جامعة دهوك

مديرية تكنولوجيا المعلومات (DOIT)

اسم السياسة:

إدارة المعلومات وأمن البيانات

رقم السياسة: UOD-POL-DOIT-021

مكتب الإصدار: DOIT,UPLO

الإصدار رقم.: 01

تاريخ الإصدار: 24/4/2025

تاريخ الإصدار الأصلي: 10/7/2024

اسم السياسة: إدارة المعلومات وأمن البيانات

غرض السياسة

تهدف هذه السياسة إلى حماية أصول المعلومات وأنظمة التكنولوجيا في جامعة دهوك من الوصول غير المصرح به، أو التعديل، أو الفقدان، أو الكشف. وتهدف إلى ضمان سرية البيانات وسلامتها وتوافرها، وذلك بالامتثال لسياسات الجامعة والمعايير التنظيمية ذات الصلة.
الجامعة توفر البنية التحتية الرقمية التي تشمل مجموعة متنوعة من الأنظمة الإلكترونية المؤسسية، وخدمات الحوسبة، والشبكات، وقواعد البيانات، وأنظمة الإدارة، وغيرها من الموارد (يشار إليها عمومًا باسم "موارد جامعة دهوك"). صُممت هذه الموارد لمساعدة أعضاء المجتمع الأكاديمي على النجاح في مساعيهم الأكاديمية. تضمن جامعة دهوك بيئة تشغيل تكنولوجيا معلومات آمنة ومأمونة لجميع أعضاء المجتمع الجامعي.

المكتب المسؤول

المديرية من تكنولوجيا المعلومات (يجب)نائب الرئيس للشؤون علمية،ورئيس في الجامعة.

المدير التنفيذي المسؤول

نائب الرئيس للشؤون الأكاديمية.

تاريخ السياسة

- تاريخ الموافقة الدائمة:
- تاريخ التعديلات: 24/04/2025

ينطبق على:

تنطبق هذه السياسة على الأكاديميين والموظفين والطلاب والهيئات الرسمية التابعة للجامعة وأي أفراد آخرين الذين يستخدمون موارد المعلومات الإلكترونية الخاصة بالجامعة أو الذين يستخدمون موارد المعلومات

اسم السياسة: إدارة المعلومات وأمن البيانات

الإلكترونية الخاصة لإجراء البحوث الجامعية ويشمل جميع الوحدات داخل حرم الجامعة أو تحت إشرافها الإداري، بما في ذلك مكتب سياسات الجامعة (UPLO) ومديرية تكنولوجيا المعلومات (DOIT).

بيان السياسة

لا يجوز نقل حقوق الوصول الفردية أو تأجيرها أو مشاركتها أو إتاحتها بأي شكل آخر أطراف ثالثةيقتصر الوصول إلى مصادر المعلومات المقيدة على أولئك الذين لديهم الترخيص الجامعي اللازم فقط.
المستخدمون مسؤولون عن أي أنشطة تحدث أثناء استخدام موارد المعلومات المخصصة لهم، وعليهم استخدام هذه الموارد بالطريقة المقصودة. نشجع الموظفين على استخدام موارد الجامعة للقيام بما يلي:جامعة عمل.بصرف النظر عن حقوق الوصول المعتمدة،لا يجوز الكشف عن سجلات معلومات الجامعة إلا استجابة لأمر من المحكمة أو حسبما يقتضيه القانون.

التعاريف:

- **الأصول المعلوماتية:** البيانات والسجلات والمحتوى الآخر الذي يتم تخزينه أو نقله أو استخدامه من خلال الأنظمة التي تديرها الجامعة، بما في ذلك بيانات البحث، وسجلات الطلاب، والمعلومات الإدارية، وتفاصيل أعضاء هيئة التدريس، ومعلومات الموظفين، والبيانات المالية.

