الجامعة الإسلامية بالمدينة المنورة

عمادة التقنية والتعلم الإلكتروني

وثيقة

" سياسة إنشاء البريد الإلكتروني"

التعديلات على الوثيقة

النسخة	التاريخ	المحرر	العملية
0.1	2024/08/10	م.أيمن الغامدي	إنشاء الملف

الغرض
تحدد هذه السياسة الإجراءات والإرشادات لإنشاء حسابات البريد الإلكتروني للموظفين والطلاب والمستخدمين المصرح لهم، لضمان الإدارة السليمة والأمان والاستخدام الصحيح لأنظمة البريد الإلكتروني بالجامعة.

النطاق
تنطبق هذه السياسة على جميع مستخدمي البريد الإلكتروني الخاصة بالجامعة، بما في ذلك الموظفين والطلاب والمتعاقدين والمستخدمين المصرح لهم.

بنود السياسة

1. الأدوار والمسؤوليات

- مالك وراع هذه السياسة هو قسم الخوادم الإفتراضية والتخزين.
- قسم الخوادم الإفتراضية والتخزين مسؤول عن صيانة ودقة السياسة.
- إلتزام جميع منسوبي الجامعة
- تتمتع قسم الخوادم الإفتراضية والتخزين بسلطة التحقق من امتثال جميع موظفي الجامعة للامتثال لهذه السياسة بالإضافة إلى المقاولين والاستشاريين والزملاء الخارجيين وسلسلة التوريد الخاصة بالطرف الثالث وأي موظفين مؤقتين لديهم حسابات على شبكة الجامعة.
- يجب توجيه أي أسئلة بخصوص هذه السياسة إلى قسم الخوادم الإفتراضية والتخزين.

2. أنواع حسابات البريد الإلكتروني المؤهلة

تقدم الجامعة الأنواع التالية من حسابات البريد الإلكتروني:

1. **بريد الأقسام:**
   - يُخصص للاستخدام الخاص بالأقسام للتعامل مع الاتصالات الرسمية.
   - تنسيق التسمية: [اسم القسم]@iu.edu.sa (مثل finance@iu.edu.sa أو admissions@iu.edu.sa). حسب توفر الاسم.
   - يجب أن يتم طلب هذه الخدمة بواسطة مدير الجهة الطالبة للبريد والموافقة عليها من عمادة التقنية والتعلم الإلكتروني.
2. **بريد الموظف الشخصي:**
   - يُخصص للموظفين الأفراد لاستخدامهم الشخصي المتعلق بالعمل.
   - تنسيق التسمية: [الحرف الأول من الاسم الأول].[اسم العائلة]@iu.edu.sa. حسب توفر الاسم.
   - يتم إنشاؤه تلقائيًا للموظفين عند التوظيف.

3. **بريد الطالب الشخصي:**
   - يُخصص لجميع الطلاب المسجلين لتسهيل التواصل الأكاديمي.
   - تنسيق التسمية: (student ID)@stu.edu.sa
   - يتم إنشاؤه تلقائيًا للطلاب عند التسجيل.
4. **بريد آخر (المتعاقدون والمتعاونون):**
   - يمكن منح حسابات البريد الإلكتروني للمتعاقدين أو المتعاونين الخارجيين حسب كل حالة.
   - تنسيق التسمية] :الغرض أو الدور المحدد.iu.edu.sa@[
   - يتطلب الموافقة من مدير الجهة الطالبة للخدمة والقسم المعني وعمادة التقنية والتعلم الإلكتروني.

3. طلب إنشاء حساب بريد إلكتروني:

- يجب تقديم طلبات إنشاء بريد الأقسام أو المتعاقدين عبر بوابة إدارة خدمات تقنية المعلومات بالجامعة أو النموذج الرسمي لطلب البريد الإلكتروني.
- يجب أن يتضمن الطلب المعلومات التالية:
  - نوع البريد المطلوب.
  - الاسم الكامل أو اسم القسم.
  - رقم الجامعة (للموظفين والطلاب).
  - مبرر أو غرض الحساب (لحسابات الأقسام والمتعاقدين).

4. عملية الموافقة:

- **بريد الجهات أو الأقسام** :يجب تقديم الطلبات من قبل مدير الجهة الطالبة للخدمة والموافقة عليها من عمادة التقنية والتعلم الإلكتروني
- **بريد الموظفون** :يتم إنشاء حسابات البريد الشخصي تلقائيًا عند التوظيف.
- **بريد الطلاب** :يتم إنشاء حسابات البريد الإلكتروني تلقائيًا عند التسجيل.
- **بريد المتعاقدون** :يجب أن يتم الموافقة على الطلبات من القسم وعمادة تقنية المعلومات.

5. إرشادات الاستخدام:

- يجب استخدام حسابات البريد الإلكتروني لأغراض الجامعة فقط.
- يجب على المستخدمين الالتزام بسياسة **استخدام البريد الإلكتروني** وضمان الامتثال لإرشادات الأمان.

6. إيقاف الحسابات:

- **بريد الأقسام** :يظل نشطًا ما لم يتم تقديم طلب لإيقافه من قبل مدير الجهة.
- **بريد الموظفين الشخصي** :يتم تعطيله عند إنهاء الخدمة ما لم يتم طلب تمديد من الجهة المعنية.
- **بريد الطلاب** :يظل نشطًا لمدة 6 أشهر بعد التخرج أو الانسحاب.
- **بريد المتعاقدين** :يتم تعطيله عند انتهاء العقد أو المشروع.

7. متطلبات الأمان:

- يجب أن تتوافق كلمات المرور مع **سياسة كلمات مرور المستخدمين**.
- التحقق بخطوتين (MFA) إلزامي لجميع الحسابات.

8. الامتثال والتنفيذ:

- قد يؤدي عدم الامتثال لهذه السياسة إلى اتخاذ إجراءات تأديبية، بما في ذلك تعليق أو إيقاف حساب البريد الإلكتروني.
- تحتفظ عمادة تقنية المعلومات بحق مراجعة استخدام البريد الإلكتروني وتكوينه لضمان الالتزام بهذه السياسة.

9. المراجعة والتحديثات:

- ستتم مراجعة هذه السياسة سنويًا أو كلما طرأت تغييرات كبيرة على أنظمة البريد الإلكتروني أو البنية التحتية ذات الصلة.

م	الاسم	المنصب	التاريخ	التوقيع
1	م.أيمن محمد الغامدي	مدير إدارة البنية التحتية	2024/08/12	
2				
3				

الجامعة الإسلامية بالمدينة المنورة

عمادة التقنية والتعلم الإلكتروني

وثيقة

" سياسة استخدام البريد الإلكتروني "

التعديلات على الوثيقة

النسخة	التاريخ	المحرر	العملية
0.1	2024/08/10	م.أيمن الغامدي	إنشاء الملف

الغرض
تهدف هذه السياسة إلى تحديد الإرشادات لاستخدام البريد الإلكتروني الخاص بالجامعة لضمان الاستخدام الآمن والمسؤول والامتثال للسياسات الداخلية والقوانين ذات الصلة.

النطاق
تنطبق هذه السياسة على جميع مستخدمي أنظمة البريد الإلكتروني الخاصة بالجامعة، بما في ذلك الموظفين والطلاب والمقاولين وأي جهة أخرى تمتلك حساب بريد إلكتروني ضمن نطاق الجامعة.

- نطاق البريد الإلكتروني للموظفين**iu.edu.sa** :
- نطاق البريد الإلكتروني للطلاب**stu.edu.sa** :

بنود السياسة

1. الأدوار والمسؤوليات

- مالك وراع هذه السياسة هو قسم الخوادم الإفتراضية والتخزين.
- قسم الخوادم الإفتراضية والتخزين مسؤول عن صيانة ودقة السياسة.
- إلتزام جميع منسوبي الجامعة
- تتمتع قسم الخوادم الإفتراضية والتخزين بسلطة التحقق من امتثال جميع موظفي الجامعة للامتثال لهذه السياسة بالإضافة إلى المقاولين والاستشاريين والزملاء الخارجيين وسلسلة التوريد الخاصة بالطرف الثالث وأي موظفين مؤقتين لديهم حسابات على شبكة الجامعة.
- يجب توجيه أي أسئلة بخصوص هذه السياسة إلى قسم الخوادم الإفتراضية والتخزين.

