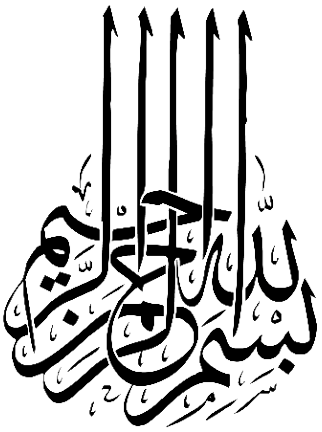
السياسة والاجراءات
بعمادة تقنية المعلومات

جامعة المجمعة
Majmaah University

DIT@
عمادة تقنية المعلومات
Deanship of Information Technology


بسم الله الرحمن الرحيم

المحتويات

السياسة العامة لأمن المعلومات

١. الهدف:

تم تصميم هذه السياسة للتأكد من أمن موارد المعلومات من الضرر أو الاستخدام الغير مصرح له مع المحافظة في نفس الوقت على متطلبات مشاركة المعلومات مع الأوساط العلمية والثقافية المحيطة بالجامعة.

٢. النطاق:

تنطبق هذه السياسة على جميع المنسوبين من موظفين وأعضاء هيئة تدريس و الطلاب, ولغيرهم ممن لديهم صلاحيات للوصول لمصادر المعلومات في جامعة المجمعة. إن على كل مستخدم في الجامعة لهذه المصادر مسؤوليات تجاه حماية ممتلكات الجامعة, بعض الأقسام والأفراد لديهم مسؤوليات خاصة تجاه ذلك. تشير هذه السياسة إلى كل مصادر المعلومات الخاصة بالجامعة سواءً كانت تخضع لتحكم وإدارة فردية أو مشتركة, سواءً كانت منعزلة أو مرتبطة بالشبكة. تنطبق السياسة أيضاً على كل أجهزة الحاسب ومنشآت الاتصالات المملوكة والممنوحة, والمشغلة, أو تلك المنطوية بعقد مع الجامعة. يتضمن ذلك الأجهزة الشبكية, الهواتف, الأجهزة اللاسلكية, الحواسيب الشخصية, الخوادم بجميع أنواعها, وأي ملحقات تابعة لها من برمجيات ونحوها, سواءً تستخدم في الإدارة, البحث العلمي, التدريس, أو غيرها من الأغراض.

٣. مبادئ أمن المعلومات:

الغرض من أمن المعلومات هو حماية مصادر المعلومات الخاصة بالجامعة من الاستخدام الغير مصرح أو الاضرار بها. المبادئ الأساسية المتبعة لتحقيق هذه الأهداف هي:

أ.توفر مصادر المعلومات (Availability):
مصادر المعلومات الخاصة بالجامعة, متضمناً الشبكة, المكونات المادية والبرمجية, المنشآت, البنية التحتية, وغيرها من المصادر, متاحة لدعم مسار التعليم والتدريس والبحث العلمي و الأدوار الإدارية الموكلة.

ب.سلامة المعلومات (Integrity):
يمكن الوثوق بالمعلومات المستخدمة لتحقيق التعليم والتدريس والبحث العلمي والإدارة لتعكس بشكل سليم حقيقة ما تمثله.

ج. سرية المعلومات (Confidentiality):
ان القدرة على الوصول وتعديل المعلومات متاحة فقط للمستخدمين المصرح لهم وللأغراض المصرح بها.

د. دعم النشاط الأكاديمي:
يجب أن تتوازن المتطلبات لحماية مصادر المعلومات مع الحاجة لدعم النشاط الرامي لتحقيق الأهداف الأكاديمية.

هـ. الوصول للمعلومات:
تزداد قيمة المعلومات كمصادر مؤسسية من خلال الاستخدام الأمثل لها, كما تتضائل من خلال سوء استخدامها, تفسيرها, أو القيود الغير لازمة للوصول لها.

٤. تصنيف المعلومات:

جميع معلومات الجامعة مصنفة ضمن أربع مستويات, وذلك بناءً على درجة الخطورة والحساسية. تأخذ بعين الاعتبار هذه الأصناف الحماية القانونية، الإتفاقيات التعاقدية، الإعتبارات الأخلاقية، قضايا الخصوصية، والقيمة الامتلاكية والاستراتيجية. يحدد مستوى التصنيف الحمايات الأمنية و اساليب منح صلاحيات الوصول والتي يجب أن تستخدم مع المعلومات.

أصناف المعلومات هي كما يلي:

أ.المعلومات المحظورة:
تصنف المعلومات على أنها محظورة, إذا كانت حماية المعلومات مطلوبة حسب الأنظمة الحكومية أو القانونية, أو في حالات تنبيه فرد ما حول استخدام غير ملائم للمعلومات أو حالة إفادة جهات حكومية حول وصول غير مصرح له.

ب.المعلومات المقيدة:
تصنف المعلومات على أنها مقيدة في حال كانت متاحة لفرد أو مجموعة أو فريق أو قسم محدد دون غيره من الأفراد أو الأقسام أو الإدارات في الجامعة.

ت.المعلومات السرية:
تصنف المعلومات على أنها سرية في حال عدم إعتبارها محظورة أو مقيدة وفي نفس الوقت غير متاحة للعامة.

ث.المعلومات العامة:
جميع المعلومات التي لا تصنف تحت أي من الأصناف أعلاه تعتبر عامة. يرجى مراجعة إدارة أمن المعلومات لمعرفة أكثر المعلومات المستخدمة بشكل عام.

٥. مخالفة السياسة وإساءة استخدام المعلومات:

تتضمن مخالفة السياسة, ولا تنحصر, بما يلي:

i.وصول الفرد لمعلومات غير مصرح له بها.
ii.السماح لافراد بالوصول لمعلومات غير مصرح لهم بها.
iii.نشر معلومات بشكل يخالف سياسة أو إجراءات الاستخدام المقبول أو أي قوانين أو أحكام متصلة بها.
iv.تعديل غير ملائم أو إتلاف للمعلومات.
v.حماية غير كافية للمعلومات.
vi.تجاهل المتطلبات بإدارة واستخدام و حماية مصادر المعلومات بشكل مناسب.

قد ينتج عن هذه المخالفات فصل من الشبكة, إلغاء الوصول, إجراء تصحيحي, و/أو الملاحقة القضائية. المخالفين قد يكونون عرضة لإجراء تأديبي والذي قد يصل إلى الإقالة أو الطرد حسب السياسات و الاتفاقيات و القواعد السلوكية و غيرها من الأدوات التي تحكم العلاقة بين الفرد والجامعة.

الطعن بهذه الأحكام يجب أن يكون بناءً على البند الموافق لذلك في العقد الوظيفي للفرد, أو من خلال إتباع الإجراءات القانونية الموافقة.

أ.في حال مخالفة جهة أو قسم لهذه السياسة قد يؤخذ بعين الاعتبار عقوبات مالية وتكاليف علاج مرتبطة بنتيجة حادث أمن المعلومات.
ii.في حال مخالفة شركات طرف ثالث لهذه السياسة, فقد يكبدها التزامات مالية, بالإضافة لإلغاء العقد

سياسة الاستخدام والخصوصية لبوابة الجامعة الإلكترونية

١. نظرة عامة:

تعتبر سياسة وشروط الخصوصية الموضحة أدناه جزءاً من شروط استخدام الموقع الإلكتروني لبوابة الجامعة الإلكترونية وأحكامها.

لا يقوم هذا الموقع بجمع معلومات شخصية عنك عندما تقوم بزيارة الموقع إلا إذا اخترت تحديداً وبمعرفتك تقديم هذه المعلومات لنا. وفي حال اخترت تقديم معلومات لنا، فإننا لا نستخدمها إلا لإنجاز طلبك للحصول على معلومات أو خدمات من قبل جامعة المجمعة . وباستخدامك هذا الموقع ، فإنك توافق على شروط سياسة الخصوصية هذه ، مع ملاحظة أن المعلومات المرسلة من قبلك قد يتم مشاركتها مع الجهات الحكومية السعودية الأخرى في حال تطلب إنجاز طلبك لذلك و دون الرجوع إلى أي طرف من الأطراف .

تحتفظ جامعة المجمعة بالحق في إجراء أي تعديل طفيف أو جذري لشروط سياسة الخصوصية من وقت لآخر من دون الحاجة إلى تقديم إخطار بذلك . كما يحق لجامعة المجمعة اتخاذ التدابير التي تراها ملائمة للحماية من أي فقدان أو إساءة استخدام أو تغيير للمعلومات الموجودة على الموقع الإلكتروني وذلك من دون أن تضمن جامعة المجمعة في هذه الحال ، الاحتفاظ بسرية محتويات هذا الموقع الإلكتروني ، ولا تعتبر مسؤولة قانوناً عن أي ضرر قد تتعرض له أنت أو أي طرف آخر نتيجة لانتهاك السرية بشأن المعلومات التي تكون قد نقلتها إلى الموقع أو التعويض عنه.

كما يقوم الموقع بتنفيذ إجراءات دقيقة للحماية من فقد المعلومات أو إساءة استخدامها أو تغييرها . ومع ذلك فإن جامعة المجمعة لا يمكنها أن تضمن سرية استخدامك لهذا الموقع ، وهي لا تعتبر مسؤولة عن أي ضرر قد تتعرض له أنت أو أي طرف نتيجة لانتهاك السرية بشأن المعلومات التي تكون قد نقلتها إلى الموقع.

تكون قوانين المملكة العربية السعودية وحدها هي القوانين واجبة التطبيق في كل ما يتعلق بالنزاعات التي قد تنشأ من جراء استخدام هذا الموقع الإلكتروني ، كما تختص محاكم المملكة العربية السعودية حصرياً بالنظر في تلك النزاعات والبت فيها.

٢. الهدف:

تهدف هذه السياسة لتوضيح حقوق وواجبات البوابة الإلكترونية لجامعة المجمعة ومستخدميها وتحدد السياسات اللازمة للاستخدام وسياسة الخصوصية وسياسات أخرى .

٣. النطاق:

تنطبق هذه السياسة على جميع مستخدمي البوابة الإلكترونية

٤. حقوق الملكية الفكرية:

يخضع لنظام حقوق الملكية الفكرية كل مادة منشورة في بوابة الجامعة ، والمواقع التابعة لها، من : (نصوص أو رسومات أو صور أو برامج أو تصاميم أو ملفات أو غيرها) ، كما يُمنع إضافة أي مادة منشورة تنتهك حقوق الملكية الفكرية لأي جهة أو أشخاص في بوابة الجامعة .

كما يجب أخذ تصريح خطي من وحدة البوابة الإلكترونية بعمادة تقنية المعلومات عند أي استخدام عام للمواد المنشورة في موقع الجامعة ؛ عدا ما يسمح به قانون حماية الملكية الفكرية السعودي ، وما هو منصوص عليه في هذه السياسة ، وبيان حقوق الملكية الفكرية في البوابة . كما أننا نؤكد على ضرورة الإشارة المرجعية عند الرجوع أو الاستخدام لأي مادة منشورة في البوابة .

٥. سياسة الاستخدام:

يُدار الموقع الإلكتروني لجامعة المجمعة من قبل وحدة البوابة الإلكترونية ، بما في ذلك جميع المعلومات والمواد الواردة فيه ويعني استخدام الموقع الإلكتروني لجامعة المجمعة قبول المستخدم للأحكام الواردة في شروط الاستخدام وسياسة الخصوصية .