- **أنظمة جامعة دهوك:**تتبع إدارة المعلومات في جامعة دهوك نهجًا منظمًا لتنظيم البيانات وتأمينها وصيانتها طوال دورة حياتها. تشرف مديرية تكنولوجيا المعلومات على الأنظمة الرقمية الحيوية، بما في ذلك **تخطيط موارد المؤسسات نظام،نظام إدارة البريد الإلكتروني،جامعة موقع إلكتروني،ضمان الجودة، التعلم الإلكتروني (مودل),مساحة عمل جوجل, بوابة جامعة دهوك,نظام وزارة المالية في إقليم كردستان (KMFS)،إدارة بيانات كاميرات المراقبة، مركز البيانات،من بين أمور أخرى.**

لضمان أمن البيانات، تستخدم جامعة دهوك حلولاً تكنولوجية متطورة وسياسات صارمة لحماية المعلومات الحساسة من الوصول غير المصرح به أو الاختراقات أو الضياع. وتساعد ضوابط الوصول

الواضحة، والعمليات الموثقة جيدًا، والمراقبة المستمرة في الحفاظ على سلامة بيانات الجامعة الأساسية وسريتها وتوافرها.بالإضافة إلى ذلك، تعمل برامج التوعية الشاملة على تثقيف الموظفين والطلاب حول أدوارهم في تأمين معلومات الجامعة.

- **الأطراف الثالثة:**أي فرد أو منظمة/جهة ليس لديها حقوق الوصول والموافقة من القيادة العليا للجامعة.

تصنيف البيانات

يتضمن تصنيف البيانات تقسيمها إلى مجموعات محددة بناءً على حساسيتها وأهميتها ومستوى الحماية المطلوب. الهدف هو ضمان إدارة البيانات وحمايتها بشكل مناسب. تشمل التصنيفات الشائعة ما يلي:

- **مؤتمن:**الوصول مقيد،البيانات الحساسة التي قد تسبب ضررًا إذا تم الكشف عنها لجهات غير مصرح لها، مثل المعلومات الشخصية، والمعلومات المالية، والبيانات الأكاديمية والمؤسسية، والوثائق الحكومية والقانونية.
- **للاستخدام الداخلي فقط:**البيانات المستخدمة داخل الجامعة وغير المخصصة للاستخدام العام، مثل البيانات التنظيمية والإدارية، وبيانات الموارد البشرية، والبيانات الأكاديمية والبحثية، وغيرها.
- **عام:**المعلومات المخصصة للوصول العام، بما في ذلك معلومات الجامعة العامة والمحتوى الأكاديمي غير الحساس.مثل أوراق البحث العامة، والإعلانات الجامعية العامة، والمواقع الإلكترونية المتاحة للعامة، وغيرها.
- **مقيد بيانات:**المعلومات شديدة الحساسية التي تتطلب أعلى مستوى من الحماية، مثل البيانات الجامعية والأكاديمية، وبيانات تكنولوجيا المعلومات والنظام، وبيانات الموارد البشرية والموظفين، والبيانات التشغيلية والاستراتيجية، وغيرها.

اسم السياسة: إدارة المعلومات وأمن البيانات

مسؤوليات الجامعة

وبما أن موارد المعلومات الإلكترونية الخاصة بالجامعة مملوكة ومدارة من قبل القطاع العام في حكومة إقليم كردستان،وتقع على عاتق الجامعة مسؤولية مراقبة وضمان الاستخدام السليم لها.في ظل تعزيز ثقافة الثقة، يجوز للجامعة مراقبة الأنظمة للتحقق من سوء الاستخدام. وهي مسؤولة عن تدقيق جميع أنظمة تكنولوجيا المعلومات والاتصالات وأصول المعلومات لضمان الامتثال للسياسات. تضمن الجامعة سرية وخصوصية الاتصالات والبيانات؛ ومع ذلك، في حال صدور أمر قضائي أو طلب إداري مُصرّح به من الجامعة، تحتفظ بحقها في فحص البيانات وفقًا للقوانين واللوائح الإقليمية.