2. الاستخدام المصرح به

- يجب استخدام حسابات البريد الإلكتروني التابعة للجامعة للأغراض الأكاديمية والإدارية والمهام المرتبطة بأنشطة الجامعة فقط.
- يحظر استخدام البريد الإلكتروني الخاص بالجامعة للأغراض الشخصية أو التجارية أو أي نشاط غير قانوني أو غير أخلاقي.
- عدم الانخراط في أي أنشطة من شأنها المساس بسلامة أو سرية أو توفر نظام البريد الإلكتروني.
- تجنب مشاركة أو إعادة توجيه المعلومات الحساسة أو السرية (المستوى 1 والمستوى2) (البيانات المحضورة) حسب تصنيف البيانات في سياسات حوكمة البيانات الوطنية دون الحصول على الموافقات الرسمية اللازمة.
- ضمان أن تكون جميع الاتصالات عبر نظام البريد الإلكتروني تعكس الاحترافية وتتوافق مع قيم الجامعة الإسلامية والمتطلبات القانونية.
- الإبلاغ فورًا عن أي سوء استخدام مشتبه به أو خروقات محتملة لنظام البريد الإلكتروني إلى الجهة المختصة.
- يتحمل المستخدم المسؤولية الكاملة عن استخدام حساب البريد الإلكتروني الخاص به.

3. الأمان وحماية البيانات

- يجب على المستخدمين الالتزام بما يلي:
  - عدم مشاركة كلمات المرور الخاصة بحساب البريد الإلكتروني مع أي شخص.
  - استخدام المصادقة متعددة العوامل (MFA) عند تسجيل الدخول.
  - تجنب فتح الروابط أو تنزيل المرفقات المشبوهة.
  - الإبلاغ فورًا عن أي رسائل بريد إلكتروني مريبة أو محاولات تصيد إلى فريق تقنية المعلومات.

4. إرسال واستلام البريد الإلكتروني

- يجب أن تكون جميع الرسائل المرسلة عبر البريد الإلكتروني للجامعة:
  - ذات صلة بمهام الجامعة.
  - خالية من أي محتوى مسيء أو غير لائق.
  - متوافقة مع سياسات حماية البيانات والخصوصية.
- يجب أن يتحقق المستخدمون من صحة عناوين البريد الإلكتروني للمستلمين قبل إرسال الرسائل لتجنب تسريب البيانات.

5. التخزين والأرشفة

- يجب على المستخدمين إدارة بريدهم الإلكتروني بانتظام وحذف الرسائل غير الضرورية.
- يحتفظ قسم تقنية المعلومات بالحق في أرشفة البريد الإلكتروني وفقًا لسياسات الجامعة ولأغراض الامتثال.

6. الاستخدام المحظور

- يحظر استخدام البريد الإلكتروني الخاص بالجامعة في الحالات التالية:
  - نشر معلومات حساسة أو سرية دون إذن رسمي.
  - إرسال رسائل غير مرغوب فيها (Spam) أو محتوى تسويقي.
  - توزيع برامج ضارة أو رسائل تحتوي على فيروسات.
  - استخدام البريد الإلكتروني لانتهاك حقوق الملكية الفكرية أو أي قوانين أخرى.
  - استخدام البريد اللإلكتروني بما يخالف للآداب العامة والتعاليم الإسلامية.
  - استخدام البريد اللإلكتروني بما يخالف الأنظمة والقوانين للمملكة العربية السعودية.

7. الإشراف والمراقبة

- تحتفظ الجامعة بالحق في مراقبة استخدام أنظمة البريد الإلكتروني لضمان الامتثال للسياسات.
- يتم التعامل مع أي انتهاك لسياسة البريد الإلكتروني وفقًا للإجراءات التأديبية للجامعة.

8. انتهاء الصلاحية

- يتم تعطيل حسابات البريد الإلكتروني للطلاب بعد التخرج أو الانسحاب من الجامعة.
- يتم تعطيل حسابات الموظفين عند انتهاء فترة عملهم في الجامعة، بعد تأكيد نقل أو أرشفة البيانات الهامة.

المراجعة والتحديثات

- ستتم مراجعة هذه السياسة بشكل دوري لتتوافق مع التغيرات التقنية والقانونية.
- يتم تحديث السياسة عند الحاجة لضمان حماية بيانات الجامعة وتعزيز أمان أنظمة البريد الإلكتروني.

م	الاسم	المنصب	التاريخ	التوقيع
1	م.أيمن محمد الغامدي	مدير إدارة البنية التحتية	2024/08/12	
2				
3				

الجامعة الإسلامية بالمدينة المنورة

عمادة التقنية والتعلم الإلكتروني

وثيقة

" سياسة الخوادم الافتراضية VMs"

التعديلات على الوثيقة

النسخة	التاريخ	المحرر	العملية
0.1	2024/08/10	م.أيمن الغامدي	إنشاء الملف

الغرض

تهدف هذه السياسة إلى تقديم إرشادات وإجراءات لإنشاء وإعداد وإدارة الخوادم الافتراضية (VMs) داخل المنظمة لضمان الأمان والامتثال وإدارة الموارد بكفاءة.

النطاق

تنطبق هذه السياسة على جميع الموظفين والمتعاقدين والموردين الخارجيين المشاركين في طلب أو إنشاء أو إدارة الخوادم الافتراضية داخل المنظمة.

بنود السياسة

1. **الأدوار والمسؤوليات**

- مالك وراع هذه السياسة هو قسم الخوادم الإفتراضية والتخزين.
- قسم الخوادم الإفتراضية والتخزين مسؤول عن صيانة ودقة السياسة.
- إلتزام جميع منسوبي الجامعة
- تتمتع قسم الخوادم الإفتراضية والتخزين بسلطة التحقق من امتثال جميع موظفي الجامعة للامتثال لهذه السياسة بالإضافة إلى المقاولين والاستشاريين والزملاء الخارجيين وسلسلة التوريد الخاصة بالطرف الثالث وأي موظفين مؤقتين لديهم حسابات على شبكة الجامعة.
- يجب توجيه أي أسئلة بخصوص هذه السياسة إلى قسم الخوادم الإفتراضية والتخزين.

2. **التفويض والموافقة**

- يجب تقديم جميع طلبات إنشاء خادم افتراضي جديد من خلال نظام طلبات خدمة تكنولوجيا المعلومات المعتمد للموافقة عليها.
- **يُسمح فقط لمهندسي عمادة التقنية والتعلم الإلكتروني بتقديم طلبات إنشاء الخوادم الافتراضية، ويجب أن يتم اعتماد هذه الطلبات من قبل قسم الخوادم والتخزين.**
- يجب أن يتضمن كل طلب مبررًا واضحًا للاستخدام التجاري والاستخدام المقصود.
- **يجب على مقدم الطلب تقديم جميع المنافذ المطلوبة للسماح بها، بالإضافة إلى تفاصيل الاستثناءات الأمنية** أثناء عملية تقديم الطلب.

3. **معايير الإعداد والنشر**

- يجب أن تتبع الخوادم الافتراضية التكوينات القياسية التي تحددها المنظمة، والتي تشمل:
  - إصدار نظام التشغيل ومستوى التحديثات
  - تخصيص الموارد (المعالج، الذاكرة، التخزين) المناسب لحجم العمل المتوقع
  - إعدادات الشبكة وتكوينات مجموعات الأمان
- **يجب أن يكون مالك الخادم الافتراضي مهندسًا من عمادة التقنية والتعلم الإلكتروني**، ويتحمل مسؤولية إدارة الخادم وضمان الاستخدام السليم له.
- يجب توثيق أي انحرافات عن التكوينات القياسية والحصول على موافقة قسم تقنية المعلومات عليها.

