التصنيف: إدارة تكنولوجيا المعلومات

جهة الموافقة: الرئيس

الجهة المسؤولة: مساعد الرئيس للشؤون الإدارية والمالية

الجهة المنفذة: قسم تكنولوجيا المعلومات

تاريخ بدء التنفيذ: أيّار 2025

المراجعة: نيسان 2028

سياسة وإجراءات مراكز الحاسوب التابعة لتكنولوجيا المعلومات

1.0 الغرض

1.1 الغرض الرئيس من سياسة مراكز الحاسوب التابعة لتكنولوجيا المعلومات هو وضع المبادئ التوجيهية واللوائح اللازمة للاستخدام الفعّال والآمن لمراكز حاسوب الجامعة الأمريكية في بغداد. تعمل هذه السياسة كإطار لضمان الإدارة السليمة والتشغيل والصيانة لمراكز الحاسوب.

2.0 النطاق

2.1 تنطبق هذه السياسة على جميع المستخدمين الذين يدخلون إلى مراكز حاسوب الجامعة الأمريكية في بغداد ويستخدمونها، بما في ذلك على سبيل المثال لا الحصر الموظفون والطلبة والموردون من جهات خارجية.

3.0 التعاريف

3.1 سياسة الاستخدام المقبول - مجموعة من المبادئ التوجيهية والقواعد التي تحدد الاستخدام المقبول والمسؤول لموارد مركز الحاسوب. تحدد السياسة السلوكيات والأنشطة والممارسات التي يجب على المستخدمين الالتزام بها عند استخدام مرافق مركز الحاسوب، والمعدات، والشبكات، والبيانات.

3.2 التحكم في الدخول - عملية إدارة وتنظيم وصول المستخدم إلى موارد مركز الحاسوب. يتضمن التحكم في الوصول منح وإلغاء امتيازات المستخدم، وفرض آليات المصادقة، وتنفيذ سياسات الترخيص لضمان أن الأفراد المصرح لهم فقط يمكنهم الوصول إلى موارد معينة.

3.3 مركز الحاسوب - مرفق أو منطقة مخصصة داخل منظمة أو مؤسسة تضم أنظمة الحاسوب والخوادم ومعدات الشبكات والبنية الأساسية المرتبطة المطلوبة لمعالجة البيانات وتخزينها والاتصال بها.

3.4 دعم مكتب المساعدة - الإجراءات التي يتبعها مكتب المساعدة أو فريق الدعم الفني للمساعدة في حل المشكلات المتعلقة بالحاسوب. قد تتضمن إجراءات مكتب المساعدة

3.5 أنظمة التذاكر وإجراءات التصعيد والمساعدة عن بعد وبروتوكولات اتصال المستخدم لمعالجة مشاكل المستخدم وحلها بكفاءة.

3.6 الاستجابة للحوادث - النهج المنظم والمنسق للكشف عن الحوادث الأمنية أو الاضطرابات التشغيلية داخل مركز الحاسوب والتحقيق فيها والتخفيف منها واعادة التأهيل. تهدف إجراءات الاستجابة للحوادث إلى تقليل تأثير الحوادث والحفاظ على الأدلة واستعادة الخدمات ومنع وقوع حوادث مماثلة في المستقبل.

3.7 تكوين الشبكة - عملية إعداد وتكوين شبكات الحاسوب، بما في ذلك أجهزة التوجيه والمفاتيح وجدران الحماية وبروتوكولات الشبكة. وهي تتضمن تحديد عناوين بروتوكول الإنترنت وأقنعة الشبكة الفرعية وإعدادات (نظام أسماء النطاقات) وضوابط الدخول إلى الشبكة لإنشاء بنية تحتية آمنة وموثوقة للشبكة.

3.8 نشر البرامج - الإجراءات الخاصة بنشر وتثبيت وتكوين تطبيقات البرامج على أنظمة الحاسوب أو الشبكات. قد يتضمن نشر البرامج إنشاء حزم النشر واختبار التوافق وتنسيق جداول الطرح وضمان الامتثال للترخيص المناسب.

3.9 مسؤول النظام - الموظفون المخولون المسؤولون عن إدارة وتكوين وصيانة البنية الأساسية لمركز الحاسوب، بما في ذلك الخوادم وأجهزة الشبكة والبرامج المرتبطة بها. يضمن مسؤولو النظام الأداء السليم والأمان والتوافر لمركز الحاسوب.

