوكمة البيانات في الجامعة.
ممثل بيانات الأعمال	هو الموظف الذي يتم تعيينه من قبل الإدارة العليا في الجامعة والذي يمثل المرجعية النهائية بما يخص تطبيق سياسات وضوابط ومعايير إدارة البيانات في القطاع، ويقوم بتمثيل القطاع في لجان حوكمة البيانات والتأكد من قيام مختصي بيانات الأعمال ضمن القطاع بأعمال إدارة البيانات المطلوبة بما يتوافق مع سياسات ومعايير وضوابط إدارة البيانات، ومتابعة تنفيذ هذه الأعمال ضمن القطاع ومؤشرات الأداء الرئيسية المرتبطة بإدارة وحوكمة البيانات داخل القطاع.
مختص بيانات الأعمال	هو الموظف الذي يتم تعيينه من قبل الوحدات التنظيمية والأقسام داخل قطاعات الأعمال في الجامعة لتنفيذ الأعمال الخاصة بتطبيق سياسات وضوابط ومعايير البيانات داخل القطاع وتحديد وإدارة المشاكل والمخاطر المتعلقة بإدارة البيانات ورفعها الى ممثل بيانات الأعمال في القطاع.
أمين حفظ البيانات إدارة تقنية المعلومات	هو الموظف المسؤول عن إنشاء وإدارة قواعد البيانات الخاصة بأنظمة الجامعة وتخزين البيانات وضمان توفرها، وتطبيق ضوابط ومعايير السياسة على البيانات المخزنة في قواعد البيانات.
أمناء حفظ البيانات (مركز المعلومات)	هو الموظف المسؤول عن إنشاء وإدارة قواعد البيانات الخاصة بمنصة البيانات/ ذكاء الأعمال التابعة للجامعة، وتطبيق ضوابط ومعايير السياسة على البيانات في قواعد البيانات.
مستخدمي البيانات	هم جميع موظفي الجامعة الذين يقومون باستخدام البيانات والأنظمة للقيام بأعمالهم اليومية.
البيانات	مجموعة من الحقائق في صورتها الأولية أو في صورة غير منظمة مثل الأرقام أو الحروف أو الصور الثابتة أو الفيديو أو التسجيلات الصوتية أو الرموز التعبيرية.

5. التعريفات

البيانات الشخصية	كل بيان - مهما كان مصدره أو شكله - من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعله قابلاً للتعرف إليه بصفة مباشرة أو غير مباشرة عند دمجه مع بيانات أخرى، ويشمل ذلك - على سبيل المثال لا الحصر- الأسم، وأرقام الهويات الشخصية، والعناوين، وأرقام التواصل، وأرقام الحسابات البنكية، والبطاقات الائتمانية، وصور المستخدم الثابتة أو المتحركة، وغير ذلك من البيانات ذات الطابع الشخصي.
الوصول إلى البيانات	القدرة على الوصول للبيانات وقراءتها وتحميلها.
الجهة العامة	أي جهة حكومية أو جهة اعتبارية عامة مستقلة في المملكة، أو أي من الجهات التابعة لها، وتعد في حكم الجهة العامة أي شركة تقوم بإدارة المرافق العامة أو البنى التحتية الوطنية أو تشغيلها أو صيانتها، أو تقوم بمباشرة خدمة عامة فيما يخص إدارة تلك المرافق أو البنى التحتية.
البيانات الحكومية	هي البيانات التي تنتجها الجهات الحكومية.

6. إدارة الوثيقة

يتولى مكتب إدارة البيانات في الجامعة مُلكيّة السياسة، وإصدار النسخ المحدثة منها.

تطبق السياسات المتعلقة بنظام إدارة الجودة والمدونة في سياسة ضبط التوثيق رقم (0000000000)

7. المهام والمسؤوليات

7.1 مكتب إدارة البيانات (مسؤول إدارة البيانات)

7.1.1 إعداد ونشر سياسة التخزين والاستبقاء.