ويجوز لوحدة البوابة الإلكترونية تغيير سياسة الاستخدام من حين لآخر دون سابق إنذار ، وفي حالة إجراء مثل هذه التغييرات، قد تعرض الوحدة إخطارات من خلال البوابة الإلكترونية لجامعة المجمعة وذلك ليكون المستخدم على علم ودراية بها . ويتعين على المستخدم مراجعة سياسة الاستخدام أو الخصوصية للاطلاع على التغييرات في كل مرة يعتزم فيها استخدام الموقع الإلكتروني للجهة التابع لها سواء كان كلية أو عمادة أو إدارة أو موقع خاص بعضو هيئة تدريس أو غيرها من المواقع التي لها صلة باستخدام البوابة الإلكترونية . ويكون استمرار المستخدم في استعمال الموقع الإلكتروني على أساس الشروط الواردة في سياسة الاستخدام هذه حسبما يجري تعديلها من وقت لآخر .

١. التغييرات في الموقع الإلكتروني وإخلاء المسؤولية :

تحتفظ وحدة البوابة الإلكترونية بالحق في تغيير المعلومات الواردة في أي موقع تحت مظلة الجامعة في أي وقت دون سابق إنذار . وتبدى الوحدة قدراً معقولاً من الحرص للتأكد من صحة المعلومات الواردة في كل المواقع الإلكترونية، إلا إنها لا تستطيع ضمان دقتها ولا تقدم أية ضمانات من أي نوع كان فيما كان يتعلق بالمحتوى (بما في ذلك أي نص أو رسوم بيانية أو إعلانات أو وصلات أو غيرها من البنود) .

٢. حالات الانقطاع و البطء في البوابة الإلكترونية لجامعة المجمعة :

تبدي الوحدة قدراً كبيراً من الحرص للحفاظ على استمرار البوابة الإلكترونية ، إلا إن شبكة الإنترنت ليست وسيلة مستقرة في كل الأحوال ، وقد تقع في أي وقت أخطاء أو حالات انقطاع للخدمة أو تأخير لها . ولا يقع على عاتق وحدة البوابة الإلكترونية أي التزام أو مسؤولية بصفة مستمرة لتشغيل الشبكة داخل الجامعة ، وخدمات الإنترنت خارج الجامعة .

٣. الروابط للمواقع الإلكترونية الأخرى :

قد تتضمن البوابة الإلكترونية لجامعة المجمعة روابط لمواقع إلكترونية أو عناوين أخرى على الانترنت ، وتخضع الروابط المنشورة عبر البوابة الإلكترونية للجامعة لموافقة وحدة البوابة الإلكترونية ، كما يحق للوحدة تعديل أو حذف الروابط التي لا تتوافق مع سياسة البوابة ، وعند استخدام روابط معينة في هذا الموقع الإلكتروني ، فقد يغادر المستخدم الموقع الإلكتروني لجامعة المجمعة ، ولا تشكل أية مواقع إلكترونية أخرى من هذا القبيل جزءاً من البوابة الإلكترونية لجامعة المجمعة ولا تنتمي لها . ولم تقم وحدة البوابة بمراجعة أي من المواقع الإلكترونية المتصلة بالمواقع الإلكتروني لجامعة المجمعة ، كما أنها لا تتحمل مسؤولية المحتوى الوارد في هذه المواقع الإلكترونية الخارجية المتصلة ببوابة جامعة المجمعة ، ولا عن أي منتجات أو خدمات تعرضها .

٤. الخصوصية :

تلتزم وحدة البوابة الإلكترونية بالحفاظ على خصوصيات جميع مستخدمي مواقع الجامعة . وتنظم سياسة الخصوصية جميع صفحات مواقع جامعة المجمعة .

٥. سياسة تعيين المشرفين و إعطاء الصلاحيات :

أ – يحق لكل جهة بالجامعة أن تخصص مشرف خاص بها سواءً واحد أو أكثر ، على أن تُعين الجهة (مشرف رئيسي واحد لموقعها بشرط أن يتقن اللغة العربية) ، ويحصل جميع المشرفين على اسم مستخدم وكلمة مرور خاصة بالموقع ، بحيث يكونوا المسؤولين عن موقع الجهة الإلكترونية بكل محتوياته .

ب – يتم ترشيح مشرف الموقع الإلكتروني الخاص بالجهة عن طريق تعبئة النموذج المخصص في بوابة الخدمات الإلكترونية (صفحة النماذج الإلكترونية) .

ت – يحق فقط لمشرف الموقع الإلكتروني طلب استعادة كلمة السر من وحدة البوابة الإلكترونية .

ث – عند تغيير أو إضافة مشرفين فلا بد من إبلاغ وحدة البوابة الإلكترونية رسمياً بذلك . و في حال عدم دخول المشرف للوحة تحكم الموقع لمدة شهر كحد أقصى ، فيحق لوحدة البوابة الإلكترونية إيقاف صلاحية الدخول لهذا المشرف .

ج – اسم المستخدم وكلمة السر الخاصة بالمواقع الإلكترونية هي مسئولية المشرف بالدرجة الأولى ، ولا يجب مشاركة كلمات السر مع الآخرين . ويحق لوحدة البوابة الإلكترونية إغلاق صلاحيات أي مشرف يَثْبُت (بأي طريقة كانت) مشاركته لاسم المستخدم الخاص به مع أي مشرف أو شخص آخر .

د – لابد أن تضمن الجهة المرشحة للمشرف استمراره بالعمل مشرفاً لمدة لا تقل عن ثلاث ٣ ـة أشهر على الأقل .

هـ - في حال عدم الالتزام بسياسات تعيين المشرفين و إعطاء الصلاحيات المذكورة أعلاه ، فإنه يحق لوحدة البوابة الإلكترونية اتخاذ الإجراء المناسب .

٦. سياسة التدريب :

- تنظم وحدة البوابة الإلكترونية دورات تدريبية لمشرفي ومشرفات البوابات الفرعية لكيفية إدارة المواقع الإلكترونية وبشكل دوري (نهاية كل شهر هجري) في حال الحاجة لذلك .
- يحق لكل جهة لديها موقع إلكتروني تحت مظلة البوابة الإلكترونية بالجامعة طلب التدريب اللازم لإدارة المواقع الإلكترونية ، ويتم الطلب بالتنسيق مع وحدة البوابة الإلكترونية على وسائل التواصل المبيّنة أدناه .

٧.سياسة المواقع و الخدمات الإلكترونية للجامعة :

أ. لوحدة البوابة الإلكترونية الحق في عدم ربط أي موقع فرعي مع بوابة الجامعة الإلكترونية ، في حال مخالفته لسياسة الخصوصية الخاصة ببوابة الجامعة الإلكترونية .

ب. توفر وحدة البوابة الإلكترونية نطاقات فرعية مختصرة لكل جهة وذلك حسب البريد الإلكتروني الرسمي للجهة ، مثال : كلية الهندسة mu.sa/ce ، عمادة تقنية المعلومات mu.sa/dit .

ج. عند تدشين خدمة الكترونية خارج نظام ادارة المحتوى الخاص بالبوابة الالكترونية من قبل أحد الجهات التابعة للجامعة, يجب أن تحقق هذه الخدمة الشروط التالية:

١. استضافة الخدمة في مركز بيانات عمادة تقنية المعلومات بالجامعة .

٢. ربط الخدمة بنطاق فرعي تابع للنطاق الرئيسي mu.edu.sa ، على أن يتم ربط شعار الجامعة في الصفحة الرئيسية للخدمة برابط مباشر لبوابة الجامعة الرئيسية www.mu.edu.sa وكذلك إدراج عبارة (جامعة المجمعة) في أسفل الصفحة الرئيسية للخدمة وربطها ببوابة الجامعة الرئيسية .

٣. ربط الخدمة بنظام الدخول الموحد لخدمات الجامعة (SSO) .

٤. يجب أن تحتوي الصفحة الرئيسية للخدمة على بيانات التواصل مع جهة الخدمة .

٥. عدم احتواء الخدمة على محتوى يمكن تضمينه في البوابة الفرعية للجهة .

٦. يجب أن تكون الخدمة عبارة عن أنظمة تفاعلية مع الزوار أو خدمات إلكترونية .

د. النطاق الفرعي سيكون متفرعاً من النطاق الرئيسي للجامعة : mu.edu.sa ، ويتم اقتراح اسم النطاق الفرعي المطلوب من قبل نفس الجهة ذات العلاقة ، ويحق لوحدة البوابة الإلكترونية قبول اسم النطاق أو رفضه أو تعديله بحسب ما تراه مناسباً .

٥. يجب أخذ الموافقة من وحدة البوابة الإلكترونية للقالب العام للخدمة ، كما يجب أن تحتوي الخدمة على وسائل التواصل مع الجهة مثل (رقم الهاتف / التحويلة / الفاكس / البريد الإلكتروني / ... الخ) .

٨. سياسة تأمين خدمات (أنظمة) إلكترونية جديدة :

تحدد هذه السياسة الاشتراطات الواجب توفرها في حال رغبت أي جهة تأمين خدمة إلكترونية جديدة .

أولاً : تأمين الخدمة عن طريق عمادة تقنية المعلومات :

يمكن لأي جهة تتبع للجامعة طلب تنفيذ خدمة إلكترونية و ذلك عن طريق عمادة تقنية المعلومات وستتكفل العمادة بتحليل و تصميم و تنفيذ الخدمة ، و كذلك استضافتها وتشغيلها في خوادم الجامعة ، وتأمين الحماية اللازمة لها ، والنسخ الاحتياطي .

ثانياً : تأمين الخدمة عن طريق الجهة نفسها :

يمكن للجهة تأمين أي خدمة إلكترونية عن طريقها (مبرمج خاص / شركة) ، مع وجوب توفر الاشتراطات التالية :

أ. يجب التنسيق بين الجهة ذات العلاقة و بين عمادة تقنية المعلومات قبل تأمين أي خدمة إلكترونية ، وذلك لمنع الازدواجية (وجود خدمة إلكترونية مشابهة) ، أو وجود خيارات أفضل تقترحها العمادة للجهة .

ب. يجب على الجهة أن تمتلك حقوق ملكية الخدمة التي تريد تأمينها بما فيها قواعد البيانات ، وذلك لحفظ حقوقها لاحقاً .

ج. لا يمكن للعمادة منح نطاق فرعي لأي خدمة إلكترونية لا تحقق الشروط الواردة في الفقرة (٧ ، البند ج) الواردة أعلاه.

٩. سياسة أمن المعلومات :

أ. تستخدم وحدة البوابة الإلكترونية أساليب اجرائية وتقنية لوقاية وحماية المعلومات الشخصية من الضياع أو السرقة أو الاطلاع من قبل أشخاص غير مصرح لهم ، وذلك عن طريق حفظها على شكل بيانات مشفرة ، وتتعامل الوحدة مع البيانات كممتلكات لابد أن تتم حمايتها من الضياع أو الاطلاع من قبل أي أشخاص غير مصرح لهم .

ب. في حال تعرض بوابة الجامعة لأي نوع من أنواع الإضرار بقصد الإيذاء أو غير ذلك ، فسيتم اتخاذ الإجراءات والعقوبات اللازمة للمتسبب بحسب نظام مكافحة الجرائم المعلوماتية ١٤٢٨ هـ .