4. تسمية الفئات والتصنيف

- يجب أن تلتزم الخوادم الافتراضية الجديدة باتفاقيات التسمية المعتمدة في المنظمة لضمان سهولة التعرف عليها وإدارتها.
- يجب تصنيف الخوادم الافتراضية بناءً على القسم، واسم المشروع، والبيئة (مثل الإنتاج، التطوير، الاختبار).

5. الأمان والتحكم في الوصول

- يجب أن تحتوي جميع الخوادم الافتراضية الجديدة على عناصر الأمان الأساسية، بما في ذلك جدران الحماية وبرامج مكافحة الفيروسات والتحديثات الأمنية.
- **يجب أن يقتصر الوصول إلى الخوادم الافتراضية على مالكها من مهندسي عمادة تقنية المعلومات فقط**، ويجب أن تكون الصلاحيات مبنية على مبدأ أقل امتياز ممكن.
- يجب أن يتطلب الوصول عن بُعد إلى الخوادم الافتراضية المصادقة متعددة العوامل.(MFA)
- لا يُسمح للمالك بتحميل أي ملفات أو مجلدات أو تنصيب أي نظام إلى الخادم الافتراضي بخلاف ملفات النظام، وسيتم حذف أي ملفات أو مجلدات غير معتمدة من قبل قسم الخوادم والتخزين.
- لا يُسمح للمالك بمشاركة أي مجلد أو ملف على الخادم الافتراضي.

6. تخصيص الموارد وتحسينها

- يجب تخصيص الموارد للخوادم الافتراضية بناءً على أحجام العمل المتوقعة لتجنب الإفراط أو القصور في التخصيص.
- يجب على مسؤولي تقنية المعلومات مراقبة تخصيص الموارد بانتظام وإجراء التعديلات لضمان الأداء الأمثل.
- إذا كانت هناك أدوات تلقائية متاحة، يجب استخدامها لتقييم استخدام الموارد وإجراء التعديلات اللازمة.

7. متطلبات النسخ الاحتياطي والاستعادة

- يجب دمج جميع الخوادم الافتراضية الجديدة في نظام النسخ الاحتياطي الخاص بالمنظمة عند نشرها.
- يجب أن يكون لكل خادم افتراضي خطة نسخ احتياطي واستعادة تتماشى مع سياسات الاحتفاظ بالبيانات واستعادتها في المنظمة.
- يجب تحديد تكرار النسخ الاحتياطي ومتطلبات الاحتفاظ بناءً على أهمية الخادم الافتراضي.

8. الامتثال والتوثيق

- يجب أن يتوافق إنشاء ونشر الخوادم الافتراضية مع جميع اللوائح والمعايير الصناعية ذات الصلة بالإضافة إلى السياسات الأمنية الداخلية.
- يجب أن تتضمن الوثائق الخاصة بكل خادم افتراضي ما يلي:
  - مبرر الاستخدام التجاري والاستخدام المقصود
  - إعدادات التكوين والأمان
  - قوائم التحكم في الوصول والصلاحيات
  - خطط النسخ الاحتياطي والاستعادة
- يجب تخزين الوثائق في موقع يسهل الوصول إليه للمراجعة والتدقيق.

9. **إيقاف التشغيل وإدارة دورة الحياة**

- يجب أن يكون لكل خادم افتراضي دورة حياة محددة، بما في ذلك الإيقاف أو إعادة الاستخدام بمجرد عدم الحاجة إليه.
- يجب مسح الخوادم الافتراضية التي تم إيقاف تشغيلها بشكل آمن لإزالة أي بيانات حساسة، مع الاحتفاظ بسجلات عملية الإيقاف لأغراض التدقيق.

الأدوار والمسؤوليات

- **القسم الطالب** :يجب أن يكون مقدم الطلب **مهندسًا من عمادة تقنية المعلومات** ويتحمل مسؤولية تقديم المبرر التجاري وجميع المنافذ المطلوبة وتفاصيل الاستثناءات الأمنية وطلب إنشاء الخادم الافتراضي.
- **مسؤولو تقنية المعلومات** :مسؤولون عن إعداد الخوادم الافتراضية وضمان الأمان والحفاظ على التكوينات القياسية.
- **فريق أمن تقنية المعلومات** :مسؤول عن ضمان تنفيذ ضوابط الأمان، بما في ذلك إدارة الوصول، لجميع الخوادم الافتراضية الجديدة.
- **مسؤول الامتثال** :مسؤول عن التحقق من أن جميع الخوادم الافتراضية الجديدة تتوافق مع اللوائح والسياسات الداخلية ذات الصلة.

التنفيذ

قد يؤدي عدم الامتثال لهذه السياسة إلى اتخاذ إجراءات تأديبية، بما في ذلك إلغاء حقوق الوصول والامتيازات. وقد تؤدي حالات عدم الامتثال المتكررة إلى اتخاذ إجراءات إدارية أو عقابية إضافية.

المراجعة

ستتم مراجعة هذه السياسة سنويًا لضمان بقائها متوافقة مع أهداف المنظمة والتطورات التكنولوجية والتحديثات التنظيمية.

م	الاسم	المنصب	التاريخ	التوقيع
1	م.أيمن محمد الغامدي	مدير إدارة البنية التحتية	2024/08/12	
2				
3				

الجامعة الإسلامية بالمدينة المنورة

عمادة التقنية والتعلم الإلكتروني

وثيقة

" سياسة طلب الوصول إلى الخوادم الافتراضية (VM)"

التعديلات على الوثيقة

النسخة	التاريخ	المحرر	العملية
0.1	2024/08/10	م.أيمن الغامدي	إنشاء الملف

الغرض

تحدد هذه السياسة الإجراءات والمتطلبات لطلب الوصول إلى الخوادم الافتراضية (VM) ضمن البنية التحتية لتقنية المعلومات في الجامعة لضمان التفويض المناسب والأمان والمساءلة.

النطاق

تنطبق هذه السياسة على جميع الموظفين والمتعاقدين والأفراد المصرح لهم الذين يطلبون الوصول إلى الخوادم الافتراضية المدارة ضمن البنية التحتية لتقنية المعلومات بالجامعة.

بنود السياسة

1. الأدوار والمسؤوليات

- مالك وراع هذه السياسة هو قسم الخوادم الإفتراضية والتخزين.
- قسم الخوادم الإفتراضية والتخزين مسؤول عن صيانة ودقة السياسة.
- إلتزام جميع منسوبي الجامعة
- تتمتع قسم الخوادم الإفتراضية والتخزين بسلطة التحقق من امتثال جميع موظفي الجامعة للامتثال لهذه السياسة بالإضافة إلى المقاولين والاستشاريين والزملاء الخارجيين وسلسلة التوريد الخاصة بالطرف الثالث وأي موظفين مؤقتين لديهم حسابات على شبكة الجامعة.
- يجب توجيه أي أسئلة بخصوص هذه السياسة إلى قسم الخوادم الإفتراضية والتخزين.

2. الأهلية للحصول على الوصول إلى الخوادم الافتراضية

1. تعطى صلاحية الوصول للخادم للقسم والمهندس المالك للخادم بعمادة تقنية المعلومات إلى الوصول إلى الخوادم الافتراضية تقديم طلبات الوصول.
2. سيتم منح الوصول فقط للأفراد الذين تتطلب أدوارهم ومسؤولياتهم ذلك، بناءً على تقييم القسم التابع له وإدارة الخوادم والتخزين.

3. عملية طلب الوصول

- يجب تقديم جميع طلبات الوصول إلى الخوادم الافتراضية عبر بوابة إدارة خدمات تقنية المعلومات الرسمية.
- يجب أن تتضمن الطلبات التفاصيل التالية:

- مبرر الوصول.
- الخادم الافتراضي المحدد المطلوب الوصول إليه.
- مدة الوصول المطلوبة.
- مستوى الوصول المطلوب (مثل: مسؤول، مستخدم).

- أي متطلبات خاصة أو إعدادات إضافية.
- يجب الموافقة على الطلب من قبل:

  - رئيس القسم التابع له مقدم الطلب.
  - قسم الخوادم والتخزين.