7.1.2 تدقيق الامتثال لسياسة التخزين والاستبقاء وتقديم تقرير التدقيق مع التوصيات بمراجعة إجراءات التخلص من البيانات في نهاية فترة الأرشفة.

7.1 مكتب إدارة البيانات (مسؤول إدارة البيانات)

7.2.1. تخزين البيانات باستخدام الممارسات الرائدة والمعتمدة من قبل الجامعة التي تضمن سلامة وجودة البيانات.

7.2.2. تطبيق عملية الأرشفة الآلية.

7.2.3. تحديد قائمة مفصلة بطرق الإتلاف المعتمدة وإنفاذها لكل نوع من البيانات المؤرشفة سواء كانت على وسائط تخزين مادية مثل الأقراص الصلبة أو الأقراص المدمجة الرقمية أو أشرطة النسخ الاحتياطية أو محركات الأقراص الصلبة أو الأجهزة المحمولة أو محركات الأقراص المتنقلة أو في سجلات قواعد البيانات أو ملفات النسخ الاحتياطية.

7.2.4. تحديد فترة الاحتفاظ بكيانات البيانات الهامة وكيانات البيانات غير الهامة، المصنفة وفقا لسياسة تصنيف البيانات" ووفقا للأنظمة واللوائح المعمول بها في الجامعة.

8. المبادئ الأساسية للتخزين والاستبقاء

8.1 تحديد الغرض: من المهم تعريف شروط التخزين التي تضمن ، التخزين التي تضمن حماية للبيانات في حالات الكوارث.

8.2. المعرفة والاطلاع الاطلاع المستمر على آخر الممارسات الرائدة والمعتمدة لحلول تخزين البيانات.

8.3. المسؤولية تعتبر البيانات أصولا قيمة لذلك يجب ضمان تخزينها بشكل آمن وسهل.

9. الضوابط التخزين والاستبقاء

9.1. الاحتفاظ بالبيانات

9.1.1. يُعرف الاحتفاظ بأنه حفظ البيانات في بيئة إنتاج أو بيئة فعلية خلال فترة استخدامها النشطة" بحيث يمكن الوصول إليها من قبل المستخدم المصرح له في إطار أنشطته العادية.

9.1.2. ينبغي عدم الاحتفاظ بالبيانات المستخدمة في العمل المؤقت، أو التطوير أو الاختبار أو مسودات البيانات إلى ما بعد فترة استخدامها النشطة ولا ينبغي نسخها في بيئات الإنتاج أو البيئات الفعلية.

9.2. شروط التخزين التي تضمن حماية للبيانات في حالات الكوارث

9.2.1. يجب التأكد أن البيانات محمية بجدول نسخ احتياطي مناسب، ومن إمكانية استعادة البيانات من النسخ الاحتياطية.

9.3. فترات استبقاء البيانات بناء على نوع ومستوى تصنيفها وقيمتها في الأعمال والمتطلبات القانونية

9.3.1. يجب أن تحدد فترة الاحتفاظ لكل نوع من البيانات وفقا لما يلي:

9.3.2. بيانات دائمة الحفظ - بيانات حيوية وهي البيانات التي لا يمكن الاستغناء عنها ويجب توفرها دائما للقيام بأعمال الجامعة اليومية.

9.3.3. بيانات مؤقتة الحفظ - بيانات غير حيوية : وهي البيانات التي يتم استخدامها لفترة محددة ولا يوجد حاجة للرجوع إليها بعد فترة الاحتفاظ حيث من المقترح التخلص من البيانات المؤقتة بشكل ربع سنوي).

9.3.4. ينبغي عدم الاحتفاظ بالبيانات المستخدمة في العمل المؤقت أو التطوير أو الاختبار أو مسودات البيانات إلى ما بعد فترة استخدامها النشط ولا ينبغي نسخها في بيئات الإنتاج أو البيئات الفعلية.