ج. كما أنه في حال اكتشاف ما يُسبب تهديد أمني لبوابة الجامعة الإلكترونية أو الخدمات الإلكترونية التابعة لها ، فيحق لوحدة البوابة الإلكترونية باتخاذ الإجراء الوقائي اللازم .

١٠. سياسة النشر :
بوابة جامعة المجمعة الإلكترونية هي وسيلة نشر إلكتروني ، و واجهة إعلامية للجامعة ، و لجميع منسوبي وقطاعات الجامعة ويجب استخدامها فيما يعود بالنفع على الجامعة ومنسوبيها وقطاعاتها المختلفة وبما لا يخل بأي شكل من الأشكال بسمعة الجامعة ومنسوبيها أو يعرضهم للمسائلة القانونية ، لذا يجب التأكد من إتباع سياسات النشر المذكورة في هذه الوثيقة . و التأكيد على ترجمة أي محتوى مدخل للغة الإنجليزية و العكس .

١١. حقوق النشر :
جميع المحتويات المنشورة في صفحات البوابة يجب أن تتوافق مع حقوق النشر وسياسة النشر الإلكتروني بالجامعة وهذا يشمل التالي :

- البحوث المنشورة في مؤتمرات علمية ومجلات علمية .
- الكتب والمؤلفات المتوفرة بصيغة إلكترونية .
- أي مواد إلكترونية تنتهك حقوق الملكية الفكرية .

١٢. المحتوى غير الملائم :
وهذا المحتوى يشمل التالي :
أ. ما يحتوي على لهجة نابية أو متهجمة أو عنصرية أو مهددة سواء كان نصاً أو صورة أو فكرة .
ب. ما هو مخالف لأنظمة الدولة والجامعة أو أعراف المجتمع .
ج. ما فيه تعرض لخصوصية الآخرين بأي شكل من الأشكال .
د. مع التأكيد على مراعاة قواعد اللغة المستخدمة لإنشاء الصفحة أو المادة الإلكترونية والتأكد من سلامتها وخلوها من الأخطاء ، وتحتفظ وحدة البوابة الإلكترونية بحقها في مراجعة أي مادة أو محتوى منشور و التعامل مع ما تراه غير ملائم .

١٣. حداثة المعلومات :
يجب التأكد من تحديث محتوى الصفحات والمواد المختلفة بشكل يضمن حداثتها وقت الزيارة ، وهذا يشمل الأخبار ومعلومات الاتصال وأرقام الهواتف والبريد الإلكتروني ووصف المواد وغيرها من المعلومات .

١٤. تغيير سياسات البوابة الإلكترونية للجامعة :
تحتفظ وحدة البوابة الإلكترونية بعمادة تقنية المعلومات بالحق الكامل في تغيير هذه السياسة عند الضرورة دون سابق إنذار ، مع الإشارة إلى أن هذه السياسة متاحة من خلال بوابة الجامعة الإلكترونية (أسفل صفحات البوابة) .

١٥. إخلاء مسؤولية :
تبذل عمادة تقنية المعلومات أقصى جهودها لتحقيق مستوى عالي من الجودة والدقة في بوابة الجامعة الإلكترونية ، إلا أنها لا تتحمل أي مسئولية أو تبعات قد تنتج إثر مخالفة السياسات المبيّنة أعلاه .

سياسة الاستخدام المقبول

١- نظرة عامة:

وضعت هذه السياسة لحماية الجامعة وموظفيها من عواقب الأعمال غير المشروعة من قبل الأفراد الذين يستخدمون شبكة الجامعة.
تضم شبكة جامعة المجمعة: أنظمة ذات الصلة بالاكسترانت/ الإنترنت / الانترانت بما في ذلك أجهزة الكمبيوتر والشبكة والبرامج وأنظمة التشغيل ووسائط التخزين وحسابات المستخدمين والتراسل الفوري ونظام تخطيط موارد المؤسسات والتصفح و مشاركة الملفات والتي جميعها تخدم احتياجات الجامعة بالإضافة إلى جميع المستخدمين. إن الحماية الفعالة لأجهزة الحاسب تتطلب تظافر جهود جميع الموظفين بما فيهم المستخدمين المصرح لهم بالتعامل مع المعلومات و نظم المعلومات. لذلك كل مستخدم للكمبيوتر مطالب بمعرفة الأنظمة والسياسات الخاصة باستخدام شبكة الجامعة والالتزام بما فيها من إجراءات.

٢- الهدف:

تهدف هذه السياسة إلى وصف الشروط الخاصة المتعلقة بالحصول على تصريح باستخدام الشبكة وحماية المستخدمين المصرح لهم وأن أي استخدام غير مصرح به قد يعرض الجامعة إلى العديد من المخاطر بما في ذلك المسؤولية القانونية والفيروسات ونظم الشبكات والخدمات والمعلومات.

٣- النطاق:

تنطبق هذه السياسة على جميع الأشخاص الذين يعملون على أجهزة الجامعة المتصلة بالشبكة أو حتى الأجهزة الشخصية والمتصلة بشبكة جامعة المجمعة.

٤- السياسة العامة

A. الإستخدام العام والملكية

- إن البيانات التي يتم إنشاؤها من قبل المستخدمين المصرح لهم على شبكة الجامعة تعتبر ملك للجامعة و ليس هناك ما يضمن سرية المعلومات المخزنة على شبكة الجامعة.
- إن الاستعمال المرخص للشبكة يقتضي استخدام شخصي مقبول للشبكة من قبل المستخدمين المصرح لهم. وعليه فإن الإدارات مسؤولة عن وضع إراشادات للاستخدام الشخصي لشبكة الجامعة وفي حالة عدم توفر الإرشادات اللازمة, فإن على المستخدمين استشارة عمادة تقنية المعلومات.
- إن أي معلومات تعتبر من قبل المستخدم هامة أو حساسة يجب أن يتم تشفيرها. لمزيد من المعلومات حول تشفير البريد والمستندات يرجى التواصل مع عمادة تقنية المعلومات.
- قد تخضع شبكة جامعة المجمعة والبيانات المتدفقة في أي وقت للمراقبة الأمنية والفنية من قبل موظفين مصرح لهم من عمادة تقنية المعلومات, وذلك بما يتوافق مع إجراءات أمن المعلومات.
- إن عمادة تقنية المعلومات في الجامعة لها الحق في مراجعة وتدقيق الشبكات والأنظمة بشكل دوري لضمان مطابقتها لسياساتها وإجراءاتها.

B. معلومات الحماية والملكية

- ينبغي على المستخدمين المصرح لهم تصنيف البيانات الموجودة على شبكة جامعة المجمعة إلى «معلومات سرية» أو «معلومات غير سرية»، كما هو مذكور في إرشادات الجامعة السرية. وتتضمن المعلومات السرية ,على سبيل المثال لا الحصر: بيانات الجامعة الخاصة والمواصفات ومعلومات الموظف والبيانات البحثية. لذلك كل موظفي قسم تقنية المعلومات مطالبين باتخاذ جميع الخطوات اللازمة لمنع الوصول غير المصرح به إلى هذه المعلومات المهمة.
- يجب من جميع المستخدمين المرخص لهم باستخدام الشبكة عدم اطلاع الاخرين على كلمات المرور والحسابات الخاصة بهم.
- يجب على جميع المستخدمين عمل «تسجيل خروج» أو على الأقل إغلاق جميع الأنظمة والحسابات في حال عدم استخدامها.
- يجب أن يكون تشفير المعلومات مطابقا للاستخدام الصحيح للتشفير الخاص بسياسة أمن المعلومات.
- يجب على المستخدمين المرخص لهم العناية بالأجهزة المحمولة والتي هي جزء من أو متصلة بشبكة جامعة المجمعة وفقا لـ «دليل حماية الأجهزة المحمولة.»
- عند إضافة مواد من قبل المستخدمين المصرح لهم, فإن على المستخدمين وضع تنويه بأن هذه الأفكار لا تمثل بالضرورة الجامعة وإنما هي آراء شخصية إلا في حالة كون هذه المواد جزء من عمل الجامعة.
- يجب أن يتم فحص جميع أجهزة الكمبيوتر المتصلة بشبكة الجامعة والمستخدمة من قبل المستخدمين المصرح لهم، سواء الأجهزة المملوكة للأفراد أو للجامعة، بشكل دوري عن طريق برنامج فحص الفيروسات الخاص بالجامعة
- يجب على جميع المستخدمين المصرح لهم توخي الحذر الشديد عند فتح مرفقات البريد الإلكتروني المرسلة من أشخاص غير معروفين، والتي قد تحتوي على فيروسات وقنابل البريد الإلكتروني، أو رموز حصان طروادة.

C. الاستخدام غير المقبول لشبكة جامعة المجمعة.

يمنع ممارسة الأنشطة التالية إلا للموظفين المصرح لهم أثناء أداءهم لواجباتهم الوظيفية. كما لا يسمح لأي مستخدم بالانخراط في أي نشاط غير قانوني أثناء استخدام شبكة جامعة المجمعة بموجب القانون المحلي والدولي.

هناك أشكالا عدة للاستخدام غير المقبول وليس مقتصرا على الأنشطة التالية:

الأنشطة الخاصة بالنظام والشبكة :
يمنع وبدون أي استثناءات ممارسة الأنشطة التالية:

- انتهاكات حقوق أي شخص أو منظمة محمية بموجب حقوق الطبع والنشر، والأسرار التجارية، وبراءات الاختراع أو غيرها من الممتلكات الفكرية، أو قوانين أو لوائح مماثلة، بما في ذلك، وليس على سبيل الحصر، تثبيت أو توزيع برامج ليست مرخصة للاستخدام من قبل الجامعة.
- إجراء أي نوع من أنوع النسخ الغير مصرح به والذي يتضمن (ليس على سبيل الحصر) النسخ الرقمي و توزيع الصور من المجلات أو الكتب أو غيرها من المصادر , أو حتى تثبيت أي برامج لها حقوق الطبع والنشر والجامعة لا تمتلك رخصة استخدامها.
- إن تصدير أي برمجيات، أو معلومات تقنية، أو برامج تشفير بشكل فيه انتهاك للقوانين الدولية أو الإقليمية يعتبر غير قانوني ويجب استشارة الجهة المسؤولة عن أي محتويات قبل نشرها.
- إدخال برمجيات ضارة إلى شبكة الجامعة (على سبيل المثال, الفيروسات

وأحصنة طروادة، وقنابل البريد الإلكتروني، الخ).