3.10 إدارة النظام - عملية إدارة وصيانة أنظمة الحاسوب والشبكات والخوادم وتطبيقات البرامج لضمان الأداء السليم والأمان والأداء. وهي تتضمن مهام مثل إدارة المستخدمين وتثبيت البرامج وتحديثات النظام واستكشاف الأخطاء وإصلاحها.

3.11 مراقبة النظام وضبط الأداء - الإجراءات الخاصة بمراقبة أنظمة الحاسوب والشبكات وتطبيقات البرامج لضمان أدائها وتوافرها على النحو الأمثل. تتضمن إجراءات مراقبة النظام جمع مقاييس الأداء وتحليل صحة النظام واتخاذ تدابير استباقية لمعالجة المشكلات أو الاختناقات المحتملة.

3.12 المستخدم - الفرد الذي يُمنح حق الدخول المصرح به إلى مركز الحاسوب وموارده. قد يشمل المستخدمون الموظفين أو الطلبة أو أي أفراد آخرين يتمتعون بصلاحيات معتمدة.

3.13 إدارة دخول المستخدم - الإجراءات المتعلقة بمنح وإدارة دخول المستخدم إلى أنظمة الحاسوب والشبكات وتطبيقات البرامج داخل مركز الحاسوب. يتضمن ذلك إنشاء حسابات المستخدم وتعيين امتيازات الدخول المناسبة وإدارة كلمات المرور وإلغاء تنشيط الحسابات عند الضرورة للحفاظ على أمان النظام وحماية المعلومات الحساسة.

4.0 السياسة

4.1 تنفيذ تدابير أمنية قوية، مثل ضوابط الدخول والتشفير وأنظمة اكتشاف الاختراق وعمليات التدقيق الأمني المنتظمة، لحماية مركز الحاسوب من الدخول غير المصرح به وانتهاكات البيانات والتهديدات الأمنية الأخرى.

4.2 يتحمل المستخدمون مسؤولية الحفاظ على أمان حساباتهم والالتزام بسياسات وإرشادات الأمان التي وضعتها المنظمة لمركز الحاسوب.

4.3 يحظى أمان مركز الحاسوب وموارده بأهمية قصوى. ويجب أن تُتخذ جميع التدابير اللازمة لضمان سرية وسلامة وتوافر البيانات والأنظمة داخل مركز الحاسوب.

4.4 يجب استخدام موارد مركز الحاسوب بطريقة مسؤولة وعلى وفق سياسة الاستخدام المقبولة للمؤسسة.

4.4.1 من المتوقع أن يلتزم المستخدمون بالقوانين واللوائح والمعايير الأخلاقية المعمول بها عند استخدام مرافق مركز الحاسوب، والمعدات، والشبكات، والبيانات.

4.4.2 يُحظر إساءة استخدام موارد مركز الحاسوب أو الدخول غير المصرح به إليها وقد يؤدي ذلك إلى اتخاذ إجراءات تأديبية.

4.5 تلتزم المؤسسة بحماية خصوصية وسرية البيانات التي تتم معالجتها وتخزينها داخل مركز الحاسوب.

4.5.1 تنفيذ تدابير مثل تشفير البيانات وضوابط الدخول وبروتوكولات نقل البيانات الآمنة وتصنيف البيانات لحماية المعلومات الحساسة داخل مركز الحاسوب.

4.5.2 وضع سياسات الاحتفاظ بالبيانات والتخلص منها لضمان الامتثال للوائح حماية البيانات المعمول بها والحد من مخاطر الكشف غير المصرح به عن البيانات داخل مركز الحاسوب.

4.6 إجراء عمليات تدقيق وتقييم منتظمة لتقييم الامتثال وتحديد مجالات التحسين داخل مركز الحاسوب.

4.7 مراجعة السياسات والإجراءات والضوابط الخاصة بمركز الحاسوب وتقييمها وتحديثها بانتظام لمعالجة المخاطر الناشئة والثغرات وأفضل الممارسات.

4.8 تشجيع الملاحظات من المستخدمين وأصحاب المصلحة وأخذها بالحسبان لدفع التحسينات وتعزيز الفعالية العامة لمركز الحاسوب.