9.4. أرشفة البيانات

9.4.1. يتم أرشفة البيانات وفق مستويات تصنيفها وبناء على سياسة النسخ الاحتياطي للبيانات واستردادها.

9.5. التخلص من البيانات

9.5.1. يُعرف التخلص من البيانات على أنه الإتلاف الفعلي أو الفني بصورة تجعل البيانات الموجودة على وسائط التخزين غير قابلة للاسترجاع من خلال الوسائل التقنية المتوفرة والمعتمدة.

9.5.2. ينبغي على الإدارة المعنية بالأرشفة والاحتفاظ بالبيانات تحديد قائمة مفصلة بطرق الإتلاف المعتمدة وإنفاذها لكل نوع من البيانات المؤرشفة سواء كانت على وسائط تخزين مادية مثل الأقراص الصلبة أو الأقراص المدمجة الرقمية أو أشرطة النسخ الاحتياطية أو محركات الأقراص الصلبة أو الأجهزة المحمولة أو محركات الأقراص المتنقلة أو في سجلات قواعد

10. التعامل مع حالات عدم الامتثال

في حال عدم الامتثال لضوابط السياسة مثل عدم الامتثال لضوابط التخلص من البيانات، يخضع موظفي الجامعة المعنيين للمساءلة حيث تقوم لجنة إدارة وحوكمة البيانات بتحديد الضرر الناجم عن عدم الامتثال ورفع النتائج إلى الإدارة القانونية لاتخاذ الإجراء النظامي المناسب.

11. التغييرات والاستثناءات

11.1. لا يوجد استثناءات مرتبطة بالسياسة.

11.2. يتم مراجعة السياسة وإصدار نسخ محدثة منها ومراجعة محتوياتها بشكل سنوي أو عند الحاجة أو عند استحداث تغيرات على الأولويات الاستراتيجية أو الهيكل الخاص بالجامعة.

12. الوثائق ذات الصلة

ترتبط السياسة بالوثائق التالية:

الرقم	الوثيقة	الوصف
١	إجراء التخزين والاستبقاء البيانات	وهي الوثيقة التي تبين سير عمل الاجراء المرتبط بسياسة التخزين والاستبقاء مع شرح للخطوات الرئيسية والأدوار المرتبطة بتنفيذ الإجراء.
٢	سياسة تصنيف البيانات	حيث تعتمد سياسة التخزين والاستبقاء على معرفة وتحديد مستوى تصنيف البيانات لتحديد مستوى مراقبتها وحمايتها.
٣	سياسة مشاركة البيانات	حيث تلتزم سياسة مشاركة البيانات على آليات التخزين المعتمدة عند تخزين البيانات بهدف تبادلها.
٤	ترتيب أولويات أنظمة البيانات	نموذج لترتيب أولويات أنظمة البيانات، بهدف استخدامه من قبل الوحدات التنظيمية المعنية في الجامعة لتوفير قائمة بأنظمة المعلومات ووضع ترتيب محدد لاسترجاع الأنظمة في خطة التعافي من الكوارث.
٥	تحديد السعة التخزينية المتوقعة للبيانات	نموذج لتحديد السعة التخزينية المتوقعة للبيانات، بهدف استخدامه من قبل الوحدات التنظيمية المعنية في الجامعة لتوفير معلومات عن السعات المستخدمة سابقا لحفظ البيانات في التطبيقات الرئيسية، تقييم لأداء التطبيقات، توقع الاحتياجات لسعة التخزين عة الحدود الشمالية.