- إفصاح المستخدم المصرح له عن كلمة المرور الخاصة بحسابه أو السماح للآخرين بالدخول للحساب بما فيهم أعضاء العائلة في حالة اتصال جهاز الحاسب بشبكة الجامعة سواء من المنزل أو أي مكان آخر خارج الجامعة.
- استخدام أحد مكونات الشبكة أو غيرها في عمل أو نقل مواد تنتهك قوانين التحرش الجنسي أو قوانين العمل أو أي منظمة أخرى. وتعتبر المواد الإباحية هي انتهاك لسياسات التحرش الجنسي.
- تقديم عروض احتيالية لمنتجات ومواد أو خدمات عن طريق أي حساب لجهاز متصل بشبكة الجامعة.
- التسبب في اختراقات أمنية أو انقطاع الاتصالات على شبكة الجامعة. وتشتمل الاختراقات الأمنية, على سبيل المثال لا الحصر، اطلاع المستخدم على بيانات أو اتصالات ليس مخولا بها أو تسجيل الدخول إلى حساب مستخدم آخر. أما فيما يخص انقطاع الاتصالات فمثلا ، التسلل للشبكة إغراق الشبكة، إنتحال عنوان رقمي, وإيقاف الخدمة، الخ
- فحص المنافذ أو الحماية عموماً من غير تنسيق مسبق مع إدارة أمن المعلومات.
- إجراء أي شكل من أشكال مراقبة الشبكة من قبل مستخدمين غير مصرح لهم بذلك.
- التحايل للحصول على حساب مستخدم, أو تجاوز حماية أي جهاز أو شبكة أو حساب شخصي.
- التداخل مع أو رفض خدمة أي مستخدم آخر غير الشخص المضيف.
- استخدام أي برنامج/ نص/ أمر، أو إرسال أي نوع من الرسائل بقصد التدخل أو تعطيل اتصال المستخدم بالشبكة.
- الإدلاء بمعلومات أو قوائم خاصة بموظفي الجامعة أو الطلاب إلى جهات ليس لها علاقة بالجامعة.

أنشطة البريد الإلكتروني والاتصالات

- إرسال رسائل غير مرغوب فيها بالبريد الإلكتروني، بما في ذلك «الرسائل المزعجة» أو غيرها من المواد الإعلانية للأفراد الذين لم يتواصلوا مع هذه الجهات (Email SPAM).
- القيام بأي شكل من أشكال الإزعاج عبر البريد الإلكتروني، والرسائل الفورية، والهاتف، أو النداء الآلي, سواءً بإستخدام اللغة، نبرة الصوت، أو التزوير باستخدام معلومات البريد الالكترونية.
- الاستخدام غير المصرح به أو تزييف عناوين رسائل بالبريد الإلكتروني.
- استخدام بريد الكتروني غير مصرح به لغرض إلحاق الضرر بالأخرين أو الحصول على عدة ردود.
- إنشاء أو إعادة توجيه على نفس البريد الإلكتروني أو أي نوع آخر من أنواع الخداع.
- ٦- استخدام اسم المنشأة في البريد الإلكتروني بغرض الإعلان لأي خدمة أو منتج دون إذن خطي من المنشأة.
- ٧. نشر رسائل ليس لها علاقة بعمل المنشأة لأعداد كبيرة من المجموعات البريدية.

٥- تطبيق القانون

- في حالة مخالفة أو انتهاك هذه السياسة من قبل أي مستخدم في الجامعة فإنه سيعتبر مستخدم غير مصرح له وبذلك يخضع لإجراءات تأديبية وفقا لسياسة الاستخدام غير المصرح به.

سياسة مكافحة البرمجيات الضارة

١- نظرة عامة:
هذه السياسة الداخلية خاصة بتقنية المعلومات والتي تحدد سياسة مكافحة الفيروسات على كل أجهزة الحاسب بما في ذلك كيفية فحص الفيروسات و إجراء التحديثات بشكل دوري وماهي أفضل البرامج لكشف أو منع وإزالة البرامج الضارة. هذه السياسة أيضا تحدد أنواع الملفات التي يتم حظرها من قبل خادم البريد وأي برنامج مكافحة الفيروسات سيتم تشغيله على خادم البريد وما إذا كان هناك ضرورة لاستخدام جدار الحماية الخاص بمحاربة الـ(spam). من الأشياء التي تتطرق لها هذه السياسة أيضا هو كيفية دخول الملفات للشبكة وكيف يتم فحص محتوى هذه الملفات فيما اذا كانت تحتوي على أشياء ضارة وغير مرغوب بها. فعلى سبيل المثال يمكن تحديد الملفات المرسلة إلى مؤسسة معينة من خارج نطاق شبكتها وفحص هذه الملفات بواسطة برنامج معين للتأكد من أنها لا تحتوي على فيروسات. من الأشياء التي تتطرق لها هذه السياسة أيضا هو كيفية دخول الملفات للشبكة وكيف يتم فحص محتوى هذه الملفات فيما اذا كانت تحتوي على محتويات ضارة وغير مرغوب بها. فعلى سبيل المثال تخضع الملفات التي يتم استلامها من خارج الشبكة الموثوقة للجامعة للفحص ضد البرمجيات الخبيثة بواسطة برنامج خاص.-

٢- الهدف:
تم إعداد هذه السياسة لحماية موارد الجامعة من أي هجوم عن طريق البرمجيات الخبيثة أو أي برامج ضارة أخرى.

٣- إجراءات مكافحة الفيروسات:
تستخدم الجامعة منتجين من شركة TrendMicro لمكافحة البرمجيات الخبيثة, حيث يستخدم للأجهزة الشخصية المنتج المسمى Officescan ويستخدم للخوادم المنتج المسمى Deep Security. ولضمان جودة ومفعول المنتجين لابد من توفر الحد الأدنى من المتطلبات التالية:

١. يجب أن يتم ضبط المنتجين على وضع «الكشف طوال الوقت» للبرمجيات الخبيثة «Real-time».
٢. يجب تحديث قاعدة بيانات المنتجين بشكل يومي على الأقل.
٣. يجب ضبط المنتجين لإجراء فحص دوري للبرمجيات الضارة بشكل أسبوعي على الأقل.
٤. غير مصرح لأي أحد بإيقاف المنتجين أو حذفهم أو إيقاف عمليات الفحص والتحديث إلا من قبل الموظف المختص بإدارة المنتجين في إدارة أمن المعلومات.

٤- الإجراءات المتعلقة بخادم البريد الإلكتروني
يجب توفير حماية إضافية لخادم البريد الإلكتروني ضد البرمجيات الضارة إذ أنه لابد من منع البريد الإلكتروني والبرمجيات الضارة من دخول الشبكة.

A. فحص البرامج الضارة في البريد الإلكتروني
بالإضافة لمنتج مكافح البرمجيات الضارة، يستخدم لخادم البريد الإلكتروني على منتج إضافي والمسمى (ScanMail) مقدم من شركة (TrendMicro) والذي يستخدم لفحص رسائل البريد الإلكتروني ضد البرمجيات ضارة. حيث يقوم بفحص الرسائل في حال دخولها الخادم وحال خروجها أيضاً. بالإضافة لذلك, يقوم المنتج بفحص جميع رسائل البريد الإلكتروني المخزنة مرة واحدة أسبوعيا.

في حال تم العثور على فيروس أو تم العثور على أي برنامج ضار, فإن الإجراءات تقتضي حذف البريد الإلكتروني من غير إشعار المرسل أو المتلقي. والسبب في ذلك هو أن معظم البرمجيات الخبيثة توهم المرسل عن طريق إرسال إشعار بأنه تم إرسال رسالة تحتوي على فيروس , الأمر الذي قد يؤدي إلى إخافة المرسل بالرغم من عدم ثبوت الأمر. وهذا قد يؤدي إلى تواصل الشخص بوحدة العناية بالمستفيدين للاستفسار وفي غالب الأحيان يتسبب ذلك في إضاعة وقت وجهد المسؤول عن النظام من غير فائدة. وفي المقابل أيضاً, فإن محاولة إشعار المتلقي بأن هناك محاولة لإرسال فايروس قد يتسبب في إخافة المتلقي وبالتالي يتسبب في زيادة عدد المكالمات لوحدة العناية بالمستفيدين.

B. أنواع المرفقات المحظوره:
يسمح في بريد الجامعة تبادل المرفقات النصية والتي تشمل ملفات محرر النصوص, العروض التقديمية, جداول البيانات, المستندات المعدة للقراءة فقط (PDF), إضافة إلى ملفات الصور بشتى أنواعها والملفات المؤرشفة. وعليه, يمنع مشاركة الملفات التنفيذية, الملفات البرمجية ونحوها.

٥- تطبيق القانون:
تعتبر محاولة حذف أو إيقاف أو تخريب أي من منتجات مكافحة البرمجيات الضارة الخاصة والمثبتة على الأجهزة المكتبية والمحمولة المملوكة للجامعة تعدي على أمن الجامعة ويخضع المتسبب بذلك للإجراءات التأديبية.

سياسة التطبيقات المعتمدة

١- نظرة عامة:
يجب على جميع الموظفين والعاملين الذين يستخدمون أنظمة الكمبيوتر الخاصة بالجامعة الالتزام بسياسة التطبيقات المعتمدة من أجل حماية أمن الشبكة، وسلامة البيانات، وأنظمة الكمبيوتر.

٢- الهدف:
تم إعداد هذه السياسة من أجل حماية موارد الجامعة على الشبكة عن طريق إلزام جميع مستخدمي الشبكة بتشغيل أو تثبيت البرامج التطبيقية التي تعتبر آمنة من قبل عمادة تقنية المعلومات.

٣- التطبيقات المعتمدة:
يمكن لجميع الموظفين تشغيل البرامج الموجودة على قائمة التطبيقات المعتمدة. أما في حال إذا أراد الموظف استخدام تطبيق ليس موجودا على القائمة، فينبغي حينها أن يعرض البرنامج على عمادة تقنية المعلومات للموافقة عليه قبل استخدامه على النظام المتصل بالشبكة.
في حالة تسبب الموظف في مشكلة أمنية على الشبكة عن طريق تثبيت وتشغيل برنامج غير معتمد فإنه يخضع لإجراءات تأديبية.

٤- الاستثناءات:
هناك استثناءات معينة لبعض الموظفين لمن لديهم مهام خاصة ولديهم مهارات معينة مثل:
- في حال قيام الموظف بتجربة أو اختبار تطبيقات جديدة على الشبكة التجريبية، ومن ثم على الشبكة الرئيسية.
- في حال كون الموظف مبرمج وأراد أن يجرب إحدى البرامج التي صممها بنفسه.
- يسمح لمسؤول الشبكة بتشغيل واختبار البرمجيات الجديدة.

٥- تطبيق القانون:
بما أن تشغيل برامج آمنة هو أمر هام جدا من أجل حماية الشبكة الخاصة بالجامعة, فإن أي موظف لا يلتزم بهذه السياسة سوف يخضع لإجراءات تأديبية وقد تصل إلى استبعاده من الشبكة.

٦- البرامج المعتمدة:
- IT department approved applications are listed below.
- Windows Operating system
- Microsoft Office Suite
- Microsoft Axapta
- Mozilla firefox
- Microsoft Internet Explorer
- Adobe Acrobat
- Microsoft Visio
- Symantec/ Trend micro Antivirus
- Roxio Easy CD Creator
- WinZip
- WinRAR
- Nero CD Creator
- Citrix Web client
- Power Archiver
- AutoCAD
- PDF writer

سياسة إدارة التغيير

١. الهدف:
تهدف هذه السياسة إلى وضع عملية منهجية لتوثيق وإدارة التغييرات لشبكة عمادة تقنية المعلومات في الجامعة من أجل السماح للتخطيط الفعال من قبل المختصين بالعمادة لخدمة قاعدة المستخدمين في الجامعة.

٢. النطاق:
تنطبق هذه السياسة على جميع المستخدمين المصرح لهم بتركيب والحفاظ على موارد عمادة تقنية المعلومات، بما في ذلك وليس على سبيل الحصر: أجهزة الحاسب والبرمجيات، وأجهزة الشبكات.

