التصنيف: إدارة المعلومات والتكنولوجيا

جهة الموافقة: الرئيس

الجهة المسؤولة: مساعد الرئيس للشؤون المالية والإدارية

الجهة المنفذة: قسم تكنولوجيا المعلومات

تاريخ بدء التنفيذ: أيّار 2025

المراجعة: نيسان 2028

سياسة وإجراءات معالجة البيانات والدخول إليها وتخزينها

1.0 الغرض

1.1 توفر هذه السياسة إرشادات واضحة عن الكيفية التي تدير فيها الجامعة الأمريكية في بغداد البيانات وتخزينها. وتهدف إلى حماية سرية البيانات وامنها وتوافرها منذ إنشائها إلى وقت عدم الحاجة إليها.

2.0 النطاق

2.1 تنطبق هذه السياسة على أي شخص يمكنه الدخول إلى البيانات أو التعامل معها أو عرضها أو تخزينها داخل البنية التحتية للجامعة الأمريكية في بغداد، وهذا يشمل الطلبة وأعضاء هيئة التدريس والموظفين وأي مقدمي خدمات تابعين لجهات خارجية.

2.2 تهدف هذه السياسة إلى ضمان حماية البيانات وسلامتها وإدارتها بكفاءة في الجامعة الأمريكية في بغداد. يُعدّ أمن البيانات أولوية، حيث وُضعت تدابير لحماية المعلومات الحساسة من الدخول غير المصرح به أو الكشف عنها. تحافظ الجامعة الأمريكية في بغداد على سلامة البيانات من خلال التحقق من دقة البيانات المخزنة واتساقها وموثوقيتها عبر عمليات مثل تصحيح الأخطاء والتحكم في الإصدارات. كما يُركّز على إمكانية الدخول إلى البيانات، مما يضمن سهولة استرجاع المستخدمين المصرح لهم للمعلومات، عادةً من خلال الفهرسة الفعالة.

2.3 لتحسين التخزين، تُطبّق الجامعة الأمريكية في بغداد إرشادات لإزالة البيانات المكررة، وضغط البيانات، والأرشفة بكفاءة، مما يُسهم في خفض التكاليف. تدعم هذه السياسة قابلية التوسع والمرونة من خلال اعتماد تقنيات تُواكب أحجام البيانات المتزايدة والاحتياجات المؤسسية المتطورة. بالإضافة إلى ذلك، تلتزم الجامعة الأمريكية في بغداد بمعايير المهنية للاحتفاظ بالبيانات والتخلص منها، مُحددةً مدة الاحتفاظ بالبيانات وكيفية التخلص منها بشكل آمن.

2.4 يُعزز التوحيد القياسي في جميع الأقسام من خلال استخدام صيغ وتسميات مشتركة، مما يُعزز التعاون وتبادل البيانات. جميع الممارسات متوافقة مع معايير الصناعة، وأفضل ممارسات الأمان، ومتطلبات الامتثال. تنطبق هذه السياسة على أي شخص يمكنه الدخول

2.5 إلى البيانات أو التعامل معها أو عرضها أو تخزينها داخل البنية التحتية للجامعة الأمريكية في بغداد، بما في ذلك الطلبة وأعضاء هيئة التدريس والموظفين ومقدمي الخدمات الخارجيين.

3.0 التعاريف

3.1 ضوابط الدخول - تدابير أمنية تنظم من يمكنه الدخول إلى البيانات ومستوى الدخول الذي يتمتع به، بناءً على المصادقة والتفويض وإدارة الامتيازات.

3.2 مسارات التدقيق - سجل للأنشطة والأحداث المتعلقة بتخزين البيانات، يوفر مساراً زمنياً لمن قام بالدخول إلى البيانات ومتى.

3.3 التوفر - إمكان الدخول إلى البيانات وجاهزيتها للمستخدمين المصرح لهم عند الحاجة إليها، مما يضمن إمكان الدخول إليها على نحو موثوق وسريع.

3.4 النسخ الاحتياطي - عمل نسخ من البيانات لحمايتها من الضياع أو التلف أو الحذف العرضي.

3.5 الامتثال - الالتزام بالمعايير القانونية والتنظيمية والصناعية المتعلقة بتخزين البيانات والخصوصية والأمان وغيرها من المجالات ذات الصلة.

3.6 البيانات السرية - المعلومات التي تعتبر حساسة ويجب حمايتها من الدخول غير المصرح به أو الكشف عنها، للحفاظ على سريتها.

3.7 تصنيف البيانات - يجب تصنيف البيانات بناءً على حساسيتها وأهميتها، والتأكد من حصولها على المستوى المناسب من الحماية والحفظ.

3.8 إزالة التكرار من البيانات - عملية تحديد وإزالة النسخ المكررة من البيانات لتحسين مساحة التخزين وتقليل تكاليف التخزين.

3.9 تحويل نسق البيانات - تحويل البيانات من تنسيق إلى آخر لضمان التوافق و/أو لتلبية متطلبات تخزين محددة.