1. مسؤوليات إدارة المعلومات

مديرية وزارة تكنولوجيا المعلومات مسؤولة عن تقديم المشورة بشأن الأنظمة الجديدة والمقترحة وفقًا لـQP-MUST-01- تنفيذ وصيانة أنظمة إدارة المعلومات التي تضمن التخزين السليم وتصنيف وأمن بيانات الجامعة.الأنظمة المذكورة أعلاه مثل مركز البيانات، وERP، وeUMS ... إلخ

2. إدارة الوصول

إدارة الوصول هي عملية التحكم في وصول المستخدم إلى موارد جامعة دلهي وإدارتها، مثل موقع جامعة دلهي الإلكتروني، وبوابة جامعة دلهي، وكاميرات المراقبة،المالية الإلكترونية الأنظمة.مصفوفة التحكم في الوصول إلى أنظمة UoD يوضح الدور/المسؤوليات الفردية لكل مستخدم ضمن أنظمة المؤسسة.
في حال تغيير أي عضو من أعضاء هيئة التدريس لمهامه أو ترك الجامعة، يجب إبلاغ مدير تكنولوجيا المعلومات لتحديث صلاحيات الوصول على الفور.يجب إلغاء الامتيازات برسالة رسمية.
يجب على أي عضو من أعضاء هيئة التدريس المسؤول عن أنظمة أو معلومات جامعة دهوك المقيدة التوقيع على اتفاقية سرية الجامعة.

3.الاستجابة للحوادث والإبلاغ عنها

في حال حدوث اختراق للبيانات أو الاشتباه في إساءة استخدام موارد معلومات الجامعة، يجب على المستخدمين الإبلاغ فورًا عن الحادثة عبر قنوات الإبلاغ المخصصة. يمكن الإبلاغ عن الحوادث عبر أرقام الهواتف الرسمية (واتساب، مجموعات فايبر)، والبريد الإلكتروني.IT@uod.ac.

مسؤوليات الموظف

جميع موظفي جامعة دهوك مسؤولون عن حماية المعلومات المتعلقة بعملهم والحفاظ على سرية البيانات الحساسة التي يتم الوصول إليها أثناء عملهم. تمتد هذه المسؤولية لحماية معلومات الجامعة إلى ما بعد انتهاء الخدمة الفعلية، وتستمر بعد انتهاء الخدمة، بما في ذلك التقاعد. يجب على الموظفين عدم الإفصاح عن أي معلومات سرية حصلوا عليها أثناء عملهم، أو مشاركتها، أو إساءة استخدامها.إن عدم الامتثال لهذه المسؤوليات سيعرض الأفراد للمساءلة القانونية بموجب المادتين 327 و 437 من قانون العقوبات العراقي رقم 111 لسنة 1969.

مسؤوليات المستخدم

1. الاستخدام المناسب للموارد

يُتوقع من مستخدمي أنظمة جامعة دهوك استخدام موارد المعلومات بمسؤولية، بما يتوافق مع أهداف الجامعة. يُمنع منعًا باتًا مشاركة امتيازات الوصول، ويُحظر تمامًا محاولة الوصول إلى الأنظمة المحظورة دون تصريح. قد يُعرّض إساءة استخدام موارد المعلومات لإجراءات تأديبية.

2. حماية البيانات والامتثال

- يجب على جميع المستخدمين احترام سرية المعلومات الحساسة، بما في ذلك سجلات الطلاب، والبيانات المالية، ومعلومات حسابات الموظفين (الأكاديمية والإدارية)، والمعلومات الشخصية القابلة للتعريف (PII)، ورسائل البريد الإلكتروني المؤسسية، وحسابات الملكية الفكرية.

- إن المشاركة أو التعديل أو التوزيع غير المصرح به لهذه المعلومات سيؤدي إلى عواقب وخيمة، بما في ذلك التبعات القانونية بموجب قوانين حماية البيانات (سيتم الرجوع إلى المواد 327 و 437 من قانون العقوبات العراقي رقم 111 (1969) أو التحديثات وتنفيذها.)

