

**2028 المراجعة: نيسان**

## **سياسة وإجراءات الاستخدام المقبول وتطبيق تكنولوجيا المعلومات والمساءلة**

### **1.0 الغرض**

1.1 وضع إرشادات للاستخدام الأخلاقي والمناسب لموارد تكنولوجيا المعلومات لضمان وصول آمن وموثوق وعادل لمجتمع الجامعة الأمريكية في بغداد.

### **2.0 النطاق**

2.1 تُطبق هذه السياسة على جميع أعضاء مجتمع الجامعة الأمريكية في بغداد، بمن فيهم الطلبة والموظفون وأعضاء هيئة التدريس والمتعاقدون والزوار المصرح لهم الذين يستخدمون موارد تكنولوجيا المعلومات في الجامعة

### **3.0 التعاريف**

3.1 الاستخدام المقبول - يشير إلى الاستخدام السليم والأخلاقي والقانوني لموارد تكنولوجيا المعلومات في الجامعة الأمريكية في بغداد ، بما يتماشى مع أهداف الجامعة وسياساتها ولوائحها القانونية. ويشمل ذلك دعم الأنشطة الإدارية والبحثية والتعليمية في الجامعة بخدمات تكنولوجيا المعلومات، وأدواتها، وبرامجها، وبياناتها. وتُعدّ الأنشطة التي تتعارض مع حقوق المستخدمين الآخرين ودخولهم إليها، والتي تُعدّ غير قانونية أو تُعطل الشبكة، أمثلة على الاستخدام غير المقبول.

3.2 المستخدم - يشير إلى أي فرد مُصرّح له بالدخول إلى موارد تكنولوجيا المعلومات في الجامعة الأمريكية في بغداد واستخدامها. ويشمل ذلك، على سبيل المثال لا الحصر، الطلبة والموظفين وأعضاء هيئة التدريس والمتعاقدين والزوار وأي موظفين أو ضيوف مُصرّح لهم من جهات خارجية مُنحوا حق الدخول إلى الموارد الرقمية للجامعة.

3.3 موارد تكنولوجيا المعلومات - تشمل جميع موارد الشبكات والحوسبة والاتصالات في الجامعة، بما في ذلك على سبيل المثال لا الحصر:

- الأجهزة (أجهزة الحاسوب المكتبية، والمحمولة، والخوادم، والطابعات، والماسحات الضوئية، وغيرها).
- البرمجيات (التطبيقات المرخصة، والأنظمة الخاصة، والأدوات مفتوحة المصدر، وغيرها).
- الشبكات (الإنترنت، والإنترانت، وخدمات البريد الإلكتروني، والخدمات السحابية، وغيرها).
- أنظمة وأجهزة تخزين البيانات (الخوادم، ومحركات الأقراص الخارجية، والتخزين السحابي).
- أنظمة الاتصالات (الهواتف، ومؤتمرات الفيديو، وغيرها).

3.4 بيانات الجامعة - تشير إلى أي بيانات تملكها الجامعة أو تديرها أو تنشئها. ويشمل ذلك سجلات الطلبة، ومعلومات الموظفين، وبيانات الأبحاث، والبيانات المالية، والبرامج أو المعلومات الخاصة، وغيرها من البيانات المستخدمة في تشغيل وإدارة الجامعة. يجب التعامل مع بيانات الجامعة بسرية تامة ما لم يُنص صراحةً على خلاف ذلك، كما يُحظر الدخول غير المصرح به إلى بيانات الجامعة أو إساءة استخدامها.

3.5 الدخول غير المصرح به - يُقصد به الدخول إلى أنظمة أو موارد تكنولوجيا المعلومات الخاصة بالجامعة الأمريكية في بغداد من دون إذن، إما بمحاولة تجاوز ضوابط الأمان أو باستخدام بيانات اعتماد شخص آخر. يُعدّ الدخول غير المصرح به انتهاكاً لسياسات الجامعة الأمريكية في بغداد، ويُعرّض مرتكبه لإجراءات تأديبية، بما في ذلك تعليق الصلاحيات والعواقب القانونية.

3.6 المعلومات السرية - تشمل أي بيانات غير معلنة تتعلق بعمليات الجامعة، وأنشطتها الأكاديمية، وأبحاثها، وعملياتها الإدارية. وتشمل المعلومات الشخصية عن الطلبة، والموظفين، وأعضاء هيئة التدريس، وبيانات الأبحاث، والسجلات المالية، وحقوق الملكية الفكرية، وأي معلومات أخرى يجب حمايتها بموجب القانون أو سياسة الجامعة.