3.10 التخلص من البيانات - حذف البيانات مع التأكد من عدم إمكان استردادها عندما لم تعد هناك حاجة إليها.

3.11 دورة حياة البيانات - المراحل التي تمر بها البيانات من الإنشاء/الاستحواذ إلى التخلص منها، بما في ذلك الإنشاء والتخزين والاسترجاع والتعديل والأرشفة والتخلص منها.

3.12 نقل البيانات - نقل البيانات من نظام تخزين أو مستودع أو تنسيق إلى آخر، عادةً لترقية الأنظمة.

3.13 ملكية البيانات - تحديد الأفراد أو الكيانات المسؤولة عن البيانات، بما في ذلك دقتها وأمنها والامتثال للسياسات واللوائح المعمول بها.

3.14 خصوصية البيانات - حماية المعلومات الشخصية والحساسة من الدخول غير المصرح به أو الاستخدام أو الكشف عنها على وفق قوانين ولوائح الخصوصية.

3.15 الاحتفاظ بالبيانات - الفترة التي يجب تخزين البيانات والاحتفاظ بها، بناءً على المتطلبات القانونية أو التنظيمية أو متطلبات العمل.

3.16 تخزين البيانات - تخزين البيانات بطريقة منظمة لاسترجاعها واستخدامها في المستقبل.

3.17 التحقق من صحة البيانات - ضمان دقة البيانات واكتمالها واتساقها من خلال إجراءات التحقق والتدقيق.

3.18 التشفير - تحويل البيانات إلى تنسيق غير قابل للقراءة باستخدام تقنيات التشفير لحمايتها من الدخول غير المصرح به.

3.19 النزاهة - دقة البيانات وتناسقها وموثوقيتها طوال دورة حياتها، مما يضمن بقائها كاملة ومن دون تغيير.

4.0 السياسة

4.1 تعزيز ثقافة المسؤولية عن التعامل مع البيانات من خلال تحديد الأدوار بوضوح وتوفير التدريب اللازم.

4.2 إدارة دورة حياة البيانات بالكامل، من إنشائها إلى التخلص منها، باستخدام الضوابط والضمانات المناسبة.

4.3 تشجيع التواصل المفتوح بين أعضاء الفريق لضمان إدارة فعالة للبيانات.

4.4 إعطاء الأولوية للتحسينات المنتظمة لأساليب تخزين البيانات، بما يتماشى مع التكنولوجيا الجديدة وممارسات التدقيق.

4.5 الحفاظ على أمن البيانات وخصوصيتها وسرية المعلومات من خلال تدابير أمنية قوية، والامتثال لسياسات الخصوصية، وضوابط الدخول الصارمة.

4.6 يعد الامتثال لمعايير الصناعة والمتطلبات التنظيمية إلزامياً، مع إجراء عمليات تدقيق منتظمة لضمان الالتزام.

4.7 تصنيف البيانات والاحتفاظ بها على أساس متطلبات الحساسية والتنظيم، مع وجود طرق التخلص الآمنة.

4.8 تضمن إجراءات النسخ الاحتياطي توفر البيانات وإمكان استردادها، مع إجراء اختبارات منتظمة للتحقق من سلامتها.

4.9 تم تصميم البنية الأساسية للتخزين بحيث تكون قابلة للتطوير ومُحسَّنة للأداء، مع المراقبة المستمرة وإدارة جيدة للموارد.

5.0 الإجراءات

5.1 تحدد قيادة/إدارة تكنولوجيا المعلومات الاتجاه الاستراتيجي والأهداف لإدارة التخزين داخل المؤسسة، وتضع سياسة معيار تخزين تكنولوجيا المعلومات وتنقلها إلى جميع أصحاب المصلحة المعنيين، وتخصص الموارد لتنفيذ وصيانة البنية الأساسية للتخزين.

5.2 يصنف فريق إدارة/أرشفة البيانات بناءً على قيمتها ومتطلبات الاحتفاظ بها، ويطور وينفذ سياسات وإجراءات الاحتفاظ بالبيانات، ويراقب ويدير عمليات النسخ الاحتياطي للبيانات واستعادتها.

5.3 ينشئ مسؤول الأمن وينفذ ضوابط الأمن للبيانات المخزنة داخل أنظمة التخزين، ويراقب أنظمة التخزين بحثاً عن خروقات أمنية أو دخول غير مصرح به أو فقدان البيانات، ويطور ويحافظ على آليات التشفير للبيانات الحساسة أو السرية.

5.4 يصمم فريق النسخ الاحتياطي/الاسترداد وينفذ استراتيجيات النسخ الاحتياطي/الاسترداد للبيانات المخزنة داخل أنظمة التخزين، ويطور جداول النسخ الاحتياطي ويضمن إجراء النسخ الاحتياطي المنتظم على وفق السياسات، ويراقب عمليات النسخ الاحتياطي ويتحقق من سلامة بيانات النسخ الاحتياطي.