٣. السياسة:
أي تغيير على موارد تقنية المعلومات في العمادة والشبكات التابعة لها فهو خاضع لهذه السياسة، ويجب أن يتم وفق إجراءات إدارة التغيير في الجامعة. إن جميع التغييرات التي تؤثر على المرافق المحيطة بالموظف في عمادة تقنية المعلومات والشبكات بما في ذلك تكييف الهواء، والمياه، والحرارة، والسباكة، والكهرباء، وأجهزة الإنذار، يجب الإبلاغ عنها والتنسيق مع العمادة. كما يجب تقديم طلب تغيير رسمي مكتوب إلى عمادة تقنية المعلومات بكافة التغييرات، سواء المجدولة وغير المجدولة.

كما يجب تقديم جميع طلبات التغيير إلى لجنة إدارة التغيير وفقا للإجراءات ،وذلك للنظر في الطلب واتخاذ القرار إما بقبول الطلب أو تأجيله. كما يجوز للجنة عمل أي تغييرات سواء كانت مجدولة أو غير مجدولة وذلك لأسباب منها: عدم كفاية التخطيط، عدم كفاية خطط الارتداد، والأثر السلبي لتوقيت التغيير على العمل، أو عدم كفاية الموارد المتاحة.

يجب أن تكون هناك مراجعة لكل عملية تغيير في المنظمة سواء كانت مجدولة أو غير مجدولة وسواء كانت قد تمت أو لم تتم.

يجب أن يكون هناك حساب خاص بإدارة التغييرات وأن يحتوي على التالي:

- تاريخ التقديم
- طلب التغيير
- تاريخ التغيير
- القائم بعملية التغيير
- طبيعة التغيير
- نتائج التغيير

٤. تطبيق القانون:
في حالة انتهاك هذه السياسة من قبل أي مستخدم مرخص له, فإنه يعتبر غير مرخص له ويخضع لإجراءات تأديبية وفقا لبند تطبيق القانون الموجود في سياسة الاستخدام الغير مرخص به.

سياسة مراقبة الأصول

١. نظرة عامة:

يجب على جميع الموظفين والعاملين الذين يستخدمون أنظمة الكمبيوتر الخاصة بالجامعة الالتزام بسياسة مراقبة الأصول الموضحة أدناه من أجل حماية أمن الشبكة، وسلامة البيانات، وأنظمة الكمبيوتر. إن سياسة مراقبة الأصول لن تمكن الجامعة فقط من تعقب أماكن ومستخدمي الأصول، بل ستحمي أيضا البيانات الموجودة على هذه الأصول. كما تتضمن هذه السياسة مخلفات الأصول.

عدم الخلط بين أصول عمادة تقنية المعلومات مع أصول الجامعة الأخرى مثل الأثاث.

واحد من أهم الأسباب الرئيسية لتتبع أصول عمادة تقنية المعلومات هي أمور أمنية متعلقة بالكمبيوتر. إن وجود سياسة خاصة لتتبع أصول العمادة سيمكن الجامعة من اتخاذ التدابير اللازمة لحماية البيانات وموارد الشبكات. هذه السياسة تحدد ما يجب القيام به عندما يتم نقل قطعة من الممتلكات من مبنى إلى آخر أو من موقع إلى آخر. هذه السياسة أيضا توفر قاعدة بيانات لتتبع الأصول ويتم تحديثها حتى يتم معرفة مواقع أجهزة الحاسب. كما تساعد هذه السياسة مسؤولي الشبكة على حماية الشبكة لأنها سوف تزودهم بمعلومات عن المستخدمين ومواقعهم في حالة وجود دودة (worm) قد تؤثر على الشبكة. كما تشمل هذه السياسة أيضا إمكانية حماية البيانات الحساسة في أجهزة الحاسب أثناء نقلها من موقع لآخر.

٢. الغرض:

تم إعداد هذه السياسة من أجل حماية موارد الجامعة على الشبكة من خلال وضع سياسات وإجراءات لمراقبة الأصول. كما ستساعد هذه السياسات في الحد من فقدان البيانات أو الأصول الناتج عن سوء التخطيط.

٣. تعقب الأصول:

يحدد هذا القسم من السياسة ما يجب تتبعه من أصول تقنية المعلومات وإلى أي مدى يكون هذا التتبع.

أ- أنواع الأصول الخاصة بتقنية المعلومات

فيما يلي قائمة بأنواع الأصول التي يجب تتبعها:

١. محطة العمل المكتبية
٢. أجهزة الكمبيوتر والمحمول والهاتف
٣. الطابعات، وآلات التصوير وأجهزة الفاكس، وآلات متعددة الوظائف
٤. الأجهزة المحمولة
٥. الماسحات الضوئية
٦. خوادم
٧. الجدران النارية (firewalls)
٨. الموجهات
٩. المفاتيح
١٠. أجهزة الذاكرة

ب- الأصول التي يجب تتبعها:

ليس هناك داعي من تتبع الأصول التي تقدر تكلفتها بأقل من ١٠٠ ريال سعودي بما في ذلك مكونات الكمبيوتر مثل بطاقات الفيديو أو بطاقات الصوت. أما الأصول التي تقوم بتخزين البيانات فيجب تتبعها بغض النظر عن التكلفة مثل:

١. محركات الأقراص الصلبة
٢. محركات أقراص التخزين المؤقتة
٣. الأشرطة مع البيانات المخزنة عليها بما في ذلك البيانات الاحتياطية للنظام.
٤. الأقراص المضغوطة CD والأقراص المرنة.

ت- أجهزة الذاكرة الصغيرة

لن يتم تعقب الأصول مثل ذاكرة التخزين الصغيرة عن طريق الموقع ولكن عن طريق العهدة. وتشمل هذه الأصول التالي:

١. الأقراص المرنة
٢. أقراص CD ROM
٣. عصا الذاكرة

إذا تم السماح لأحد الموظفين باستخدام هذه الأجهزة، فيجب على المستخدم التوقيع لاستلام هذه الأجهزة التي في حوزته. كما يجب على جميع الموظفين استخدام هذه الأجهزة بشكل مناسب واتباع التعليمات التالية:

- عدم حفظ بيانات ذات أهمية على الجهاز من غير إذن مسبق، وفي حالة وضع بيانات ذات أهمية، فإن ذلك يجب أن يكون مسبوق بإذن خاص ويتم حفظ الجهاز في مكان آمن.
- عدم استخدام هذه الأجهزة لجلب برامج قابلة للتنفيذ من خارج الشبكة دون ترخيص ودون فحص البرنامج عن طريق برنامج مكافح فيروسات معتمد ومحدث وأن يكون ضمن قائمة البرامج المعتمدة من قبل قسم تقنية المعلومات.

عند توقيع الموظف على عهدة استلام هذه الأجهزة، فإن عليه الالتزام بما ورد فيها من شروط. ويجب أن يقوم جميع الموظفين الذين يعملون في أي منظمة للبيانات بالتوقيع على هذه العهدة عند مباشرتهم للعمل.

٤. متطلبات تتبع الأصول:

- يجب أن تحتوي جميع الأصول على رقم معرف ويكون هذا الرقم معطى من قبل الجامعة أو يتم استخدام رقم التصنيع في وقت الحاجة إليه.
- يجب إنشاء قاعدة بيانات لتتبع الأصول وأن تحتوي على جميع معلومات نقل الاصول أو تغييرها.
- عند استلام الأصول، يوضع رقم معرف للموجودات ويتم إدخال المعلومات في قاعدة بيانات تتبع الأصول.

٥. إجراءات النقل:

١. قائمة التأكد من نقل الأصول:

عندما يتم نقل نوع من أنواع الأصول المدرجة على القائمة إلى موقع جديد أو متعهد جديد، يجب وضع اسم المتعهد الجديد ويتم الموافقة على الطلب من قبل جهة مختصة. إذا كان الشيء المستخدم هو محطة عمل، فإن المتعهد هو أكثر المستخدمين لهذا المكان. أما فيما يخص باقي الأجهزة فإن المتعهد هو الشخص المسؤول عن الصيانة أو الإشراف على هذه الأجهزة.

يجب على المتعهد ملئ نموذج خاص بالعهدة ويجب ذكر فيما إذا كانت الأصول جديدة أو تم نقلها إلى موقع جديد أو تسليمها لمتعهد آخر أو التخلص منها.. الخ . فيما يلي المعلومات التي يجب تعبئتها:

١. نوع الأصول
٢. رقم المعرف
٣. اسم الأصول
٤. الموقع الحالي

٥. اسم المتعهد
٦. الموقع الجديد
٧. المتعهد الجديد
٨. مواقع البيانات الحساسة وذات الأهمية
عندما يقوم المتعهد بتعبئة النموذج والتوقيع عليه, يجب أن يتم التوقيع على النموذج من قبل المسؤول.

٢. إدخال البيانات :
بعد اكتمال تعبئة النموذج الخاص بنقل الأصول, يعطى النموذج لمسؤول قاعدة بيانات تتبع الأصول والذي بدوره يقوم بإدخال المعلومات الموجودة على النموذج في مدة اقصاها أسبوع.

٣. فحص قاعدة البيانات :
يجب على المدراء الذين يديرون مشاريع تتعلق بنقل المعدات بشكل دوري التحقق لمعرفة ما إذا تم إضافة الأصول التي تم نقلها مؤخرا إلى قاعدة البيانات. ويجب أن تحتوي قاعدة البيانات على قائمة محدثة يمكن التحقق من خلالها بسهولة. كما ينبغي على المسؤول مراجعة قاعدة البيانات أسبوعيا للتأكد من أن الموجودات التي تم نقلها خلال أسبوعين أو ثلاثة قد تم إدراجها في قاعدة البيانات.

٦. تحويلات الأصول:
تنطبق هذه السياسة على أي تحويلات للأصول بما في ذلك ما يلي:
- شراء الأصول
- نقل الأصول
- تغيير صاحب العهدة عند مغادرته أو نقله لمكان آخر.
- التصرف في الأصول

في كل هذه الحالات يجب أن تكتمل تعبئة النموذج الخاص بنقل الأصول.

٧. التخلص من الأصول:
في حالة التخلص من الأصول يجب التأكد من إزالة جميع البيانات الحساسة وذات أهمية والتي يتم تحديد أهميتها من قبل المسؤول. وفيما يلي سرد لكيفية التعامل مع الأجهزة بناء على حساسية البيانات وفقا لعملية تقييم البيانات.

١. بيانات ليس ذات أهمية :
لا يشترط مسح البيانات ولكن من الحكمة مسحها باستخدام أي وسيلة مثل إعادة تهيئة.
٢. بيانات ذات أهمية : يتم إزالة البيانات باستخدام أي وسيلة مثل إعادة تهيئة.
٣. بيانات سرية وذات أهمية متوسطة :
في هذه الحالة يجب أن يتم مسح البيانات باستخدام تقنية معتمدة للتأكد من أنها غير قابلة للقراءة مرة أخرى.
٤. بيانات غاية في الأهمية (سرية) :
في هذه الحالة يجب أن يتم مسح البيانات باستخدام تقنية معتمدة للتأكد من أنها غير قابلة للقراءة مرة أخرى. إن التقنيات المعتمدة والمذكورة في وثيقة إجراءات إزالة وسائط البيانات تتضمن:
- القرص المرن
- عصا الذاكرة
- DVD أو CD ROM
- شريط التخزين
- القرص الصلب.
- ذاكرة RAM
- ذاكرة ROM أو أجهزة الذاكرة ROM.