### 3.7 قسم تكنولوجيا المعلومات - يُقصد به القسم المسؤول داخل

الجامعة عن إدارة وصيانة وتأمين البنية التحتية لتكنولوجيا المعلومات وخدماتها. كما أنه مسؤول عن مراقبة الامتثال للسياسات، وتقديم الدعم في الحالات الفنية، وضمان استخدام موارد تكنولوجيا المعلومات في الجامعة بفعالية وأمان.

## 4.0 السياسة

### أهمية الاستفادة من موارد تكنولوجيا المعلومات

4.1 يجب على جميع أعضاء مجتمع الجامعة الأمريكية في بغداد الالتزام بسياسات الجامعة المتعلقة باستخدام تكنولوجيا المعلومات. أي إجراء يخالف هذه السياسات سيترتب عليه عواقب.

4.2 يجب على المستخدمين مراجعة سياسات الجامعة ذات الصلة لضمان الاستخدام الأمثل لموارد تكنولوجيا المعلومات.

### الامتثال والمبادئ التوجيهية لاستخدام موارد تكنولوجيا المعلومات

4.3 يُعد الامتثال لجميع السياسات والإجراءات والقوانين المتعلقة بالدخول إلى موارد تكنولوجيا المعلومات في الجامعة الأمريكية في بغداد واستخدامها أمرًا بالغ الأهمية. ولضمان سلامة وأمن موارد الجامعة، يجب على الجميع قراءة هذه القواعد وفهمها بدقة.

4.4 من الضروري أن يتبع الجميع هذه القواعد لضمان سلاسة الإجراءات وفعاليتها. ويجب على أي زائر يُمنح حق الدخول إلى موارد تكنولوجيا المعلومات الالتزام بدقة بالقواعد التي تحكم المستخدمين العاديين.

4.5 لأي استفسارات تتعلق بالدخول المصرح به أو الاستخدام أو أي أمور أخرى خارج نطاق سياسات وقواعد ومعايير وإرشادات وإجراءات الجامعة، من الضروري مراجعة مسؤولي النظام أو أمناء البيانات للاستفسار.

4.6 تقع على عاتق المستخدم مسؤولية حماية جهاز الحاسوب المكتبي أو المحمول، والمعلومات المخزنة عليه من التلف والفقْدان والسرقة.

4.7 في حالة تلف أو سرقة أو فقْدان جهاز حاسوب محمول أو محمول، من الضروري إبلاغ خدمات تكنولوجيا المعلومات بالجامعة على الفور.

4.8 يُنصح المستخدم بعدم ترك جهازه المحمول أو هاتفه المحمول من دون مراقبة في الأماكن العامة.

4.9 يجب على المستخدمين حماية شاشات القفل بكلمات مرور فورًا بعد الانتهاء من استخدام الحاسوب المحمول أو الحاسوب المكتبي أو الأجهزة المحمولة.

4.10 باعتبارك مستخدمًا لموارد تكنولوجيا المعلومات في الجامعة الأمريكية في بغداد، فإن من مسؤوليتك ضمان محتوى اتصالاتك الشخصية. لا تتحمل الجامعة الأمريكية في بغداد أية مسؤولية عن دخول غير مصرح به أو شخصي لمواردها من قبل المستخدمين.

4.11 يجب على المستخدمين أن يكونوا على علم بأننا نعطي الأولوية للأمان ونضمن حماية كاملة لبيانات المستخدم. من المهم اتخاذ التدابير الوقائية. لا تضمن الجامعة الأمريكية في بغداد الأمان والخصوصية المطلقة. يجب على المستخدمين اتباع الإجراءات الأمنية المناسبة.

4.12 من الضروري أن يمتنع المستخدم عن إجراء أي تعديلات على الوظائف الإدارية على الحاسوب المحمول، الذي يشمل نظام التشغيل أو كلمة مرور مدير النظام. يُنصح بشدة ألا يقوم المستخدمون بتوصيل أجهزتهم الشخصية بشبكة الجامعة.

4.13 إذا ما شهدت على أي انتهاكات لهذه السياسة، من الضروري الإبلاغ عنها إلى السلطات الإدارية المناسبة وإلى قسم تكنولوجيا المعلومات.

### الوصول المشترك إلى موارد تكنولوجيا المعلومات

4.14 تُعد أجهزة الحاسوب والشبكات وأنظمة المعلومات الإلكترونية أساسية لتحقيق رسالة الجامعة في التعليم والبحث والخدمة. ولذلك، تُتيح الجامعة لأعضاء المجتمع الوصول المشترك إلى هذه الموارد.

### الوصول إلى موارد تكنولوجيا المعلومات

#### 4.15 تُخصص موارد تكنولوجيا المعلومات والخدمات ذات

الصلة للموظفين والطلبة بناءً على حالة عضويتهم التي تحددها مكاتب إدارة الموارد البشرية وإدارة التسجيل في الجامعة الأمريكية في بغداد.