3. الاستخدام الشخصي

- يُسمح بالاستخدام الشخصي المحدود لأنظمة جامعة ديار بكر، شريطة ألا يتعارض ذلك مع العمليات، أو يتسبب في تكاليف للجامعة، أو ينتهك سياسات جامعة ديار بكر.
- استخدام الموارد لتحقيق مكاسب مالية شخصية،يُحظر القيام بالحملات السياسية أو أي أنشطة خارجية غير مصرح بها.

تدابير أمن البيانات

1. **التحكم في الوصول:**يجب أن تخضع جميع عمليات الوصول إلى موارد المعلومات الخاصة بالجامعة لنظام تحكم صارم في الوصول**مصفوفة** الذي يتطلب تحديد هوية المستخدم والمصادقة عليه.
2. **إدارة كلمة المرور:**يُنصح جميع المستخدمين بتحديث كلمات مرورهم بانتظام وفقًا لإرشادات الأمان. عند مغادرة أي مستخدم للجامعة، يجب إلغاء حساباته وصلاحيات وصوله فورًا. ومع ذلك، في بعض الحالات، كما هو موضح في **سياسة مشاركة الخريجين أو** في ظروف محددة أخرى حيث يعتبر الوصول المستمر ضروريًا، قد يتم منح وصول محدود إلى الحساب لفترة محددة.
3. **النسخ الاحتياطي والاسترداد:**كل مالك النظام يجب الحفاظ على أنظمة النسخ الاحتياطي القوية التي تضمن استرداد البيانات في حالة فشل النظام أو الخروقات أو الحوادث الأخرى.
4. **تشفير البيانات:**يجب تشفير البيانات أثناء السكون والنقل باستخدام SSL/TLS وبروتوكولات أخرى.
5. **أمن الشبكات:**يجب تطبيق جدران الحماية الحديثة، وأنظمة الكشف عن التسلل/منع التسلل، وتقسيم الشبكة لتأمين حركة المرور.
6. **الأمن المادي:**تقييد الوصول المادي إلى الخوادم والأجهزة الحساسة.
7. **أمان نقطة النهاية:**قم بتثبيت برامج مكافحة الفيروسات/مكافحة البرامج الضارة، وتأكد من أن جميع الأجهزة تحتوي على برامج وتحديثات محدثة.

8. **إدارة المخاطر:** تتضمن إدارة المخاطر تحديد المخاطر وتقييمها والتخفيف منها لضمان سلامة البيانات وسريتها وتوافرها. كما أنها تساعد على حماية البيانات من التهديدات، مثل الوصول غير المصرح به، واختراق البيانات، والهجمات الإلكترونية.

أرشفة السجلات

ولضمان حماية السجلات الإدارية وإمكانية الوصول إليها وإدارتها بشكل سليم، يجب اتباع الإرشادات التالية عند أرشفة الملفات:

- **طرق التخزين**

يجب أرشفة السجلات الإدارية بشكل آمن باستخدام أحد أو كلا الأمرين التاليين:

- منصة تخزين سحابية آمنة (مع عناصر تحكم في الوصول والتشفير المناسبين)
- جهاز تخزين خارجي مخصص.

- **تنظيم الملفات**

- يجب أن تكون جميع الملفات واضحة**مُرمَّز**(على سبيل المثال، حسب القسم أو نوع المستند أو رقم المرجع)
- يجب أن يكون كل ملف مؤرخة للإشارة إلى وقت إنشائه أو آخر تعديل له
- متسقة بنية **المجلد ينبغي** استخدامها لسهولة التنقل والاسترجاع

- **إمكانية الوصول**

- يجب تنظيم الملفات المؤرشفة بطريقة تجعلها سهل **الوصول من** قبل الموظفين المعتمدين عند الحاجة
- يجب إجراء فحوصات منتظمة للتأكد من إمكانية الوصول إلى جميع الملفات ووظيفتها