٨. استخدام وسائط التخزين:
تحدد هذه السياسة أنواع البيانات التي يمكن تخزينها على وسائط التخزين القابلة للإزالة وما إذا كان سيتم إزالة هذه الوسائط وتحت أي ظرف. وسائط التخزين تشمل التالي:
١. القرص المرن
٢. عصا الذاكرة
٣. DVD أو CD ROM
٤. شريط التخزين

فيما يلي سرد لكيفية التعامل مع الأجهزة بناء على حساسية البيانات وفقا لعملية تقييم البيانات.
- **بيانات غير سرية** - يمكن إزالة البيانات بناء على موافقة المسؤول ويسري هذا القرار بشكل دائم مالم تقتضي الضرورة خلاف ذلك. كما يمكن نقل هذه الوسائط باستخدام أي وسيلة نقل سواء كانت عامة أو خاصة.
- **بيانات حساسة** - في هذه الحالة يجب أن لا تتم إزالة البيانات من المناطق الآمنة إلا بإذن المدير أو الإدارة العليا ويكون القرار ساري لمرة واحدة فقط.
- **بيانات سرية** - في هذه الحالة يجب أن لا تتم إزالة البيانات من المناطق الآمنة إلا بإذن نائب المسؤول أو الإدارة العليا ويجب أن تكون هناك بعض الاحتياطات الأمنية المعتمدة لطريقة النقل والوجهة.
- **بيانات سرية للغاية** - في هذه الحالة يجب أن لا تتم إزالة البيانات من المناطق الآمنة.

٩. تطبيق القانون:
بما أن أمن البيانات وسلامتها بالإضافة إلى حماية الموارد أمر بالغ الأهمية لعمل الجامعة، فإن عدم التزام الموظفين بهذه السياسة سوف يعرضهم لإجراءات تأديبية قد تصل إلى حد إنهاء خدماتهم. كما يرجى من كل موظف لدية علم بأي انتهاك لهذه السياسة إبلاغ مشرفه أو الجهة المختصة.

سياسة التدريب على الحاسب الآلي

إن سياسة التدريب على الحاسب الآلي وتدريب مستخدمي الكمبيوتر سوف يعود بالنفع على الجامعة في كل من زيادة الإنتاجية والتقليل من الحوادث الأمنية. تعتبر هذه السياسة عامة وتوضح بعض الجوانب التي تؤكد بأن تدريب المستخدم سيكون مفيدا جدا للجامعة.
ومع ذلك، فإنه من خلال النظر إلى أهمية حماية الحاسب في هذه الايام, وأن العديد من الهجمات التي تتعرض لها الجامعة تكون عن طريق المتصفح أو من خلال البريد الإلكتروني الخاص بالمستخدم، لذلك أصبح تدريب المستخدم أمرا ضروريا من أي وقت مضى. كما يجب تثقيف المستخدمين بأساليب الهجوم من أجل حماية أنفسهم في كثير من الحالات. إن تدريب المستخدمين لا يشترط أن يحتوي على أمور تقنية بالغة في الدقة ولكن يجب التأكد من أن المستخدم لديه علم بالأمور الأساسية المتعلقة بالحاسب إضافة إلى دراية بأنواع الهجمات التي قد يتعرض لها.

١. نظرة عامة:

تحدد هذه السياسة الحد الأدنى من التدريب للمستخدمين على الشبكة لتوعيتهم بالمخاطر الأساسية لحماية كل من أنفسهم والشبكة. تنطبق هذه السياسة بشكل خاص على الموظفين الذين لديهم إمكانية الوصول إلى البيانات الحساسة أو تنظيمها.

٢. الهدف:

تم صياغة هذه السياسة من أجل حماية موارد الجامعة على الشبكة وزيادة كفاءة الموظفين وذلك عن طريق وضع سياسة خاصة بتدريب المستخدمين. عندما يتم تدريب المستخدمين على استخدام الحاسب والتهديدات التي قد يتعرضون لها، فإن هذا يزيد من كفاءة المستخدمين و قدرتهم على حماية موارد المنظمة من أي تهديد خارجي.

٣. مستويات التدريب:

تشتمل مستويات التدريب على المجالات التالية:

- **الأساسيات:**
  - ما هي الملفات
  - كيفية استعراض ملف للحصول على التفاصيل وإظهار نوعه
  - لماذا يعتقد بأن امتدادات الملفات لا يعتبر خطر على أمن الجهاز
  - حجم تخزين الملف - كيفية تحديد ذلك
  - مرفقات البريد
  - مكان تخزين الملفات
  - كيفية استخدام محرك أقراص شبكة الاتصال الخاصة بك
  - ما هو محرك أقراص الشبكة الخاص بك وماذا يعني لك
  - كيفية نسخ الملفات
  - طرق لزيادة الكفاءة على الكمبيوتر مثل اختصارات لوحة المفاتيح

- **طرق للحصول على البرامج الضارة أو المزعجة :**
  - عن طريق البريد الالكتروني
  - من خلال المتصفح
  - من خلال الاتصال
  - عن طريق تثبيت برامج غير معتمدة

- **فيروسات البريد الإلكتروني:**
  - كيف تنتشر
  - انتحال المرسل لشخصية أخرى
  - مرفقات خطيرة

- **البريد الالكتروني غير المرغوب فيه:**
  - حماية عنوان البريد الإلكتروني الخاص بك
  - فحص البريد المزعج

- **الخدع:**
  - التصيد
  - أساليب الاحتيال

- **استخدام البريد الإلكتروني:**
  - كيفية عمل بريد إلكتروني للمستخدمين عن بعد أو مع ISP مع POP3
  - كيفية إعداد الرد من مكتب
  - كيفية وضع أسس لفحص البريد الإلكتروني
  - كيفية استخدام واستيراد وتصدير مجلدات شخصية
  - ماذا يعني عدم تسليم الرسالة

- **استخدام متصفح الإنترنت:**
  - متصفح آمن؟
  - تجنب برامج التجسس مثل adware and spyware - تجاهل الإعلانات التي قد تضر جهاز الكمبيوتر الخاص بك
  - كيفية تغيير إعدادات المتصفح لزيادة الأمان
  - منتجات لمنع البرامج الضارة.

- **كلمات السر:**
  - لماذا تتم حماية كلمة المرور الخاصة بي؟
  - لماذا أحتاج إلى تغيير كلمة السر كل ٣٠ يوما
  - كيفية تغيير كلمة السر الخاصة بك
  - كيفية اختيار كلمات مرور قوية يمكنك تذكرها
  - إذا قمت بتسجيل الدخول على موقع, هل يمكن لشخص ما معرفة كلمة المرور الخاصة بي؟

- **أخرى:**
  - أسباب جدار الحماية - الديدان (worms) وغيرها
  - لماذا القلق بشأن البرامج الضارة؟
  - ما هو الضعف؟
  - لماذا لا يتم تشغيل كافة الخدمات؟
  - الهندسة الاجتماعية

٤. فرص التدريب:

يجب توفير التدريب الأساسي كما هو موضح في القسم ٣ من قبل الجامعة، ويتضمن الفرص التالية:
حلقات تدريبية لمدة ١ إلى ٤ ساعات في اليوم الواحد.

٥. المتطلبات:

يجب على جميع الموظفين في الجامعة إحراز تقدم ملموس ومستمر في مجالات التدريب المدرجة في القسم ٣.ويتعين على كل مدير التأكد من أن الموظفين تحت إشرافه قد أحرزوا تقدم في مجالات التدريب المطلوبة. كما يجب على كل موظف الإلمام بمجالات التدريب المذكورة في القسم ٣ خلال السنة الأولى من عمله.

٦. تطبيق القانون:

بما أن التدريب مهم جدا لأمن المنظمة، فإنه يجب استخدام المتابعة كآلية للتأكد من أن سياسة التدريب فعالة. وتشمل آلية المتابعة اختبار الموظفين عشوائيا في المجالات المدرجة في القسم ٣.

سياسة النسخ الاحتياطي للبيانات

١. الهدف والنطاق :

إن الهدف من هذه السياسة هو ما يلي:

- حماية أصول المعلومات لجامعة المجمعة.
- منع فقدان البيانات في حالة وقوع الحذف العرضي أو تلف البيانات، أو فشل النظام، أو أي كوارث أخرى.
- استرجاع البيانات والعمليات في الوقت المناسب في حال حدوث أي طارئ مما سبق.
- إدارة وتأمين النسخ الاحتياطي وعمليات استرجاع البيانات.
- اختراقات امنية.

٢. تنطبق هذه السياسة على كافة الخوادم التابعة لعمادة تقنية المعلومات والمراكز، بما في ذلك التخزين المتصل بالشبكة (NAS) وSAN

٣. صممت فترات تخزين المعلومات في نظام النسخ الاحتياطي بطريقة يتم من خلالها استرجاع المعلومات بشكل سريع كما لو لم تكن فقدت اصلاً.

- قد تتعارض مدة الاحتفاظ بالنسخ الاحتياطية مع مدة التي تحددها المتطلبات القانونية أو الأعمال التجارية.

إن نظام النسخ الاحتياطي لا يخدم الأغراض التالية:

- أرشفة البيانات للرجوع إليها مستقبلا.
- توفير نسخة من البيانات للرجوع إليها.

٤. السياسة:

أ- سوف يتم عمل نسخة للنظام وفقا للجدول أدناه:

- يتم عمل نسخ احتياطية بانتظام للبيانات المخزنة على أجهزة NAS و SAN على النحو التالي:
- عمل نسخة احتياطية كاملة بشكل اسبوعي (السبت) والبيانات الموجودة خارج الموقع.

يتم عمل نسخة احتياطية لخوادم DMZ على النحو التالي:

- زيادة النسخ الاحتياطية بشكل يومي (الاحد والجمعة). والبيانات الموجودة في الموقع.
- عمل نسخة احتياطية كاملة بشكل اسبوعي (السبت) والبيانات الموجودة خارج الموقع.

يتم عمل نسخ احتياطية لمحرك أقراص بياناته VM بشكل منتظم كما يلي:

- سيتم عمل النسخ الاحتياطية للصور الخاصة بالأجهزة الظاهرية (virtual machine) يومي (الاحد إلى الجمعة). وسيتم تخزين هذه الملفات الاحتياطية في الموقع.
- سيتم عمل نسخ احتياطية كاملة للملفات والمجلدات الأسبوعية يوم السبت وسيتم تخزين هذه الملفات الاحتياطية خارج الموقع.

يتم عمل نسخ احتياطية لشريط الدليل بانتظام على النحو التالي:

- عمل نسخ احتياطية للكتالوج يوميا (الاثنين إلى الجمعة). على القرص الصلب NAS وSANs
- عمل نسخ احتياطية كاملة أسبوعيا (السبت) ونسخها على شريط خارج الموقع.