#### حقوق الوصول واستخدام البرامج

4.16 يقوم رئيس وحدة الموظف أو الطالب بتحديد حقوق دخول لأعضاء هيئة التدريس الزائرين والمستخدمين بالساعة والمتعاقدين مع الجامعة لفترات طويلة.

4.17 يُمنع منعاً باتاً، في أي ظرف من الظروف، على مشغلي الحاسوب، أو الخوادم، أو أجهزة تكنولوجيا المعلومات، أو الخدمات ضمن شبكة الجامعة الأمريكية في بغداد بمنح الدخول إلى الحسابات على مواردهم وخدمات تكنولوجيا المعلومات من دون الموافقات المناسبة.

4.18 منع تنصيب البرامج غير المعترف بها والتشفير غير المرخص.

4.19 يُمنع استخدام برامج فحص الشبكة، ونسخ البرامج، وتوزيعها أو اعتراض المعلومات أو اغتنام كلمات المرور بدون إذن محدد. يجب دائماً أخذ شروط الترخيص لأي برنامج بالحسبان. تُستخدم البرامج على وفق القوانين الفيدرالية أو المحلية في البلد، بما في ذلك قوانين حقوق الطبع، والنشر، والمعاملات التجارية، والبراءات.

#### الاستخدام المسؤول لموارد الجامعة

4.20 موارد الجامعة قيمة للغاية ويجب إدارتها بمسؤولية قصوى للحفاظ على سلامتها وأمنها وتوافرها للأنشطة التعليمية والتجارية المناسبة. تتوقع من المستخدمين المصرح لهم استخدام هذه الموارد بكفاءة وفعالية ومسؤولية. لن يتم التسامح مع أي انحراف عن هذه التوقعات.

4.21 تقوم الكليات والأقسام والوحدات الإدارية بمواءمة سياسات استخدام التكنولوجيا الخاصة بها مع سياسات الجامعة وأي سياسات أخرى لاستخدام التكنولوجيا ذات الصلة. يعد الامتثال للسياسات المعمول بها إلزامياً لجميع الاستخدامات الشخصية لموارد تكنولوجيا المعلومات بالجامعة. يجب ألا يعيق هذا الاستخدام الموظفين عن أداء واجباتهم الجامعية أو ينتهك القانون أو يؤثر سلباً على الأنشطة المتعلقة بمهمة الجامعة.

4.22 تعطى الأولوية لاستخدام موارد تكنولوجيا المعلومات للأنشطة المتعلقة بمهام الجامعة في التدريس، والتعلم، والبحث، والتوعية. موارد الحاسوب والشبكة في الجامعة محدودة السعة والطلب عليها مرتفع. للحفاظ على قدرة موارد تكنولوجيا المعلومات لجميع المستخدمين، يجب على الأفراد ممارسة ضبط النفس عند استخدام الحوسبة والموارد. قد يُطلب من المستخدمين الأفراد إيقاف أو الحد من الاستخدام غير ذي الأولوية لموارد تكنولوجيا المعلومات، مثل الخدمات غير الأكاديمية وغير المتعلقة بمصالح الجامعة.

4.23 الاستخدام غير المناسب أو الضار لأنظمة تكنولوجيا المعلومات، يشمل:

- إنشاء خاصية مشاركة الملفات التي تتم فيها مشاركة الملكية الفكرية المحمية بشكل غير قانوني.
- إدخال برامج ضارة عمداً في الشبكة أو الخادم (على سبيل المثال، الفيروسات والفيروسات المتنقلة وأحصنة طروادة وقنابل البريد الإلكتروني وما إلى ذلك).
- الاستخدام غير المناسب أو مشاركة امتيازات أو موارد تكنولوجيا المعلومات المعتمدة من الجامعة. وتغيير كلمة مرور مستخدم آخر أو دخوله أو أدوناته.
- استخدام أحد أصول الحوسبة في الجامعة الأمريكية في بغداد للمشاركة بنشاط في عرض أو الحصول على أو إرسال مواد تنتهك سياسة أو قوانين التحرش الجنسي أو النشاط غير القانوني.
- استخدام أحد أصول الحوسبة في الجامعة الأمريكية في بغداد لأي غرض خاص أو لتحقيق مكاسب شخصية.

4.24 يجوز للجامعة تعطيل الخدمة بشكل مؤقت لفرد أو جهاز حاسوب، عند حدوث إساءة استخدام واضحة لمرافق أو شبكات الحوسبة الجامعية، وقد تكون إساءة الاستخدام:

- شكوى.
- انتهاك للقانون الجنائي.