4. الموافقة على الوصول والتفعيل

- يتم تفعيل الوصول بعد الموافقة عليه من قبل قسم الخوادم والتخزين.
- سيتم منح الوصول بناءً على مبدأ أقل امتياز، مما يضمن حصول المستخدمين على أقل عدد من الصلاحيات اللازمة لأداء مهامهم.
- يجب تفعيل التحقق بخطوتين (MFA) لجميع المستخدمين الذين يصلون إلى الخوادم الافتراضية.

5. إرشادات الاستخدام

- يتحمل المستخدمون مسؤولية الحفاظ على أمان وسرية بيانات الاعتماد الخاصة بهم.
- يجب استخدام الوصول إلى الخوادم الافتراضية فقط للمهام والأنشطة المصرح بها داخل الجامعة.
- يحظر على المستخدمين:
  - مشاركة بيانات الاعتماد الخاصة بهم مع الآخرين.
  - إجراء تغييرات غير مصرح بها على إعدادات الخادم أو تكويناته.

6. المراقبة والمراجعة

- ستقوم إدارة تقنية المعلومات بمراقبة سجلات الوصول إلى الخوادم الافتراضية لضمان الامتثال لسياسات الجامعة.
- سيتم مراجعة صلاحيات الوصول بشكل دوري، وسيتم إلغاء أي صلاحيات غير مستخدمة أو غير ضرورية.

7. إلغاء الوصول

سيتم إلغاء الوصول في الحالات التالية:

- انتهاء مدة الوصول المصرح بها.
- تغيير الدور الوظيفي أو المسؤوليات التي لا تتطلب الوصول إلى الخوادم الافتراضية.
- انتهاك سياسات الجامعة أو الإرشادات الأمنية.
- يجب على الأقسام إخطار قسم الخوادم والتخزين بأي تغييرات في أهلية المستخدمين للوصول إلى الخوادم الافتراضية.

8. الامتثال والتنفيذ

- يجب على المستخدمين الامتثال لهذه السياسة وجميع السياسات الأخرى المتعلقة بتقنية المعلومات في الجامعة.
- قد يؤدي عدم الامتثال إلى:

- تعليق فوري للوصول إلى الخوادم الافتراضية.
- اتخاذ إجراءات تأديبية وفقًا للوائح الجامعة.

المراجعة والتحديثات

ستتم مراجعة هذه السياسة سنويًا أو عند حدوث تغييرات كبيرة في البنية التحتية لتقنية المعلومات بالجامعة أو المتطلبات التشغيلية.

م	الاسم	المنصب	التاريخ	التوقيع
1	م.أيمن محمد الغامدي	مدير إدارة البنية التحتية	2024/08/12	
2				
3				

الجامعة الإسلامية بالمدينة المنورة

عمادة التقنية والتعلم الإلكتروني

وثيقة

" سياسة استعادة نسخة احتياطية للخوادم الافتراضية(VM)"

التعديلات على الوثيقة

النسخة	التاريخ	المحرر	العملية
0.1	2024/08/10	م.أيمن الغامدي	إنشاء الملف

الغرض

تحدد هذه السياسة الإجراءات والمتطلبات لاستعادة نسخ الخوادم الافتراضية (VM) لضمان توفر البيانات وسلامتها وموثوقيتها ضمن البنية التحتية لتقنية المعلومات في الجامعة في حالة حدوث أعطال أو فقدان للبيانات.

النطاق

تنطبق هذه السياسة على جميع النسخ الاحتياطية للخوادم الافتراضية المدارة من قبل البنية التحتية لتقنية المعلومات في الجامعة. وتشمل عملية الاستعادة، الأدوار والمسؤوليات، والإرشادات الخاصة باستعادة النسخ الاحتياطية للخوادم الافتراضية للموظفين والمتعاقدين والمستخدمين المصرح لهم.

بنود السياسة

1. الأدوار والمسؤوليات

- مالك وراع هذه السياسة هو قسم الخوادم الإفتراضية والتخزين.
- قسم الخوادم الإفتراضية والتخزين مسؤول عن صيانة ودقة السياسة.
- إلتزام جميع منسوبي الجامعة
- تتمتع قسم الخوادم الإفتراضية والتخزين بسلطة التحقق من امتثال جميع موظفي الجامعة للامتثال لهذه السياسة بالإضافة إلى المقاولين والاستشاريين والزملاء الخارجيين وسلسلة التوريد الخاصة بالطرف الثالث وأي موظفين مؤقتين لديهم حسابات على شبكة الجامعة.
- يجب توجيه أي أسئلة بخصوص هذه السياسة إلى قسم الخوادم الإفتراضية والتخزين.

2. أهلية استعادة النسخة الاحتياطية

1. يحق فقط للقسم والمهندس المالك للخادم بعمادة تقنية المعلومات طلب استعادة النسخ الاحتياطية للخوادم الافتراضية.
2. يجب أن تستند طلبات استعادة النسخ الاحتياطية إلى حاجة مشروعة مثل فقدان البيانات أو حدوث فشل أو تلف في بيانات الخادم الافتراضي.

3. طلب استعادة النسخة الاحتياطية للخوادم الافتراضية

1. يجب تقديم جميع طلبات استعادة النسخ الاحتياطية عبر بوابة إدارة خدمات تقنية المعلومات الرسمية.
2. يجب أن تتضمن الطلبات التفاصيل التالية:

- مبرر طلب الاستعادة (مثل فقدان البيانات أو الفشل أو التلف).
- الخادم الافتراضي المحدد المطلوب استعادته.
- تاريخ ووقت النسخة الاحتياطية المطلوبة لاستعادتها.
- الهدف من الاستعادة (مثل الخادم الافتراضي الأصلي أو خادم جديد).

3. يجب الموافقة على الطلب من قبل:

- رئيس القسم المالك للخادم.
- قسم الخوادم والتخزين.

4. عملية الاستعادة:

ستقوم إدارة الخوادم والتخزين بتنفيذ الاستعادة وفقًا لما يلي:

- سيتم استعادة النسخة من النسخة الاحتياطية الصالحة والأحدث.
- إذا كان الخادم الافتراضي الأصلي غير صالح، سيتم استعادته إلى خادم افتراضي جديد بنفس التكوين والبيانات.
- سيتم استعادة النسخة وفقًا لمبدأ أقل امتياز لضمان استعادة البيانات والإعدادات اللازمة فقط.

يجب إتمام عملية الاستعادة ضمن إطار زمني معقول بناءً على تعقيد وحجم النسخة الاحتياطية.

5. سلامة البيانات والأمان

أثناء عملية الاستعادة، ستتم جميع فحوصات سلامة البيانات للتأكد من عدم وجود تلف أو فقدان للبيانات.
يجب أن تتوافق جميع الخوادم الافتراضية المستعادة مع سياسات الأمان في الجامعة، بما في ذلك تكوينات مكافحة الفيروسات والجدران النارية.
ستقوم إدارة تقنية المعلومات بالتحقق من أن الخوادم الافتراضية المستعادة تعمل بشكل صحيح ويمكن الوصول إليها من قبل المالك المفوض.

6. المراقبة والتوثيق

1. سيتم تسجيل جميع طلبات الاستعادة، بما في ذلك تفاصيل الطلب والموافقة والتنفيذ.
2. ستقوم إدارة تقنية المعلومات بمراقبة الخادم الافتراضي المستعاد لمدة معينة لضمان عمله بشكل سليم.
3. سيتم توثيق أي مشكلات تم مواجهتها أثناء عملية الاستعادة، واتخاذ الإجراءات التصحيحية إذا لزم الأمر.

7. **مسؤولية المستخدم**
- يجب على المستخدمين ضمان أن يتم إجراء النسخ الاحتياطية بانتظام على الخوادم الافتراضية الهامة وفقًا لسياسات النسخ الاحتياطي في الجامعة.
- يتحمل المستخدمون مسؤولية إخطار إدارة تقنية المعلومات على الفور في حالة فقدان البيانات أو حدوث أعطال في الخوادم الافتراضية تتطلب الاستعادة.