4.9 إنشاء خطوط اتصال واضحة، وتعزيز تبادل المعلومات لضمان التنسيق في الوقت المناسب، والاستجابة للحوادث، وحل المشكلات داخل مركز الحاسوب.

4.10 استخدام الاجتماعات المنتظمة، وبرامج التدريب، وقنوات التغذية الراجعة لتعزيز العمل الجماعي والحفاظ على التواصل الفعال داخل مركز الحاسوب.

5.0 الإجراءات

5.1 يشرف مدير قسم تكنلوجيا المعلومات على عمليات مركز الحاسوب، ويضع السياسات وينفذها، ويوفر التوجيه الاستراتيجي المتوافق مع الأهداف التنظيمية. ويقومون بتخصيص الموارد، ومراقبة أداء النظام والأمان، والتعاون مع الأقسام الأخرى لضمان التكامل السلس للخدمات والدعم داخل مركز الحاسوب.

5.2 يدير مسؤولو النظام أنظمة الحاسوب والشبكات والخوادم وتطبيقات البرامج داخل مركز الحاسوب، ويضمنون الأداء السليم والأمان من خلال التثبيت والصيانة والمراقبة وإدارة حسابات المستخدمين. كما يتعاونون مع فرق تكنولوجيا المعلومات الأخرى للحفاظ على الأنظمة المتكاملة والبنية الأساسية للشبكة داخل مركز الحاسوب.

5.3 يصمم مسؤولو الشبكة وينفذون ويديرون البنية الأساسية لشبكة مركز الحاسوب، ويهيئون أجهزة الشبكة ويحافظون عليها ويحسنون الأداء داخل مركز الحاسوب.

5.4 يقدم موظفو مكتب المساعدة/الدعم الفني الدعم الفني والمساعدة لمستخدمي مركز الحاسوب، ويستجيبون بسرعة للاستفسارات، ويحلون المشكلات، ويوثقون الطلبات والحوادث باستخدام نظام التذاكر داخل مركز الحاسوب.

5.4.1 إنشاء نظام مكتب مساعدة داخل مركز الحاسوب لتلقي وتتبع ومعالجة استفسارات المستخدمين والمشاكل والطلبات.

5.4.2 تعيين تذاكر الدعم وإعطائها الأولوية داخل مركز الحاسوب بناءً على شدتها وتأثيرها.

5.4.3 الرد على استفسارات المستخدمين وتقديم المساعدة الفنية في الوقت المناسب وبطريقة احترافية داخل مركز الحاسوب.

5.4.4 تصعيد المشكلات المعقدة أو غير المحلولة داخل مركز الحاسوب إلى الفرق الفنية المناسبة لمزيد من التحقيق والحل.

5.4.5 الحفاظ على قاعدة معرفية للمشكلات الشائعة والحلول الخاصة بمركز الحاسوب لتسهيل دعم المستخدم الذاتي.

5.5 إنشاء وإدارة حسابات المستخدمين للموظفين الذين يستخدمون مركز الحاسوب، مع ضمان مستويات الدخول والأذونات المناسبة داخل مركز الحاسوب.

5.5.1 تنشيط وتعطيل حسابات المستخدمين بناءً على انضمام الموظفين ونقلهم ومغادرتهم داخل مركز الحاسوب.

5.5.2 فرض سياسات قوية لكلمات المرور وإعادة تعيين كلمات المرور بشكل دوري لتعزيز أمان الحساب داخل مركز الحاسوب.

5.5.3 تقديم الدعم المتعلق بحساب المستخدم، بما في ذلك إعادة تعيين كلمات المرور وإعادة تفعيل الحساب واستكشاف أخطاء الدخول وإصلاحها داخل مركز الحاسوب.

5.6 جدولة فترات الصيانة الدورية لإجراء تحديثات النظام والتصحيحات والتحسينات داخل مركز الحاسوب.

5.6.1 اختبار التحديثات والتحقق منها في بيئة خاضعة للرقابة قبل نشرها على أنظمة الإنتاج داخل مركز الحاسوب.

5.6.2 توثيق أنشطة الصيانة، بما في ذلك إجراءات النسخ الاحتياطي وخطط الإلغاء وسجلات التغيير الخاصة بمركز الحاسوب.

5.6.3 إبلاغ المستخدمين بالصيانة المخطط لها مسبقاً، مما يقلل من الانقطاعات في الخدمات داخل مركز الحاسوب.