ملحق رقم (3)

طلب الحصول على VPN

Section 1. Contact Information (NAME IN BLOCK LETTERS ONLY)	
College or Department or Company:	
User Full Name:	
Mobile:	Email:
Tel: Extension:	ITSM NO:
Date:	IQAMA ID:

Section 2.0 VPN – Network			
Create Account ☑	Activate Account ☑	Remove Account ☒	Change Password ☒
New ☑ Renewal ☒	Grant Permission ☒	Remarks: Banner Application Access	
Reason for Server Access in Detail Banner Application Access		Access period: From Date Access period: To Date _____	
Daily VPN Access Timings: _____		Risk Factor Risk ☒ No Risk ☑	

VPN-User IP	Destination IP : Application / Server	Ports :	Remarks
(DIT-Use only)			

☐ Requestor Department Dean / Vice Dean /Manager		
	Name	Signature
☐ Approval ☐ Reject		

Internal use – Deanship of Information Technology – Dean / Vice Dean Approval		
	Name	Signature
☐ Approval ☐ Reject		

Internal use – Deanship of Information Technology – Enginee		
	Name	Signature
☐ Approval ☐ Reject		

VPN Policy and Terms

1. Overview

A virtual Network (VPN) is a secured private network connection for NBU Networks over Internet. AVPN provided a secure encrypted connection or Tunnel over the Internet between and NBU Networks and other Network.

Use of VPN allows approved authorized users to securely access the NBU Network, anywhere from outside of NBU over Internet.

2. Definitions

Authorized Users: They are NBU Employee, Faculty, and contracted vendor company's employees.

3. VPN User Conditions

3.1 The Provided VPN network is highly confidential and it's the responsibility of approved and authorized users to ensure, no share of VPN services to anyone.

3.2 If one VPN account will be used by one user, then it must be informed prior to the application.

3.3 Authorized users must connect to VPN through their own machine only. Login through different machine may lead the hack of the Password for the user and it's also breach to the policy.

4. VPN Account Policy

4.1 The renewal request of VPN must come before 7 days of expiry.

4.2 The VPN Services provided are Deanship of IT Proprietary and the client / user using our services must have suitable application.

4.3 The User computer connected to VPN must have updated Anti-Virus.

4.4. The connection will be disconnected directly for authorized once the status is inactive.

4.5 Every authorized user will have specified privileges as per their need.

5. Enforcement

Above terms and conditions must be followed strictly by every user /client. Any violation will be treated as per Anti-Cyber Crime Law and the user will be responsible for the loss to NBU in case of any.

سياسات وشروط بالشبكة الخاصة الافتراضية

1. نبذة:

الشبكة الخاصة الافتراضية هي عبارة عن شبكة خاصة مؤمنة مثل شبكة الانترنت لتوفر اتصال آمن ومشفر عبر نفق خاص من خلال شبكة الأنترنت للاتصال بين شبكة جامعة الحدود الشمالية وغيرها من الشبكات الأخرى. إن استخدام الخاصة الافتراضية يسمح للأشخاص المخولين بالوصول من خارج شبكة الجامعة بشكل آمن.

2. تعريفات:

الأشخاص المخولين: هم الموظفين وأعضاء هيئة التدريس والشركات المتعاقدة مع الجامعة.

3. شروط الاستخدام:

1.الشبكة الخاصة الافتراضية الممنوحة تعتبر سرية للغاية ويقع على عاتق الأشخاص المخولين المصرح لهم من قبل إدارة تقنية المعلومات التأكد من أنه لا يسمح للأشخاص غير المصرح لهم المشاركة في خدمات الشبكة الخاصة الافتراضية.

2إذا الشبكة الخاصة الافتراضية ستستخدم من قبل أكثر من مستخدم يفترض ذكر هذا مسبقا في نموذج طلب الخدمة.

3يجب على الأشخاص المخولين بتوصيل جهاز الحاسب الآلي والاتصال بالشبكة الخاصة الافتراضية ومنع الأشخاص غير المخول لهم من الحصول على كلمة المرور الخاصة بهم أو الوصول واستخدام الحاسب الآلي أثناء عملية الاتصال.

4. سياسة حساب الشبكة الخاصة الافتراضية:

1في حال الحاجة لتجديد حساب الشبكة الافتراضية الخاصة يجب عليك تجديد الطلب قبل انتهاء المدة المحددة ب 7 أيام.