ب- يتم نقل أشرطة النسخ الاحتياطية وتخزينها كما هو موضح أدناه:

- يتم عنونة الوسائط وتخزينها في منطقة آمنة بحيث لا يمكن الوصول إليها إلا لموظفي تقنية المعلومات أو العاملين المتعاقدين خارج الموقع.
- ثناء نقل أو تغيير الوسائط، يجب أن لا تترك من غير مراقبة.
- يتم تخزين النسخ الاحتياطية اليومية في الموقع داخل خزانة مقاومة للحريق وتقع في مبنى منفصل من مركز البيانات.
- سيتم الاحتفاظ بالنسخ الاحتياطية اليومية لمدة أسبوعين.
- تخزين النسخ الاحتياطية الأسبوعية في مكان امن خارج الموقع ويحتفظ به طرف ثالث.
- سيتم الاحتفاظ بالنسخ الاحتياطية الأسبوعية لمدة ثلاثة أسابيع.
- بعد انقضاء فترة ثلاثة أسابيع، سيتم إرجاع الأشرطة لتقنية المعلومات وسيتم إما إعادة استخدامها أو إتلافها

تعتبر الوسائط غير صالحة ويمكن التخلص منها في الحالات التالية:

- يجب على قسم أنظمة التشغيل بعمادة تقنية المعلومات قبل اتلاف الوسائط التأكد من التالي:
  ١. أن الوسائط لا تحتوي على صور احتياطية نشطة.
  ٢. لا يمكن قراءة محتويات الوسائط الحالية أو السابقة أو استردادها من قبل طرف غير مصرح له.

- يجب على القسم التأكد من أن جميع النسخ الاحتياطية للوسائط قد تم إتلافها قبل التخلص منها

سيتم التحقق من النسخ الاحتياطية بشكل دوري:

- استعراض المعلومات المسجلة من كل عملية نسخ احتياطي بشكل يومي للأغراض التالية:
  ١. للتحقق من الأخطاء وتصحيحها.
  ٢. لمراقبة مدة عملية النسخ الاحتياطي.
  ٣. لتحسين أداء النسخ الاحتياطي إذا كان ذلك ممكنا.

- سيقوم قسم أنظمة التشغيل بعمادة تقنية المعلومات بالبحث عن المشاكل واتخاذ إجراءات تصحيحية لتقليل أي مخاطر مرتبطة بفشل النسخ الاحتياطي.
- عمل اختبار عشوائي مرة واحدة في الأسبوع من أجل التحقق من أن النسخ الاحتياطية كانت ناجحة
- يقوم قسم أنظمة التشغيل بعمادة تقنية المعلومات بالاحتفاظ بسجلات تثبت استعراض تسجيل الدخول و اختبار الاستعادة للتأكد من اتباع هذه السياسة لأغراض التدقيق.

ج- استعادة البيانات:

- في حالة حدوث فشل النظام، فإن النسخ الموجودة خارج الموقع يجب أن تكون متاحة للمستخدمين في غضون ٣ أيام عمل في حال تم استبدال المعدات التي دمرت في ذلك الوقت.
- في حالة عدم حدوث فشل النظام أو خطأ المستخدم، فإن البيانات ستكون متاحة للمستخدمين في غضون يوم عمل واحد.

د- طلب إستعادة :

- في حالة الحذف العرضي أو تلف المعلومات، يجب التقدم بطلب لعمادة تقنية المعلومات بجامعة المجمعة لاستعادة المعلومات المطلوبة.

سياسة أمن مركز البيانات

مقدمة:

إن أمن الأجهزة والبيانات في مراكز البيانات لجامعة المجمعة هو أمر هام جدا لمواصلة الأعمال اليومية.
تهدف هذه الوثيقة لتوعية الموظفين بالسياسات والإجراءات والتي سيتم من خلالها الحصول على إذن بالدخول ومتابعة أعمال الأفراد داخل مراكز البيانات المختلفة.

١. الأدوار والمسؤوليات:

أ- التسمية الشخصية:

- مدير مركز البيانات: مسؤول الاتصالات والبنية التحتية (مدير العمليات)
- موظفي مركز البيانات: فريق مركز تقنية المعلومات المخولين بالدخول إلى مركز البيانات للصيانة الدورية وعمل النسخ الاحتياطية.(نموذج مسؤول الفريق، منسق أمن تقنية المعلومات، المدير الفني لتقنية المعلومات)
- الموظفين المصرح لهم: مسؤولين الخوادم الذين يحتاجون إلى نموذج تفويض للدخول إلى مقر الخوادم في مركز البيانات.
- الأفراد: أي شخص غير مفوض للدخول إلى مركز البيانات مثل الموردين، وكالة التنظيف ... الخ
- المدققين: عميد تقنية المعلومات ووكيل العمادة للشؤون الفنية ومدير مركز البيانات والمدقق الخارجي.

ب- العمل التفاعلي:

يمكن تعريف العمل التفاعلي بأنه ردة الفعل التي يتم القيام بها من أجل النظام أو حاجة المستخدم. ومن أمثلة ذلك التعامل مع مشاكل النظام، وتعطل الأجهزة، و طلبات تغيير الترخيص، والحسابات، وإعدادات التطبيق. إذا كان العمل مرتبط بشيء مهم فيجب تدارك المشكلة إما عن طريق ايجاد حل مؤقت مع استمرار النظام أو حتى تغيير الإعدادات.

ج-العمل الاستباقي:

العمل الاستباقي يقصد به كل الأعمال التي يمكن جدولتها للقيام بها في المستقبل لضمان الحفاظ على استمرارية النظام والعمليات بشكل جيد وآمن.

د- تصريح الدخول:

مراكز البيانات في جامعة المجمعة هي عباره عن غرف خوادم موحده تعمل على مدار ٢٤ ساعة بدون توقف، وتوفر بيئة آمنة للأنظمة التي تحتاج إلى مستوى عالي من الأمن.

- **هناك نوعين من التفويض بناء على مستوى الصلاحية المطلوبة**

١. المستوى الأول:

يسمح للموظفين والأفراد والمراقبين بالدخول إلى مركز البيانات خلال ال ٢٤ ساعة في اليوم ولا تعطى لهم بطاقات دخول.
كما يجب أن يتواجد أحد مسؤولي مركز البيانات من أجل السماح لاحد بالدخول.
إجراءات الحصول على إذن بالدخول للمستوى الأول هي على النحو التالي:

- يجب تعبئة نموذج إذن بالدخول (المستوى الأول) لأي موظف يريد الدخول إلى مركز البيانات.
- يجب كتابة الغرض من الدخول لكل زيارة وأن يتم التوقيع حال الدخول والخروج من مركز البيانات.

٢. المستوى الثاني:

يسمح لمدير مركز البيانات وموظفيه بالدخول إلى مركز البيانات من غير مساعدة وفي أي وقت خلال ٢٤ ساعة في اليوم وليس هناك حاجة لمنحهم بطاقات دخول.
إجراءات الحصول على إذن بالدخول للمستوى الثاني هي على النحو التالي:

- يجب تعبئة نموذج إذن بالدخول (المستوى الثاني) لأي موظف يريد الدخول إلى مركز البيانات.
- يجب كتابة الغرض من الدخول لكل زيارة وأن يتم التوقيع حال الدخول والخروج من مركز البيانات.

٣. إجراءات الزوار:

أي شخص ليس موظف في مركز البيانات وليس مصرح له بالدخول أو حتى بائع معتمد فإنه يعتبر زائرا وعليه اتباع الإجراءات التالية :

- يجب على جميع الزوار الدخول عن طريق المدخل الرئيسي لمركز البيانات في تقنية المعلومات.
- يجب أن يتم مرافقة الزوار في جميع الأوقات من قبل موظفي مركز البيانات أو أي موظف مصرح له أثناء تواجدهم في مركز البيانات. أما إذا كانت هناك حالات استثناء فإن ذلك يتطلب موافقة من مدير مركز البيانات.
- يجب كتابة الغرض من الدخول لكل زيارة وأن يتم التوقيع حال الدخول والخروج من مركز البيانات.
- يجب على الزوار ارتداء شارة زائر في جميع الأوقات.
- ينبغي تحديد مواعيد الزيارات من خلال مدير مركز بيانات على الأقل ٢٤ ساعة قبل موعد الزيارة. أما الزيارات الغير مجدولة من أجل تركيب جهاز أو أداء مهام أخرى فإنه قد يتم إلغاؤها أو تأجيلها.

٤. صلاحيات مفتاح التحكم:

يجب الحفاظ على مفتاح التحكم في مركز البيانات بشكل جيد في جميع الأوقات عن طريق موظفي العمليات. جميع الأفراد الذين لديهم صلاحية الدخول الى مركز البيانات هم مسؤولون بشكل مباشر عن هذا المفتاح.
يجب اتباع الإجراءات التالية:

- يتم السماح لأي شخص بالدخول الى مركز البيانات في حال تم مرافقته وعليه التسجيل للدخول بشكل صحيح إلى مفتاح التحكم وقت دخوله في كل مره. كما يجب على الشخص المرافق التوقيع على النموذج وتعبئة الجزء الخاص به.
- يجب على كل شخص عند مغادرة مركز البيانات (حتى لو كان الخروج لوقت قصير) تسجيل الخروج بشكل صحيح من مفتاح التحكم وقت الخروج في كل مره. كما يجب على الشخص المرافق للزائر تعبئة الجزء الخاص من النموذج الخاص بالخروج.

٣. إجراءات جدولة أعمال الصيانة:

على موظفي مركز البيانات تحديد مواعيد الصيانة والالتزام بها عند تغيير النظام الذي يتطلب تعطل النظام. وسيكون هناك حرص على الحد من وقت تعطل النظام قدر الإمكان وأن لا يتم عمل الصيانة خارج أوقات الجدول المحدد.

٤. متطلبات الأجهزة:

يجب تهيئة مكان في الرفوف لجميع الأجهزة الجديدة التي يتم إدخالها لمركز البيانات مالم تقتضي الضرورة خلاف ذلك وفق ترتيب مسبق. كما

يسمح بقاء الأجهزة الموجودة في مركز البيانات والتي لم يهيأ لها مكان بعد على أن يتم استبدالها بأجهزة أفضل في فترة زمنية معقولة أو أن يتم تغيير أماكن هذه الأجهزة. كما يجب التنسيق مع موظفي مركز البيانات وجدولة الأجهزة التي سيتم إدخالها إلى مركز البيانات. هناك حاجة ماسة إلى توسع تدريجي في البنية التحتية لمركز البيانات في حالة زيادة عدد الأجهزة والذي يعني تأخر في تركيب الأجهزة حتى يتم توفير البنية التحتية المناسبة لمركز البيانات.

٥. تركيب وإزالة الأجهزة:

نظرا لوجود الخوام في مركز البيانات, فإنه يعتبر من أقل الأماكن التي يمكن الوصول إليها. لذلك ينبغي على مسؤولين أنظمة الأجهزة والتي تقع في مركز البيانات وضع الخوادم بطريقة لا يمكن الوصول إليها إلا وقت الضرورة لعمل بعض التعديلات أو تغيير الأجهزة. كما ينصح بشدة أن يتم إعداد الخوام بأدوات ذات أمنية عالية تمكن من صيانتها عن بعد.

يجب على أي موظف يرغب في تركيب أجهزة في مركز البيانات أن يقدم استمارة خاصة بالتركيب.

يجب على أي موظف يرغب في إزالة أجهزة من مركز البيانات أن يقدم استمارة خاصة بالإزالة.