8. **الوصول والمراجعة**
- سيتم منح الوصول إلى الخوادم الافتراضية المستعادة بناءً على مبدأ أقل امتياز، مما يضمن وصول المالك المفوض فقط.
- بعد الاستعادة، سيتم مراجعة صلاحيات الوصول والتصاريح لضمان الامتثال لسياسات الجامعة.

9. **الامتثال والتنفيذ**
- يجب أن تتوافق جميع عمليات استعادة النسخ الاحتياطية للخوادم الافتراضية مع سياسات تقنية المعلومات في الجامعة، بما في ذلك سياسات حماية البيانات والأمان والمعايير التشغيلية.
- قد يؤدي عدم الامتثال إلى سياسة استعادة النسخ الاحتياطية إلى اتخاذ إجراءات تأديبية، بما في ذلك تعليق الوصول إلى الخادم الافتراضي أو اتخاذ تدابير تصحيحية أخرى.

10. **المراجعة والتحديثات**
ستتم مراجعة هذه السياسة سنويًا أو عند حدوث تغييرات كبيرة في بنية تقنية المعلومات بالجامعة أو ممارسات النسخ الاحتياطي.

م	الاسم	المنصب	التاريخ	التوقيع
1	م.أيمن محمد الغامدي	مدير إدارة البنية التحتية	2024/08/12	
2				
3				

الجامعة الإسلامية بالمدينة المنورة

عمادة التقنية والتعلم الإلكتروني

وثيقة

" سياسة حذف خوادم الأجهزة الافتراضية"

التعديلات على الوثيقة

النسخة	التاريخ	المحرر	العملية
0.1	2024/08/10	م.أيمن الغامدي	إنشاء الملف

الغرض
تهدف هذه السياسة إلى وضع الإرشادات والإجراءات اللازمة لحذف خوادم الأجهزة الافتراضية (Virtual Machines) بطريقة آمنة ومنظمة، لضمان حماية البيانات والحفاظ على سلامة البنية التحتية لتقنية المعلومات في الجامعة.

النطاق
تنطبق هذه السياسة على جميع خوادم الأجهزة الافتراضية المُدارة أو المُستضافة ضمن البنية التحتية لتقنية المعلومات التابعة للجامعة الإسلامية.

بنود السياسة

1. الأدوار والمسؤوليات

- مالك وراع هذه السياسة هو قسم الخوادم الإفتراضية والتخزين.
- قسم الخوادم الإفتراضية والتخزين مسؤول عن صيانة ودقة السياسة.
- إلتزام جميع منسوبي الجامعة
- تتمتع قسم الخوادم الإفتراضية والتخزين بسلطة التحقق من امتثال جميع موظفي الجامعة للامتثال لهذه السياسة بالإضافة إلى المقاولين والاستشاريين والزملاء الخارجيين وسلسلة التوريد الخاصة بالطرف الثالث وأي موظفين مؤقتين لديهم حسابات على شبكة الجامعة.
- يجب توجيه أي أسئلة بخصوص هذه السياسة إلى قسم الخوادم الإفتراضية والتخزين.

2. شروط طلب الحذف

- يجب أن يقدم طلب حذف الخادم الافتراضي من قبل مالك الخادم (مهندس من عمادة تقنية المعلومات).
- يجب أن يتضمن الطلب ما يلي:
  - سبب الحذف.
  - تأكيد أن البيانات المخزنة على الخادم لم تعد مطلوبة أو تم نقلها إلى موقع آمن.
  - أي تفاصيل إضافية تتعلق بإعدادات الخادم أو تكامله مع أنظمة أخرى.

3. الموافقة

- يتم مراجعة طلب الحذف والموافقة عليه من قبل **قسم الخوادم والتخزين**.
- يتم التحقق من استيفاء جميع المتطلبات قبل تنفيذ الحذف.

4. إجراءات الحذف

- يتم نسخ جميع البيانات المهمة أو الضرورية احتياطيًا أو نقلها بناءً على طلب صاحب الخادم قبل تنفيذ الحذف.
- يتم إزالة الخادم الافتراضي من جميع قوائم الشبكة والتكامل مع الأنظمة الأخرى.
- يتم التأكد من حذف جميع المعلومات المرتبطة بالخادم من البنية التحتية لتقنية المعلومات.

5. الأمان

- يتم التحقق من أن جميع البيانات المخزنة على الخادم قد تم حذفها بشكل آمن ونهائي لتجنب أي استرجاع غير مصرح به.
- يتم تنفيذ إجراءات الحذف بواسطة فريق معتمد من **قسم الخوادم والتخزين**.

6. التوثيق

- يتم توثيق عملية الحذف، بما في ذلك:
  - تاريخ الحذف.
  - هوية الشخص المسؤول عن التنفيذ.
  - أي ملاحظات تتعلق بالعملية.

7. التزام الجهات

- يتحمل مالكو الخوادم مسؤولية ضمان نقل البيانات المهمة أو طلب نسخ احتياطية قبل الحذف.
- يتحمل **قسم الخوادم والتخزين** مسؤولية تنفيذ عملية الحذف بما يتماشى مع هذه السياسة.

8. مراجعة الطلبات

- يتم الاحتفاظ بجميع طلبات الحذف ووثائقها للرجوع إليها عند الحاجة.
- يتم إجراء مراجعة دورية لضمان الالتزام بإجراءات الحذف.

المراجعة والتحديثات

- ستتم مراجعة هذه السياسة بشكل دوري لضمان توافقها مع التغييرات التقنية والتنظيمية.
- يتم تحديث السياسة عند الحاجة لتعكس أي تغييرات في الإجراءات أو المتطلبات.

م	الاسم	المنصب	التاريخ	التوقيع

1	م.أيمن محمد الغامدي	مدير إدارة البنية التحتية	2024/08/12	
2				
3				

الجامعة الإسلامية بالمدينة المنورة

عمادة التقنية والتعلم الإلكتروني

وثيقة

" سياسة سطح المكتب الافتراضي (VDI)"

التعديلات على الوثيقة

النسخة	التاريخ	المحرر	العملية
0.1	2024/08/10	م.أيمن الغامدي	إنشاء الملف

الغرض

تحدد هذه السياسة المعايير والإرشادات لاستخدام وإدارة وأمان البنية التحتية لسطح المكتب الافتراضي (VDI) لضمان الوصول الآمن والفعال إلى موارد الجامعة عن بُعد.

النطاق

تنطبق هذه السياسة على جميع المستخدمين الذين يصلون إلى البنية التحتية لسطح المكتب الافتراضي (VDI) الخاصة بالجامعة، بما في ذلك الموظفين والطلاب والمتعاقدين والمستخدمين المصرح لهم.

بنود السياسة

1. الأدوار والمسؤوليات

- مالك وراع هذه السياسة هو قسم الخوادم الإفتراضية والتخزين.
- قسم الخوادم الإفتراضية والتخزين مسؤول عن صيانة ودقة السياسة.
- إلتزام جميع منسوبي الجامعة
- تتمتع قسم الخوادم الإفتراضية والتخزين بسلطة التحقق من امتثال جميع موظفي الجامعة للامتثال لهذه السياسة بالإضافة إلى المقاولين والاستشاريين والزملاء الخارجيين وسلسلة التوريد الخاصة بالطرف الثالث وأي موظفين مؤقتين لديهم حسابات على شبكة الجامعة.
- يجب توجيه أي أسئلة بخصوص هذه السياسة إلى قسم الخوادم الإفتراضية والتخزين.

2. الأهلية والوصول

المستخدمون المؤهلون:

- الوصول إلى (VDI) متاح لموظفي الجامعة والطلاب والمتعاقدين المصرح لهم الذين يحتاجون إلى الوصول إلى موارد الجامعة عن بُعد.
- يجب أن تتم الموافقة على طلبات الوصول إلى (VDI) من قبل رئيس قسم الخوادم والتخزين.