2خدمة الشبكة الخاصة الافتراضية مقدمة من قبل إدارة تقنية المعلومات ويفترض لاستخدام هذه الخدمة الحصول على البرنامج المستخدم في الإدارة لهذا الغرض.

3يجب أن تكون جميع الأجهزة المتصلة بالشبكة الجامعة من خلال الشبكة الخاصة الافتراضية مزودة ببرنامج كطافة للفيروسات.

4سيتم قطع الاتصال تلقائيا على الأشخاص المخولين بالدخول على الشبكة الخاصة الافتراضية في حال عدم نشاط الحساب.

5قد تخضع أجهزة الأشخاص المخولين لتقييد الوصول إلى شبكة الجامعة وفقا لاحتياجات العمل الخاصة بهم.

5. الجزاءات:

يجب التقيد بالشروط الموضحة أعلاه من قبل أي مستخدم للخدمة، وفي حال عدم التقيد بالشروط الموضحة اعلاه سوف يتم تطبيق نظام مكافحة الجرائم المعلوماتية

Name:			الاسم:
Job Title:			الوظيفة:
Signature:			التوقيع:
STAMP			

ملحق رقم (4)

نموذج طلب مشروع

تعليمات

1. الالتزام بتعبئة النموذج بدون التعديل عليه والتأكد من صحة البيانات.
2. إرفاق موافقة صاحب الصلاحية.
3. إرفاق المستندات الداعمة.
4. لن يتم النظر في الطلبات غير المكتملة.
5. تعبئة جدول الكميات والمواصفات باللغة العربية.
6. إرفاق النموذج ومو افقة صاحب الصلاحية وجميع المستندات الداعمة في نظام (برق) أو البريد الإلكتروني بنفس الصيغة.(Word)

1. المعلومات الأساسية عن الجهة

الجهة الطالبة	
البريد الإلكتروني لممثل الجهة	
رقم الجوال لممثل الجهة	
تاريخ الطلب	
اعتماد صاحب الصلاحية	إرفاق صورة من موافقة صاحب الصلاحية

2. معلومات عامة عن المشروع

اسم المشروع	
وصف المشروع	
مدة المشروع	
التكلفة التقديرية للمشروع	

3. دراسة الوضع الحالي

العنصر	الإيضاح
أهداف ومنافع المشروع	
مبررات المشروع	مثال: يلزم تنفي المشروع لأسباب تتعلق بالالتزام بضوابط .....
تقييم الوضع الراهن	
دراسة السعة	على سبيل المثال: الموارد البشرية الحالية بتقنية المعلومات الرخص الحالية من حيث العدد الخدمات الحالية من حيث العدد البنية التحتية من حيث نسبة الاستخدام، وغيرها من معلومات مرتبطة بالوضع الحالي.
دراسة الطلب	تقديم دراسة الطلب للمتطلبات التي تدعم البرنامج / المشروع. على سبيل المثال: الموارد المستقبلية التي تحتاجها الجهة من حيث العدد الرخص المستقبلية من حيث العدد الخدمات المستقبلية من حيث العدد.
هل المشروع ضمن أهداف الخطة الاستراتيجية للجامعة	إذا كانت الاجابة نعم يرجى تحديد الهدف الرئيسي والتفصيلي والرقم المرجعي.
هل المشروع ضمن مشاريع التحول الرقمي	إذا كانت الاجابة نعم يرجى تحديد المشروع والرقم المرجعي.
هل المشروع ضمن الخطة الاستراتيجية للجهة	إذا كانت الاجابة نعم يرجى تحديد المبادرة المشروع والرقم المرجعي.
دوافع المشروع	توضيح مساهمة تطبيق المشروع في دعم الاستراتيجية أو التعليمات والقرارات الخاصة بالجامعة (مثال: الرؤية، برنامج التحول الاهداف الاستراتيجية التعليمات والقرارات.
الفئة المستهدفة	