- امكان التسبب في تداخل كبير مع مرافق أو خدمات الجامعة.
  - قد يتسبب في أضرار جسيمة لشخص آخر.
  - قد ينتج عنه مسؤولية تجاه الجامعة.
- 4.24.1 يؤمن الاتصال بالشخص المسؤول عن الحساب أو الجهاز قبل تعطيل الخدمة ما لم تحظر سلطات إنفاذ القانون ذلك، أو يقرر موظفو خدمات تكنولوجيا المعلومات والخدمات أن الإجراء الفوري ضروري للحفاظ على سلامة شبكة الجامعة. على أي حال، يجب إبلاغ المستخدم في أقرب وقت ممكن حتى يتمكن من تقديم أسباب كتابية لعدم اعتبار استخدامه انتهاكاً أو أن لديه إدناً بالاستخدام.
- 4.24.2 قد يتم إصدار تحذيرات للمستخدمين، وقد يُطلب منهم الموافقة على شروط استمرار الخدمة، أو قد يتم تعليق امتيازاتهم أو رفضها إذا: قررت هيئة تأديب الموظفين بعد سماع تفسير المستخدم للانتهاك المزعم أن المستخدم قد انخرط في انتهاك للقانون.
- 4.24.3 يمكن إحالة انتهاكات سياسة الاستخدام المقبول لموارد تكنولوجيا المعلومات في الجامعة لاتخاذ إجراءات تأديبية. قد تقوم الجامعة بفرض رسوم لتعويض أضرار الحادث.

## 5.0 الإجراءات

### إنفاذ السياسة

- 5.1 يتولى قسم تكنولوجيا المعلومات في الجامعة الأمريكية في بغداد مسؤولية إنفاذ هذه السياسة. ويشمل ذلك مراقبة الامتثال، والتحقيق في الانتهاكات المحتملة، واتخاذ الإجراءات اللازمة ضد كل من لا يلتزم بالإرشادات المعمول بها.
- 5.2 يقوم قسم تكنولوجيا المعلومات بمراقبة وتدقيق استخدام موارد تكنولوجيا المعلومات بشكل نشط للكشف عن الاستخدام غير المصرح به أو غير السليم، ومعالجة أي عدم امتثال على الفور.

### مسؤولية الأفراد

- 5.3 يتحمل جميع مستخدمي موارد تكنولوجيا المعلومات في الجامعة الأمريكية في بغداد، بمن فيهم الطلبة وأعضاء هيئة التدريس والموظفون، مسؤولية ضمان الاستخدام السليم والمحافظة على الأجهزة والبرامج والمنصات الرقمية التي توفرها الجامعة. كما يتعين على المستخدمين الإبلاغ فوراً عن أي نشاط مشبوه أو غير مصرح به قد يخالف هذه السياسة إلى قسم تكنولوجيا المعلومات.
- 5.4 يجب على المستخدمين أن يظلوا منتبهين لحماية أجهزتهم وأنظمتهم من الضياع أو السرقة أو التلف، والتأكد من استخدامها فقط للأغراض التي تتوافق مع مهمة وسياسات الجامعة الأمريكية في بغداد.

### الإجراءات التأديبية

- 5.5 تُواجه مخالفات هذه السياسة بإجراءات تأديبية. وتُحدد شدة الاجراء بناءً على طبيعة المخالفة وأي عوامل مخففة. قد تشمل الإجراءات التأديبية، على سبيل المثال لا الحصر، ما يأتي:
- إنذارات شفوية أو كتابية.
  - تعليق مؤقت لامتيازات تكنولوجيا المعلومات.
  - تعويض مالي عن الأضرار الناجمة عن المخالفة.
  - في حالات المخالفات الجسيمة، قد تُتخذ إجراءات أكثر جدية، مثل الفصل من المؤسسة أو اتخاذ إجراءات قانونية.
  - تُطبق الإجراءات التأديبية بعد إجراءات منظمة، تضمن منح الأفراد فرصة لشرح أفعالهم قبل اتخاذ القرار النهائي.
- 5.6 يجب على المستخدمين الامتناع عن المشاركة في أنشطة تنتهك سياسات الجامعة. يؤدي عدم الامتثال لهذه السياسة إلى اتخاذ إجراءات تأديبية على وفق قواعد السلوك في الجامعة وسياسات توظيف الموظفين وأعضاء هيئة التدريس.
- 5.7 تتبع الإجراءات التأديبية، عند فرضها، الإجراءات القانونية الواجبة، ويُبلغ المستخدمون بحقوقهم في تقديم تفسير أو دفاع بشأن الانتهاكات المزعومة.

5.8 في حالات الانتهاكات الجسيمة أو المتكررة، قد يُمنع المستخدمون بشكل دائم من استخدام موارد تكنولوجيا المعلومات في الجامعة، وقد تُتخذ إجراءات قانونية عند الضرورة.

#### **السياسات والوثائق ذات الصلة**

سياسة الاستخدام المقبول

سياسة قواعد السلوك

سياسة أمن تكنولوجيا المعلومات

سياسة خصوصية البيانات