5.5 يتعاون فريق الامتثال والشؤون القانونية مع فرق أخرى لضمان امتثال سياسات وإجراءات التخزين للوائح حماية البيانات والمتطلبات الخاصة بالصناعة، ويراقب ويقيم التغييرات في لوائح حماية البيانات والاحتفاظ بها، ويجري عمليات تدقيق وتقييم منتظمة للتحقق من الامتثال لمعايير التخزين.

5.6 يدير المستخدمون النهائيون ومالكو التطبيقات استخدام البيانات والتخزين بكفاءة، على وفق الممارسات المحددة، ويتعاونون مع مسؤول التخزين لمعالجة المشكلات المتعلقة بالتخزين وتحسين استخدام التخزين، ويلتزمون بإرشادات الاحتفاظ بالبيانات والأرشفة من أجل الإدارة السليمة وتخزين البيانات.

التخطيط لسعة التخزين

5.7 تخطط قيادة/إدارة تكنولوجيا المعلومات وتخصص موارد تخزين كافية لاستيعاب زيادة البيانات.

5.8 تراقب قيادة/إدارة تكنولوجيا المعلومات استخدام التخزين بانتظام لتحديد القيود المحتملة للسعة واتخاذ تدابير استباقية لمعالجتها.

توفير التخزين

5.9 تحدد قيادة/إدارة تكنولوجيا المعلومات متطلبات التخزين للتطبيقات والمستخدمين والأنظمة المختلفة.

5.10 تخصص قيادة/إدارة تكنولوجيا المعلومات وتوفر موارد التخزين بناءً على معايير محددة، مثل الأداء والتوافر وتصنيف البيانات.

تصنيف البيانات وتبويبها

5.11 يصنف فريق إدارة/أرشفة البيانات بناءً على حساسيتها وخطورتها والمتطلبات التنظيمية.

5.12 يطبق فريق إدارة/أرشفة البيانات سياسات التخزين المناسبة وضوابط الدخول واستراتيجيات النسخ الاحتياطي بناءً على تصنيف البيانات وتبويبها.

النسخ الاحتياطي للبيانات واستعادتها

5.13 يطور فريق النسخ الاحتياطي/الاسترداد استراتيجية نسخ احتياطي تتوافق مع أهداف الاحتفاظ بالبيانات واستمرارية الأعمال.

5.14 يقوم فريق النسخ الاحتياطي/الاسترداد بنسخ البيانات احتياطياً طبقاً لجداول النسخ الاحتياطي المحددة، مع مراعاة أهمية البيانات.

5.15 يتحقق فريق النسخ الاحتياطي/الاسترداد من سلامة بيانات النسخ الاحتياطي من خلال الاختبار والتحقق المنتظمين.

5.16 ينفذ فريق النسخ الاحتياطي/الاسترداد إجراءات لاستعادة البيانات في حالة فقد البيانات أو فشل النظام.

أرشفة البيانات والاحتفاظ بها

5.17 يحدد فريق إدارة البيانات/الأرشفة سياسات الاحتفاظ بالبيانات بناءً على المتطلبات التنظيمية والتجارية.

5.18 يحدد فريق إدارة البيانات/الأرشفة البيانات التي تحتاج إلى أرشفة للتخزين والاسترجاع على المدى الطويل.

5.19 يراقب فريق إدارة البيانات/الأرشفة عمليات الاحتفاظ بالبيانات والأرشفة، ويضمن الامتثال للسياسات المحددة.

أمن التخزين وضوابط الدخول

5.20 ينفذ مسؤول أمن البيانات ضوابط الدخول والأذونات لضمان الدخول المصرح به إلى البيانات المخزنة.

5.21 يقوم مسؤول الأمان بمراجعة وتحديث ضوابط الدخول بشكل منتظم لتتماشى مع التغييرات في أدوار المستخدم ومسؤولياته وتصنيف البيانات.

مراقبة أداء التخزين وتحسينه

5.22 تعمل قيادة/إدارة تكنولوجيا المعلومات على مراقبة مقاييس أداء التخزين بشكل مستمر، بما في ذلك معدل نقل البيانات المدخلة/المخرجة، وزمن الدخول، وأوقات الاستجابة.

5.23 تعمل قيادة/إدارة تكنولوجيا المعلومات على تشخيص ومعالجة الاختناقات في أداء التخزين أو قيود السعة.

الامتثال والتدقيق

5.24 يقوم فريق الامتثال والقانون بمراجعة وتقييم ممارسات التخزين بشكل منتظم لضمان الامتثال للمعايير التنظيمية والصناعية.

5.25 يجري فريق الامتثال والقانون عمليات تدقيق داخلية للتحقق من الالتزام بسياسات التخزين وضوابط الأمان.

5.26 يوثق فريق الامتثال والقانون نتائج التدقيق، ويعالج أي فجوات أو مشكلات عدم امتثال محددة، وينفذ الإجراءات التصحيحية.

السياسات والوثائق ذات الصلة

خصوصية البيانات
أمن المعلومات