4. دراسة الحالة المستهدفة

العنصر	الإيضاح
المتطلبات الفنية للمشروع	مثال: يجب أن يمتلك مقدمو الخدمات المهارات المعرفية التالية:
نطاق العمل	في هذا البند يتم توضيح نطاق العمل الخاص بالمشروع والتفاصيل التي يجب مراعاتها عند تقديم الخدمة للمتعاقد. ويمكن إضافة ملف مرفق منفصل للمتطلبات المعقدة في التنسيق والإشارة بذلك في الملاحق"
جدول الكميات	يرجى تحديد البنود والوحدة والكمية لكل بند وذلك في ملف منفصل
مكان تنفيذ المشروع	مثال: يقع موقع المشروع في حي . في محافظة / مدينة ..... في منطقة بحسب الاحداثيات التالية (إن وجد).

ملحق رقم (5)

مركز البيانات DATA CENTER

Request/Permit#:

تصريح الدخول REQUEST ENTRY PERMIT

REQUEST DATE		تاريخ الطلب
Name		اسم
Occupation		المسمى الوظيفي
Iqama Number		رقم الهوية/ الاقامة
Mobile Number		رقم الهاتف المحمول
Company		شركة
Company Contact Number		رقم الاتصال بالشركة
Date and time of entry		تاريخ الدخول
Duration Date and time		تاريخ المدة

سبب الزيارة REASON OF VISIT

ACCESS PERMIT APPROVED BY:

Deanship Of Information Technology:	
SIGNATURE:	
APPROVED DATE:	

IQAMA COPY

نموذج طلب صلاحية على البوابة

الرقم:

التاريخ: / /

بيانات مقدم الطلب:

الاسم	
رقم السجل المدني	
الايميل	
رقم الجوال	
الجهة	
الموقع الفرعي المطلوب الصلاحية له	

إقرار:

أنا الموقع أدناه أقر وأتعهد بأنني قمت بالاطلاع وقراءة جميع بنود سياسة إدارة المحتوى وأن أية مخالفة لهذه السياسات تكون سبباً للرفض حسب الأنظمة المتبعة

توقيع طالب الخدمة:

اسم مسؤول الجهة: **التوقيع:**

سياسة إدارة المحتوى V1.0

1. اعتماد وضبط الوثيقة

1.1 اعتماد الوثيقة

الإعداد والمراجعة			
الاسم	المسمى الوظيفي	الدور	التوقيع / التاريخ
المصادقة والاعتماد			
الاسم	المسمى الوظيفي	الدور	التوقيع / التاريخ

1.2 الاصدارات

الإصدار والتاريخ	أعده وراجعه	اعتمده	التغيير

فهرس السياسة

الهدف:

من خلال هذه السياسة يتم وضع الشروط والمبادئ والقواعد وصلاحيات عمليات النشر وتنسيق الاستخدام الفعال لمحتوى البوابة الإلكترونية لجامعة الحدود الشمالية، والتي يجب اتباعها والالتزام بمتطلباتها في إعداد المواد التي يتم عرضها ونشرها على الموقع الإلكتروني.

تشتمل السياسة على ما يلي:

- المسؤوليات والصلاحيات
- المبادئ العامة.
- معايير نصوص المحتوى.
- معايير الصور.
- معايير الروابط.
- معايير المحتوى وسهولة البحث.
- معايير النشر.
- معايير التعليقات والمشاركة الإلكترونية

المسؤوليات والصلاحيات:

يلتزم فريق إدارة المحتوى في إدارة تقنية المعلومات عن النشر ومراجعة المحتوى وابداء الملاحظات بما يراه مناسباً يتوافق مع الظهور الإعلامي للجامعة ويحقق مستهدفاتها. وتلتزم الإدارات المعنية في الجامعة عن إنشاء المحتوى الإلكتروني كلاً فيما يخصه مع المتابعة المستمرة لتحديث محتواها عن طريق تحديد ضابط اتصال من كل إدارة في الجامعة للتأكد من جودة المحتوى المرسل "صحة المعلومات واعتمادها.....وغيرها" مع تزويد إدارة المحتوى بأي تحديث يطرأ على المحتوى المنشور في البوابة الرسمية للجامعة والاستجابة الفورية لمتطلبات فريق إدارة المحتوى.