5.7 تطوير وتنفيذ استراتيجية النسخ الاحتياطي للبيانات لضمان النسخ الاحتياطي المنتظم والآمن للبيانات الهامة داخل مركز الحاسوب.

5.7.1 تحديد جداول النسخ الاحتياطي وفترات الاحتفاظ ومواقع تخزين النسخ الاحتياطية الخاصة بمركز الحاسوب.

5.7.2 إجراء نسخ احتياطية دورية للبيانات والتحقق من سلامتها وإمكانية استردادها داخل مركز الحاسوب.

5.7.3 اختبار وتوثيق إجراءات استرداد البيانات لضمان الاستعادة في الوقت المناسب في حالة فقد البيانات أو فشل النظام داخل مركز الحاسوب.

5.8 إنشاء عملية إدارة الحوادث للاستجابة للحوادث المتعلقة بتكنولوجيا المعلومات وحلها داخل مركز الحاسوب.

5.8.1 تصنيف الحوادث بناءً على شدتها وتأثيرها داخل مركز الحاسوب لتحديد أولويات جهود الاستجابة.

5.8.2 التحقيق في الحوادث وتشخيصها داخل مركز الحاسوب، وتحديد الأسباب الجذرية والحلول المحتملة.

5.8.3 توثيق تفاصيل الحوادث والحلول والدروس المستفادة للرجوع إليها في المستقبل وتحسينها داخل مركز الحاسوب.

5.8.4 توصيل تحديثات الحوادث للمستخدمين المتضررين وأصحاب المصلحة داخل مركز الحاسوب بطريقة شفافة وفي الوقت المناسب.

5.9 تنفيذ عملية إدارة التغيير للتحكم في التغييرات وإدارتها في أنظمة تكنولوجيا المعلومات والبنية الأساسية داخل مركز الحاسوب.

5.9.1 تقييم وتقدير التغييرات المقترحة داخل مركز الحاسوب، مع مراعاة المخاطر والتأثيرات والفوائد المحتملة.

5.9.2 التخطيط وجدولة التغييرات داخل مركز الحاسوب، وضمان إجراء الاختبارات والموافقات والاتصالات المناسبة.

5.9.3 تنفيذ التغييرات بطريقة منظمة ومنسقة داخل مركز الحاسوب، مع تقليل الاضطرابات وضمان التوثيق المناسب.

5.9.4 إجراء مراجعات وتحليلات ما بعد التغيير داخل مركز الحاسوب لتقييم فعالية وتأثير التغييرات المنفذة.

5.10 الاحتفاظ بمخزون من أصول تكنولوجيا المعلومات الخاصة بمركز الحاسوب، بما في ذلك الأجهزة، والبرامج، والتراخيص، والضمانات.

5.10.1 تتبع تفاصيل الأصول الخاصة بمركز الحاسوب، مثل تواريخ الشراء والمواقع والمستخدمين المعينين.

5.10.2 إجراء عمليات تدقيق منتظمة للأصول داخل مركز الحاسوب لضمان الدقة والامتثال لاتفاقيات الترخيص.

5.10.3 التخلص بشكل صحيح من الأصول القديمة داخل مركز الحاسوب باتباع إرشادات محو البيانات والبيئة المناسبة.

5.11 تطوير وتنفيذ سياسات وإجراءات أمن تكنولوجيا المعلومات الخاصة بمركز الحاسوب لحماية الأنظمة والشبكات والبيانات.

5.11.1 تنفيذ ضوابط الأمن الخاصة بمركز الحاسوب، مثل جدران الحماية وبرامج مكافحة الفيروسات وأنظمة اكتشاف الاختراق.

5.11.2 تحديث تدابير الأمن بانتظام لمعالجة التهديدات والثغرات الناشئة.

5.11.3 إجراء تدريب على التوعية الأمنية للموظفين لتعزيز ممارسات الحوسبة الآمنة.

5.11.4 مراقبة الحوادث الأمنية والتحقيق فيها، والاستجابة السريعة للتخفيف من المخاطر ومنع حدوثها في المستقبل.

السياسات والوثائق ذات الصلة

الاستخدام المقبول

الدخول والأذونات

جمع البيانات وتسليمها

الاستجابة للحوادث

أمن المعلومات

الخصوصية والسرية