❖ **الأمن والامتثال**

- يجب أن تتوافق طرق التخزين مع قوانين **حماية البيانات وسياسات الجامعة**
- يجب تخزين جميع الملفات الرقمية باستخدام الأنظمة التي توفر التشفير **والنسخ الاحتياطي والتحكم في الإصدارات**
- القرص الصلب الخارجي يجب أن تبقى محركات الأقراص في مواقع **آمنة ومقيدة الوصول**

❖ **الصيانة والتحديثات**

- يجب أن تكون الأرشيفات سيتم **تحديث البيانات وأرشفتها بانتظام وفقًا لهذه السياسة**
- يجب تحديد الملفات القديمة أو المكررة تم **إزالتها بأمان أو أرشفتها بشكل منفصل**

باتباع هذه الخطوات، تضمن جامعة دهوك حفظ السجلات الإدارية المهمة بشكل آمن، وتنظيمها بشكل جيد، وإتاحتها للرجوع إليها مستقبلًا. تُعد هذه الممارسة أساسيةً للحفاظ على أمن المعلومات، ودعم إدارة البيانات بكفاءة، والحفاظ على المعرفة المؤسسية.

الامتثال لقانون حكومة إقليم كردستان

تلتزم جامعة دهوك بالقوانين والأنظمة التي وضعتها حكومة إقليم كردستان والعراق لضمان إدارة المعلومات وأمن البيانات.سيتم الرجوع إلى الأطر القانونية التالية في حالة انتهاك السياسة:

اسم السياسة: إدارة المعلومات وأمن البيانات

1. **حماية حقوق النشر**

بموجب قانون حقوق الطبع والنشر رقم 17 لسنة 2012 لحكومة إقليم كردستان، سيتم تطبيق المادتين 36 و37 في حالات انتهاك حقوق الطبع والنشر المتعلقة بالمحتوى المملوك للجامعة أو التابع لها.

2. **إساءة استخدام أجهزة الاتصالات**

يخضع أي استخدام غير سليم للإنترنت أو الهواتف المحمولة أو الأجهزة الإلكترونية لقانون حكومة إقليم كردستان رقم 6 (2008)، "قانون منع إساءة استخدام أجهزة الاتصالات". وتُطبق المواد من 1 إلى 8 في حالات إساءة الاستخدام داخل شبكة الجامعة وأنظمتها.

3. **الحماية من الكشف غير المصرح به عن البيانات**

بالنسبة للقضايا المتعلقة بالإفصاح غير المصرح به عن البيانات الحساسة أو السرية، سيتم الرجوع إلى المادتين 327 و 437 من قانون العقوبات العراقي رقم 111 (1969) وتطبيقهما.

4. **الإجراءات التأديبية بموجب القانون رقم 14 (1991)**وبالإضافة إلى ما سبق، فإن الموظفين الذين يخالفون هذه السياسة قد يواجهون إجراءات تأديبية وفقاً للمادة 8 من القانون رقم 14 (1991)، المعدل.

بيان إخلاء المسؤولية عن السياسة

أي انحراف عن السياسات أو الإجراءات أو الإرشادات المعتمدة والمعلنة على موقع uplo.uod.ac من قِبل مكتب سياسات الجامعة (UPLO)، لا يجوز القيام به إلا بالتعاون بين UPLO والجهة الطالبة، مع إتاحة وقت كافٍ لإجراء تحليل مناسب للمخاطر من قِبل SCSP، والتوثيق، وعرضه على مجلس الجامعة للموافقة النهائية. قد يُعاقَب عدم الالتزام بالسياسات الرسمية المكتوبة لـ UPLO بعقوبات من الجامعة.

السياسات أو الإجراءات أو المبادئ التوجيهية ذات الصلة

- سرية الجامعة الاتفاقية.
- مصفوفة التحكم في الوصول إلى أنظمة UoD

- مصفوفة تصنيف البيانات
- **سياسة مشاركة الخريجين**
- QP-MUST-01
- يمكن الوصول إلى UPLO علىأعلى.uod.ac. أرسل الأسئلة أو طلبات الموافقة إلىuplo.office@uod.ac

الملحق

- الترجمة الكردية
- الترجمة العربية