المبادئ العامة:

- الاهتمام بجودة المادة المنشورة من حيث جمال الصياغة وترتيب الأفكار وسلاسة التعبير.
- أن يكون المحتوى غير مخالف لأنظمة المواقع أو أنظمة الدولة.
- عدم إضافة محتوى يتعرض لخصوصيات الآخرين.
- التأكد من صحة المحتوى وخلوه من الأخطاء اللغوية والإملائية.
- تنسيق المحتوى ليظهر بالشكل اللائق من حيث التناسق والترتيب والمظهر.
- ان لا يتعارض مع الدين أو أنظمة الحكومة أو السياسات المعتمدة والجامعة والدولة أو الجهات المشرفة على تقنية المعلومات.

معايير نصوص المحتوى

- يجب أن تشتمل بداية الصفحة على عنوان يجذب القارئ ويفهم من خلاله مضمون الموضوع.
- استخدام عناوين فرعية وعناوين رئيسية مع التمييز بينها.
- عدم الاكثار من استخدام انواع الخطوط المختلفة والاكتفاء باستخدام خط أو خطين على الأكثر.
- التأكد من صحة البيانات وخلوها من الأخطاء اللغوية والإملائية.
- أن تكون النصوص مختصرة في عرض الفكرة التي تتضمنها الصفحة.
- عدم وضع أكثر من موضوع في صفحة واحدة بقدر الإمكان.
- قم بالتلخيص ووضع النقاط الرئيسية للموضوع في البداية حتى لا تفوت الفرصة على المستخدم ولا يقرأ بالتفصيل.
- المستخدم يبحث عن المعلومة المهمة لاحتياجه ولا يريد قراءة كل حرف فساعده بإبراز المهم بعلامة، وضعه كعنوان، تعداد.

معايير الصور:

- الاهتمام بجودة الصورة وإخراجها الفني وتوفير عنصر الجذب فيها.
- ضبط مقاس وحجم الصورة على حسب المطلوب.
- أن تكون الصورة ملائمة للمحتوى ومعبرة عنه.
- وضع نص يوضح الصور التي تحتوي على أشكال بيانية أو رسوم توضيحية.
- عدم نشر صور تخالف الشريعة الإسلامية أو أنظمة الدولة أو يكون بها خدش للحياء.

معايير الروابط:

- جميع الروابط المدرجة في المحتوى تعمل بشكل صحيح وسليم.
- عدم الربط بمواقع مجهولة المصدر ويجب ان تكون الروابط حكومية أو معتمدة.
- عدم إضافة روابط فارغة ويجب التأكد أن جميع الروابط بها محتوى.

معايير المحتوى وسهولة البحث:

- استخدام كلمات متنوعة وشائعة الاستخدام بما يضمن زيادة فرص البحث عن المحتوى.
- الالتزام عند كتابة عناوين المحتوى بالوضوح والتفصيل حتى يسهل البحث عنها في محركات البحث.

معايير النشر:

- مراجعة المحتوى جيدا وتدقيقه قبل النشر.
- اعتماد المحتوى من الإدارة المختصة مالكة المحتوى قبل نشره.
- سرعة نشر المحتوى بما يتزامن مع الحدث.
- ترتيب المادة المنشورة حسب تاريخها.
- يجب مراعاة حقوق النشر وحقوق الملكية الفكرية.

فريق العمل

رئيس الفريق	د. سلطان بن صالح الخليوي المشرف العام على إدارة تقنية المعلومات
محرر الوثيقة	م. خالد حسن المعايعة
مراجع داخلي	د. عبدالله الشنطي
مراجع خارجي	أ. سلمان الرويلي