متطلبات الوصول:

- يجب أن يمتلك المستخدمون حساب في الجامعة صالحًا وأن يتم الإلتزام بـ **سياسة كلمات مرور المستخدمين**.
- التحقق بخطوتين (MFA) إلزامي للوصول إلى.(VDI)

3. طلب الوصول إلى (VDI)

يجب على المستخدمين الذين يطلبون الوصول إلى (VDI) تقديم طلب رسمي لقسم الخوادم والتخزين بعمادة التقنية والتعلم الإلكتروني، متضمنًا:

- مبرر الحاجة إلى الوصول إلى(VDI) .
- مدة الوصول المطلوبة.
- أي موارد أو تطبيقات محددة مطلوبة.

يجب مراجعة الطلبات والموافقة عليها من قبل:

- مدير الجهة التابع له المستخدم.
- عمادة التقنية والتعلم الإلكتروني.

4. إرشادات الاستخدام

- يجب استخدام (VDI) فقط للمهام والأنشطة المتعلقة بالجامعة.
- يُحظر على المستخدمين تثبيت أي برامج غير مصرح بها أو تعديل إعدادات النظام.
- يجب تخزين البيانات على الخوادم المعتمدة الخاصة بالجامعة وليس على الأجهزة المحلية.
- يجب على المستخدمين تسجيل الخروج من جلسة (VDI) بعد الانتهاء من المهام لضمان الأمان.

5. الأمان والمراقبة:

إجراءات الأمان:

- يتم تشفير جلسات (VDI) لضمان سرية بيانات الجامعة.
- يجب أن تكون برامج مكافحة الفيروسات والجدران النارية مفعّلة ومحدثة على الأجهزة المستخدمة للوصول إلى.(VDI)

المراقبة:

- ستقوم قسم الخوادم والتخزين بمراقبة استخدام (VDI) لضمان الامتثال لهذه السياسة.
- سيتم الاحتفاظ بسجلات الجلسات الخاصة بـ(VDI) ، بما في ذلك أوقات الوصول والأنشطة، ومراجعتها بشكل دوري.

6. تخصيص الموارد

يتم تخصيص أسطح المكتب الافتراضية بناءً على متطلبات المستخدم، بما في ذلك:

- وحدة المعالجة المركزية (CPU) والذاكرة والتخزين.
- الوصول إلى تطبيقات أو خدمات محددة.

ستتم مراجعة الموارد بشكل دوري لضمان الأداء الأمثل والتخصيص المناسب.

7. تعطيل الوصول إلى(VDI)

سيتم تعطيل الوصول إلى (VDI) في الحالات التالية:

- عند انتهاء خدمة الموظف أو انتهاء عقد المتعاقد.
- بعد التخرج أو الانسحاب للطلاب.
- بعد انتهاء فترة الوصول المعتمدة.

يجب على جهات الجامعة إخطار عمادة التقنية والتعلم الإلكتروني بأي تغييرات في الأهلية.

8. الامتثال والتنفيذ

- يجب على المستخدمين الامتثال لهذه السياسة وجميع السياسات الأخرى ذات الصلة بتقنية المعلومات في الجامعة.
- قد يؤدي عدم الامتثال إلى:

- تعليق الوصول إلى.(VDI)
- اتخاذ إجراءات تأديبية وفقًا للوائح الجامعة.

9. المراجعة والتحديثات

ستتم مراجعة هذه السياسة سنويًا أو عند حدوث تغييرات كبيرة في البنية التحتية لتقنية المعلومات بالجامعة أو المتطلبات ذات الصلة.

م	الاسم	المنصب	التاريخ	التوقيع
1	م.أيمن محمد الغامدي	مدير إدارة البنية التحتية	2024/08/12	
2				
3				

الجامعة الإسلامية بالمدينة المنورة

عمادة التقنية والتعلم الإلكتروني

وثيقة

" سياسة كلمات المرورلحسابات المستخدمين"

التعديلات على الوثيقة

النسخة	التاريخ	المحرر	العملية
0.1	2024/08/10	م.أيمن الغامدي	إنشاء الملف

الغرض
تهدف هذه السياسة إلى ضمان حماية حسابات المستخدمين من الوصول غير المصرح به عن طريق تطبيق معايير قوية لإنشاء وإدارة كلمات المرور.

النطاق
تنطبق هذه السياسة على جميع المستخدمين الذين لديهم حسابات داخل أنظمة وتقنيات الجامعة، بما في ذلك الموظفين والطلاب والمقاولين.

بنود السياسة

1. الأدوار والمسؤوليات

- مالك وراع هذه السياسة هو قسم الخوادم الإفتراضية والتخزين.
- قسم الخوادم الإفتراضية والتخزين مسؤول عن صيانة ودقة السياسة.
- إلتزام جميع منسوبي الجامعة
- تتمتع قسم الخوادم الإفتراضية والتخزين بسلطة التحقق من امتثال جميع موظفي الجامعة للامتثال لهذه السياسة بالإضافة إلى المقاولين والاستشاريين والزملاء الخارجيين وسلسلة التوريد الخاصة بالطرف الثالث وأي موظفين مؤقتين لديهم حسابات على شبكة الجامعة.
- يجب توجيه أي أسئلة بخصوص هذه السياسة إلى قسم الخوادم الإفتراضية والتخزين.

2. إنشاء كلمة المرور

- يجب أن تتبع كلمات المرور المعايير التالية:
  - يجب أن تكون بطول **8أحرف على الأقل**.
  - يجب أن تحتوي على مزيج من الأحرف الكبيرة (A-Z) والصغيرة.(a-z)
  - يجب أن تحتوي على رقمًا واحدًا على الأقل.(0-9)
  - يجب أن تتضمن رمزًا خاصًا واحدًا على الأقل (مثل !, @, #, $, %).

3. إدارة كلمة المرور

- لا يجوز إعادة استخدام أي من **الـ5 كلمات مرور السابقة**.
- يجب تغيير كلمة المرور **كل 90 يومًا** على الأقل.
- في حال الاشتباه بأن كلمة المرور قد تم اختراقها، يجب تغييرها على الفور.

4. استخدام كلمة المرور

- يمنع مشاركة كلمات المرور مع أي شخص، بما في ذلك أفراد العائلة أو الزملاء.
- لا يجوز استخدام كلمات المرور الخاصة بحسابات الجامعة في أي أنظمة خارجية.
- يجب استخدام كلمات مرور مختلفة لكل نظام أو تطبيق يستخدمه المستخدم.

5. الأمان وحماية كلمة المرور

- يجب على المستخدمين:
  - عدم كتابة كلمات المرور في أماكن غير آمنة أو مشاركتها عبر البريد الإلكتروني أو الرسائل النصية.
  - استخدام مدير كلمات مرور آمن إذا لزم الأمر لحفظ وإدارة كلمات المرور.
  - الإبلاغ فورًا عن أي نشاط مشبوه أو محاولة لاختراق الحسابات إلى فريق الأمن السيبراني.

6. تأمين الحسابات

- سيتم قفل الحساب بعد **5محاولات فاشلة** لتسجيل الدخول.
- يمكن للمستخدم طلب إعادة تعيين كلمة المرور من خلال النظام الرسمي أو التواصل مع الدعم الفني.

7. التزام المستخدمين

- يتحمل جميع المستخدمين مسؤولية حماية كلمات المرور الخاصة بهم والحفاظ على سرية بيانات اعتمادهم.
- يعد أي انتهاك لهذه السياسة مسؤولية شخصية وقد يؤدي إلى اتخاذ إجراءات تأديبية.

المراجعة والتحديثات

- ستتم مراجعة هذه السياسة بشكل دوري لضمان التوافق مع أحدث معايير الأمان.
- يتم تحديث السياسة عند حدوث تغييرات تقنية أو أمنية تؤثر على إدارة كلمات المرور.

تنبيه :قد يؤدي عدم الامتثال لهذه السياسة إلى تعليق الحساب أو فرض قيود على الوصول.

م	الاسم	المنصب	التاريخ	التوقيع
1	م.أيمن محمد الغامدي	مدير إدارة البنية التحتية	2024/08/12	
2				
3				

الجامعة الإسلامية بالمدينة المنورة

عمادة التقنية والتعلم الإلكتروني

وثيقة

" سياسة تعطيل حسابات المستخدمين"

التعديلات على الوثيقة

النسخة	التاريخ	المحرر	العملية
0.1	2024/08/10	م.أيمن الغامدي	إنشاء الملف

الغرض
تهدف هذه السياسة إلى وضع معايير وإجراءات لتعطيل حسابات المستخدمين لضمان أمن المعلومات وحماية الموارد التقنية في الجامعة الإسلامية.

النطاق
تنطبق هذه السياسة على جميع حسابات المستخدمين المرتبطة بأنظمة الجامعة، بما في ذلك الموظفين والطلاب والمقاولين وأي جهة أخرى تمتلك حسابات في أنظمة الجامعة.

بنود السياسة

1. الأدوار والمسؤوليات

- مالك وراع هذه السياسة هو قسم الخوادم الإفتراضية والتخزين.
- قسم الخوادم الإفتراضية والتخزين مسؤول عن صيانة ودقة السياسة.
- إلتزام جميع منسوبي الجامعة
- تتمتع قسم الخوادم الإفتراضية والتخزين بسلطة التحقق من امتثال جميع موظفي الجامعة للامتثال لهذه السياسة بالإضافة إلى المقاولين والاستشاريين والزملاء الخارجيين وسلسلة التوريد الخاصة بالطرف الثالث وأي موظفين مؤقتين لديهم حسابات على شبكة الجامعة.
- يجب توجيه أي أسئلة بخصوص هذه السياسة إلى قسم الخوادم الإفتراضية والتخزين.

2. أسباب تعطيل الحسابات

يتم تعطيل حسابات المستخدمين في الحالات التالية:

- انتهاء فترة عمل الموظف في الجامعة أو انتهاء عقده.
- تخرج الطالب أو انسحابه من الجامعة.
- طلب رسمي من المستخدم لتعطيل حسابه.
- الاشتباه في حدوث نشاط غير مصرح به أو خرق أمني.
- عدم الامتثال لسياسات الجامعة المتعلقة باستخدام الحسابات.
- أي استخدام لحساب معطل قد يُعتبر انتهاكًا أمنيًا ويؤدي إلى اتخاذ إجراءات تأديبية.

3. إجراءات تعطيل الحسابات

- يتم تقديم طلب لتعطيل الحساب من خلال الجهة المسؤولة أو مدير القسم.
- يتم تعطيل حسابات موظفي الجامعة بعد إنهاء فترة العمل للموظف بجميع الحالات تلقائياً من خلال النظام الإداري والمالي.
- يتم تعطيل حسابات طلاب الجامعة بعد إنهاء فترة إنتساب الطالب بالجامعة بجميع الحالات تلقائياً من خلال النظام الإكاديمي.

- يتم تعطيل الحسابات حال الإشتباه أو عدم الإمتثال بطلب من الجهات العليا المعنية ويجب أن يتضمن الطلب المعلومات التالية:
  - اسم المستخدم.
  - سبب التعطيل.
  - أي متطلبات إضافية (مثل نقل البيانات).
- يقوم قسم الخوادم والتخزين بمراجعة الطلب وتنفيذه وفقًا للإجراءات المعتمدة.

4. تعطيل الحسابات المؤقتة

- يمكن تعطيل الحسابات بشكل مؤقت عند الحاجة (مثل الإجازات الطويلة أو غياب المستخدم).
- يتم إعادة تنشيط الحساب بناءً على طلب رسمي من الجهة المسؤولة.

5. إدارة البيانات

- قبل تعطيل الحساب بشكل دائم، يجب:
  - نقل جميع البيانات الحساسة أو الهامة إلى جهة معتمدة داخل الجامعة.
  - أرشفة البريد الإلكتروني والملفات المرتبطة بالحساب وفقًا لسياسات الأرشفة.

6. الإبلاغ والمتابعة

- يتم إخطار المستخدم (إن أمكن) بتعطيل حسابه وسبب التعطيل.
- في حالة النشاطات المشبوهة، يتم إرسال تقرير إلى فريق الأمن السيبراني لإجراء تحقيق إضافي.

7. إعادة تنشيط الحسابات

- لا يتم إعادة تنشيط الحسابات المعطلة إلا بعد تقديم طلب رسمي وموافقة القسم المسؤول.
- يتم إعادة التحقق من هوية المستخدم قبل تنشيط الحساب.

8. التزام الجهات

- يتحمل كل قسم مسؤولية الإبلاغ عن الحسابات التي يجب تعطيلها.
- يتولى قسم تقنية المعلومات تنفيذ التعطيل وضمان الالتزام بالإجراءات الأمنية.

المراجعة والتحديثات

- ستتم مراجعة هذه السياسة بشكل دوري لضمان توافقها مع المتطلبات الأمنية والتقنية الحديثة.
- يتم تحديث السياسة عند حدوث تغييرات في البنية التحتية أو الإجراءات التنظيمية.

م	الاسم	المنصب	التاريخ	التوقيع
1	م.أيمن محمد الغامدي	مدير إدارة البنية التحتية	2024/08/12	
2				
3				

الجامعة الإسلامية بالمدينة المنورة

عمادة التقنية والتعلم الإلكتروني

وثيقة

" سياسة التكامل/الإرتباط مع الدليل النشط (Active Directory)"

التعديلات على الوثيقة

النسخة	التاريخ	المحرر	العملية
0.1	2024/08/10	م.أيمن الغامدي	إنشاء الملف

الغرض
تهدف هذه السياسة إلى تحديد الإرشادات والمعايير الخاصة بتكامل الأنظمة والخدمات مع الدليل النشط (Active Directory) في الجامعة الإسلامية لضمان الأمان، الكفاءة، والإدارة المركزية.

النطاق
تنطبق هذه السياسة على جميع الأنظمة، التطبيقات، والخدمات التي تتطلب التكامل مع بيئة الدليل النشط للجامعة.

بنود السياسة

1. الأدوار والمسؤوليات

- مالك وراع هذه السياسة هو قسم الخوادم الإفتراضية والتخزين.
- قسم الخوادم الإفتراضية والتخزين مسؤول عن صيانة ودقة السياسة.
- إلتزام جميع منسوبي الجامعة
- تتمتع قسم الخوادم الإفتراضية والتخزين بسلطة التحقق من امتثال جميع موظفي الجامعة للامتثال لهذه السياسة بالإضافة إلى المقاولين والاستشاريين والزملاء الخارجيين وسلسلة التوريد الخاصة بالطرف الثالث وأي موظفين مؤقتين لديهم حسابات على شبكة الجامعة.
- يجب توجيه أي أسئلة بخصوص هذه السياسة إلى قسم الخوادم الإفتراضية والتخزين.

2. شروط التكامل

- يجب الموافقة على جميع طلبات التكامل مع الدليل النشط من قبل **قسم الخوادم والتخزين**.
- يجب أن تتوافق الأنظمة والخدمات مع معايير الأمن والبنية التحتية المحددة من قبل **عمادة التقنية والتعلم الإلكتروني**.
- يتم تطبيق التكامل فقط للأنظمة والخدمات المرتبطة بالمهام الأكاديمية والإدارية للجامعة.

3. إدارة الهوية

- يتم إدارة جميع الحسابات عبر الدليل النشط لضمان الامتثال للسياسات المركزية للجامعة.
- يجب أن تتبع جميع حسابات المستخدمين سياسة كلمات المرور الخاصة بالجامعة.
- يتم منح الصلاحيات على أساس مبدأ أقل الامتيازات، لضمان وصول المستخدم فقط للموارد الضرورية لأداء مهامه.

4. الأمان

- يجب أن تدعم الأنظمة المتكاملة المصادقة متعددة العوامل.(MFA)
- يجب تشفير جميع الاتصالات بين الأنظمة والدليل النشط باستخدام بروتوكولات آمنة) مثل.(LDAPs
- يتم مراجعة وضبط تكوينات الأمان بشكل دوري لضمان حماية بيانات الجامعة.

5. إجراءات التكامل

- يجب تقديم طلب مكتوب يوضح:
  - الغرض من التكامل.
  - متطلبات النظام.
  - تأثير التكامل على البنية التحتية.
- يتم مراجعة الطلب من قبل **قسم الخوادم والتخزين** لضمان ملاءمته ومعالجة المخاطر المحتملة.
- يتم تنفيذ عملية التكامل من قبل فريق معتمد من **عمادة التقنية والتعلم الإلكتروني**.

6. إدارة التغييرات

- يجب إخطار قسم الخوادم والتخزين مسبقًا بأي تغييرات جوهرية في الأنظمة المتكاملة (مثل التحديثات، الإضافات، أو الإزالة).
- يتم تقييم تأثير التغييرات على البيئة العامة وإجراء اختبارات قبل تطبيقها.

7. إلغاء التكامل

- في حال عدم الحاجة إلى نظام أو خدمة متكاملة، يتم تقديم طلب لإلغاء التكامل.
- يتم التأكد من نقل البيانات الحساسة وحذف أي معلومات مرتبطة بالنظام من الدليل النشط.
- يتم توثيق جميع عمليات الإلغاء لضمان التتبع المستقبلي.

8. الامتثال والتدقيق

- يتم مراجعة جميع الأنظمة المتكاملة بشكل دوري لضمان الامتثال لسياسات الجامعة.
- أي انتهاك لهذه السياسة قد يؤدي إلى إيقاف النظام أو الخدمة وإبلاغ الجهة المسؤولة لاتخاذ الإجراءات المناسبة.

المراجعة والتحديثات

- ستتم مراجعة هذه السياسة بشكل دوري لضمان توافقها مع المعايير التقنية والأمنية الحديثة.
- يتم تحديث السياسة عند الحاجة لتعكس التغييرات في البنية التحتية للجامعة أو متطلبات التشغيل.

م	الاسم	المنصب	التاريخ	التوقيع
1	م.أيمن محمد الغامدي	مدير إدارة البنية التحتية	2024/08/12	
2				
3				

الجامعة الإسلامية بالمدينة المنورة

عمادة التقنية والتعلم الإلكتروني

وثيقة

" سياسة طلب نشر DNS الداخلي"

التعديلات على الوثيقة

النسخة	التاريخ	المحرر	العملية
0.1	2024/08/10	م.أيمن الغامدي	إنشاء الملف

الغرض

تحدد هذه السياسة المعايير والإجراءات الخاصة بتقديم ومراجعة والموافقة على طلبات نشر سجلات نظام أسماء النطاقات (DNS) الداخلية. الهدف هو ضمان إدارة جميع سجلات DNS الداخلية بشكل آمن ومنظم وبما يتماشى مع متطلبات الحوكمة التشغيلية للجامعة.

النطاق

تنطبق هذه السياسة على جميع طلبات نشر سجلات DNS الداخلية للخدمات والتطبيقات والموارد التي يمكن الوصول إليها فقط داخل شبكة الجامعة الداخلية.

بنود السياسة

1. الأدوار والمسؤوليات

- مالك وراع هذه السياسة هو قسم الخوادم الإفتراضية والتخزين.
- قسم الخوادم الإفتراضية والتخزين مسؤول عن صيانة ودقة السياسة.
- إلتزام جميع منسوبي الجامعة
- تتمتع قسم الخوادم الإفتراضية والتخزين بسلطة التحقق من امتثال جميع موظفي الجامعة للامتثال لهذه السياسة بالإضافة إلى المقاولين والاستشاريين والزملاء الخارجيين وسلسلة التوريد الخاصة بالطرف الثالث وأي موظفين مؤقتين لديهم حسابات على شبكة الجامعة.
- يجب توجيه أي أسئلة بخصوص هذه السياسة إلى قسم الخوادم الإفتراضية والتخزين.

2. التفويض والموافقة

- يمكن فقط لمهندسي **عمادة التقنية والتعلم الإلكتروني** أو الموظفين المخولين في الأقسام ذات الصلة تقديم طلبات نشر DNS الداخلي.
- يجب أن تتم الموافقة على جميع الطلبات من قبل **قسم الخوادم والتخزين** لضمان الحاجة التشغيلية.
- يجب أن تتم الموافقة على جميع الطلبات من قبل **إدارة الأمن السيبراني** لضمانالامتثال لمعايير الأمان.

3. متطلبات تقديم الطلب

- يجب تقديم الطلبات عبر النظام الرسمي لطلبات تقنية المعلومات قبل تاريخ النشر بصلاثة أيام عمل، ويجب أن تتضمن:
  - اسم المضيف أو النطاق الفرعي المطلوب إنشاؤه.
  - عنوان IP أو نقطة النهاية للموارد المرتبطة.
  - نوع سجل DNS المطلوب (مثل A ، CNAME، TXT، SRV).
  - الغرض التشغيلي للسجل ومدى أهميته.
  - أي استثناءات أمان أو تكوينات خاصة.

4. اتفاقيات التسمية

- يجب أن تلتزم جميع سجلات DNS الداخلية باتفاقيات التسمية الرسمية للجامعة لضمان الاتساق وتجنب التضارب.
- يجب أن تكون أسماء المضيفين:
  - وصفية وتمثل الخدمة أو المورد بشكل واضح.
  - خالية من الأسماء العامة أو الغامضة.

5. الأمان والامتثال

- يجب ألا تكشف سجلات DNS الداخلية عن بيانات حساسة أو سرية.
- يجب أن تتبع الموارد المرتبطة بسجلات DNS الداخلية مبدأ الحد الأدنى من الامتيازات، مما يضمن اقتصار الوصول على المستخدمين أو الأنظمة المخولة فقط.
- يجب أن تتوافق جميع سجلات DNS المنشورة مع سياسات تقسيم الشبكات والجدران النارية للجامعة.

6. المراجعة الدورية

- يجب مراجعة جميع سجلات DNS الداخلية **سنوياً** لضمان:
  - استمرار الحاجة إليها وتشغيلها.
  - عدم تسببها في أي مخاطر أمنية.
  - توافقها مع السياسات المحدثة للشبكات وتقنية المعلومات.

7. الأدوار والمسؤوليات

- **القسم مقدم الطلب:**
  - ضمان أن السجل المطلوب ضروري وتقديم معلومات دقيقة ومحدثة.
  - إخطار قسم تقنية المعلومات إذا لم تعد الحاجة للسجل قائمة.
- **قسم الشبكات والأمن التقني:**
  - مراجعة واعتماد أو رفض طلبات DNS الداخلية بناءً على معايير الأمان والتشغيل.
  - الاحتفاظ بسجل شامل لجميع سجلات DNS الداخلية.
  - إجراء مراجعات دورية للتأكد من الامتثال الكامل.

8. رفض الطلب أو إلغاء السجل

- يمكن رفض طلبات DNS إذا:
  - لم تكن هناك حاجة تشغيلية مبررة.
  - تسببت في تعارض مع سجلات أخرى.
  - انتهكت سياسات الأمان أو الامتثال.
- يمكن إلغاء السجلات المنشورة إذا أصبحت غير ضرورية أو غير آمنة أو غير متوافقة مع السياسات المحدثة.

9. إدارة الحوادث

- يجب الإبلاغ فوراً عن أي تغيير غير مصرح به أو استخدام غير صحيح لسجلات DNS الداخلية إلى **فريق الأمن التقني**.
- سيقوم قسم الخوادم والتخزين بالتحقق واتخاذ الإجراءات اللازمة لتصحيح السجل أو تعطيله إذا لزم الأمر.

الامتثال

- يجب أن تتوافق جميع طلبات DNS الداخلية والنشاطات ذات الصلة مع:
  - **سياسات تقنية المعلومات والأمن السيراني الخاصة بالجامعة**.
  - القوانين واللوائح المحلية والدولية ذات الصلة.
- قد يؤدي عدم الامتثال إلى اتخاذ إجراءات تأديبية أو قيود على الوصول إلى الخدمات التقنية.

المراجعة والتحديثات

ستتم مراجعة هذه السياسة سنوياً أو عند حدوث تغييرات كبيرة في البنية التحتية أو متطلبات الأمان للجامعة.

م	الاسم	المنصب	التاريخ	التوقيع
1	م.أيمن محمد الغامدي	مدير إدارة البنية التحتية	2024/08/12	
2				
3				