٦. الأنظمة المتبعة داخل مركز البيانات:

- يمنع الأكل أو الشرب داخل مركز البيانات.
- يجب إزالة الأغلفة البلاستيكية من الحاسب أو الجهاز قبل إدخاله لمركز البيانات.
- يجب إزالة جميع أدوات التغليف من منطقة المشرف بعد الانتهاء من التركيب.
- يمنع دخول أدوات النظافة إلى مركز البيانات من غير إذن مسبق ويشمل هذا الماء.
- يمكن استخدام مكنسة كهربائية داخل مركز البيانات.
- يمنع تمزيق أو إتلاف اي مادة (أنابيب, بلاط) داخل مركز البيانات من غير ترتيب مسبق.
- يمنع تخزين علب وشرائط الفيديو والأقراص المدمجة وغيرها من المواد داخل مركز البيانات.
- يسمح لموظفي مركز البيانات فقط بإزالة بلاط الأرضية.
- يجب ارتداء البطاقة التعريفية وأن تكون ظاهره طول الوقت.
- يرجى التواصل مع موظفي مركز البيانات في حال وجود اي مشاكل.
- في حال الطوارئ يرجى إبلاغ موظفي مركز البيانات بشكل فوري.

سياسة استخدام وإدارة البريد الإلكتروني

مقدمة وبيان الهدف من السياسة:

البريد الإلكتروني (البريد الإلكتروني) هو عبارة عن نقل المعلومات إلكترونيا عادة ما تكون في شكل رسائل إلكترونية، ومذكرات، وملفات مرفقة من طرف المرسل إلى واحد أو أكثر من الأطراف المستقبلة عن طريق نظام الاتصالات السلكية واللاسلكية. يعتبر البريد الإلكتروني هو أداة أساسية تستخدم من قبل الشركات لتحسين الطريقة التي تمارس فيها الأنشطة التجارية من خلال توفير وسيلة سريعة وفعالة من حيث التكلفة لإنشاء ونقل والرد على الرسائل والمستندات إلكترونيا. إن التميز في إنشاء نظام بريد إلكتروني وإدارته بشكل جيد يساهم في سرعة التواصل في العمل ويقلل من الأعمال الورقية، بالإضافة إلى أتمته المهام المكتبية الروتينية وبالتالي زيادة الإنتاجية وخفض التكاليف. لكن هذه المزايا قد تكون معرضة للخطر إذا لم يتم استخدام أنظمة البريد الإلكتروني وإدارتها بشكل فعال.

إن الغرض من هذه السياسة هو تعزيز استخدام البريد الإلكتروني كأداة فعالة للتواصل وجمع البيانات. أيضا من أهداف هذه السياسة هو التأكد من أن الشركات لديها المعلومات الضرورية لاستخدام البريد الإلكتروني بشكل جيد لزيادة كفاءة أعمالها. هناك هدف آخر هو تجنب الفيروسات التي قد تصيب نظام البريد الإلكتروني للمنشأة بالإضافة إلى تجنب الإضرار التي تؤثر على الأداء الفعال لنظام البريد الإلكتروني للمنشأة. إن الامتثال لسياسية استخدام وإدارة البريد الإلكتروني بشكل جيد، سيقلل من المخاطر والتكاليف بشكل كبير مع زيادة كفاءة التواصل.

ا. النطاق:

تنطبق هذه السياسة على جميع موظفي الجامعة، بالإضافة إلى موظفي العقود الذين يستخدمون البريد الإلكتروني للجامعة.

السياسة العامة:

إن من سياسة الجامعة استخدام البريد الإلكتروني للاتصالات الداخلية والخارجية التي تخدم وظائف وأغراض الجامعة المشروعة. وأي استخدام شخصي يجب أن يكون ذا طابع عرضي وأن لا يتداخل مع عمل الجامعة. أما فيما يخص الاستعمال الشخصي، فيجب أن لا يكون لأغراض غير مشروعة مثل التحايل واستخدام البريد في أنشطة لا ترتبط بالجامعة من أجل تحقيق مكاسب وأرباح شخصية. إلخ. تخضع المعلومات المتبادلة عن طريق نظام البريد الإلكتروني للجامعة لنفس القوانين والأنظمة والسياسات وغيرها من المتطلبات التي تطبق على جميع أنواع التواصل الأخرى وأن لا يتم استخدامها لأغراض سياسية.

إن الجامعة مسؤولة عن إنفاذ هذه السياسة ووضع الإجراءات والممارسات الإدارية التي تتفق مع هذه السياسة من أجل تحقيق أهداف منها:

تطبق المعايير على جميع الوحدات الإدارية في الجامعة وتشمل (الأفراد –العمادات-الوكالات-الكليات-الوحدات)

الممارسات التي ينبغي مراعاتها لاستخدام البريد الإلكتروني من أجل الحفاظ على الخصوصية والاستخدام الامثل للخدمة كالتالي

١. التحلي بحُسن التقدير فيما يختص بمعقولية الاستخدام الشخصي للبريد الالكتروني.
٢. عدم ممارسة في أية أنشطة غير قانونية كالاختراق، والدخول غير المصرح به، أو التسبب بإدخال ما يضر بالحواسيب أو إدخال الفيروسات، أو القيام بتصرفات من شأنها التسبب في تعطيل استخدام البريد الالكتروني والتي قد يعاقب عليها النظام.
٣. يرجى الحفاظ على عدم تضمين البريد الالكتروني بالمحتوى الغير مرغوب فيه والضار والتصيد ومن الأمثلة على المحتوى أو السلوك غير المرغوب فيه:

- استخدام معلومات أو مواد محمية بأنظمة الحماية الفكرية.
- استخدام التصيد للمحاولة في التخفي في هوية كاذبة للحصول على بيانات المستخدمين الآخرين مثل كلمات المرور والتفاصيل المالية وأرقام الهوية الصادرة عن جهات حكومية.
- استخدام البريد الإلكتروني لإنشاء أو توزيع أي هجوم، أو الرسائل التخريبية، بما في ذلك رسائل تتضمن تعليقات مسيئة عن العرق أو الجنس أو السن أو التوجه الجنسي، المواد الإباحية، والديني أو المعتقدات السياسية، أو الأصل القومي أو الإعاقة.
- إرسال رسائل إلكترونية غير مرحب بها أو تطوعية.
- إرسال رسائل أو صور مغرضة أو ذات محتوى تهديدي أو كل ما يشابه ذلك.
- إرسال رسائل إلكترونية تنتهك قانون CAN-SPAM أو أية قوانين أخرى لمكافحة المحتوى غير المرغوب فيه
- بيع أو تبادل أو نشر عناوين البريد الإلكتروني لأي شخص بدون موافقته.
- استخدام office٣٦٥ في تنفيذ مخططات احتيالية أو خداع المستخدمين بأية وسيلة أخرى
- إرسال رسائل غير مصرح بها عبر خوادم مفتوحة أو خوادم جهات خارجية.
- توزيع برامج ضارة مثل الفيروسات والفيروسات المتنقلة ونقاط الخلل وأحصنة طروادة والملفات التالفة وأية عناصر أخرى من هذا القبيل ذات طبيعة تخريبية أو خداعية.

في حال حصولك على أي رسائل بريد الإلكتروني مشابه لهذا المحتوى يجب تبليغ هذا الأمر إلى عمادة تقنية المعلومات على الفور عبر بريد (infosec@mu.edu.sa) ليتم اتخاذ الاجراء اللازم.

٤. يجب عدم نقل المعلومات الشخصية أو إطلاع أية جهة أخرى عليها.
٥. عدم السماح للمستخدمين بتبادل أسماء المستخدمين وكلمات المرور فيما بينهم.
٦. عدم استخدام البريد الالكتروني الجامعي في الأنشطة التجارية، ما لم يصدر بشأنه موافقة الجهات المختصة في الجامعة.
٧. الحفاظ على خصوصية وسرية اسم المستخدم وكلمة مرور البريد الالكتروني، وتخصيصها وإستخدامها بصورة آمنة .
٨. الالتزام بالقواعد التي تنصح بها عمادة تقنية المعلومات عند اختيار كلمة المرور ، للاطلاع على القواعد اضغط هنا.
٩. في حال وجود أي شك بانكشاف كلمة المرور يجب تغييرها فوراً و إبلاغ عمادة تقنية المعلومات عبر الخدمات الالكترونية (es.mu.edu.sa) يحق للمنسوب الاشتراك في المجموعات البريدية التي تحقق أهداف العمل وليس أهداف شخصية.
١٠. يتم تعطيل بريد الموظف في حاله عدم استخدامه للبريد لمدة ٩٠ يوماً.
١١. يتم حذف الموظف من كل المجموعات فور طي قيده من الجامعة.
١٢. يسمح لمستخدمي البريد الالكتروني الجامعي الاستفادة من المميزات المتاحة في office ٣٦٥ بغرض الإفادة منها لأهداف تخدم العمل الرسمي من النواحي الإدارية والأكاديمية والبحثية وخدمة المجتمع.

١٣. يتم تقيد الاستخدام حسب قوانين المملكة المعمول بها مع عدم وضع صور مخالفة أو استخدام البريد أو تغيير البيانات الخاصة بالمستخدم من معلومات

الشخصية أو اسم المعرف أو صورة المعرف وما يتبعها من مسمى صور أو ما شابه ذلك إلى اي دلالات لا تتوافق مع سياسات وقوانين المملكة أو سياسات الجامعة المنشورة

معايير استخدام خدمة مركز الرسائل :

- المناسبات التي برعاية معالي مدير الجامعة او سعادة وكيل الجامعة
- المناسبات العامة سواء لأعضاء هيئة التدريس والموظفين، او بتوجيه من مدير الجامعة أو أصحاب السعادة وكلاء الجامعة أو من عمداء العمادات المساندة .
- المناسبات المختصة بالطلاب او الطالبات الجامعة ، بتوجيه من معالي مدير الجامعة او أصحاب السعادة وكلاء الجامعة .
- التهنئة بالأعياد والمناسبات الوطنية الرسمية.
- حفل التخرج.
- التنبيهات و التوعية الأمنية.
- رسائل تحديث الأنظمة الإلكترونية والإعلانات عن توقف الخدمات الإلكترونية للصيانة.
- الاستبانات المجازة من معالي مدير الجامعة أو سعادة وكيل الجامعة للدراسات العليا والبحث العلمي.

هناك بعض المنشآت لديها متطلبات خاصة لأمن المعلومات (على سبيل المثال، سجلات العميل السري) وقد تحتاج إلى مضاعفة الحماية لضمان أمن هذه المعلومات.

الوصول إلى خدمات البريد الإلكتروني:

إن خدمات البريد الإلكتروني متاحة لجميع الموظفين والمتعاقدين في جميع الإدارات. من اجل الحصول على هذه الخدمة, يرجى التواصل مع قسم تقنية المعلومات الخاصة بخدمة المستخدمين.

الخصوصية والوصول:

- لا تعتبر رسائل البريد الإلكتروني شخصية وذات خصوصية وعليه فإنه يحق للمسؤولين والمشرفين والموظفين التقنيين تعقب رسائل البريد الإلكتروني لأي موظف لأغراض العمل بما يتوافق مع سياسة الحماية للجامعة, ومن هذه الأغراض:
  ١. الأعمال المشروعة التي تخص الجامعة (على سبيل المثال، الحاجة الحصول على معلومات في حال غياب موظف)
  ٢. تشخيص وحل المشاكل التقنية الموجودة في أجهزة النظام، والبرمجيات، والاتصالات.
  ٣. التحقيق في احتمال اساءة استخدام البريد الإلكتروني.
- يمنع منعا باتا لأي موظف استخدام البريد الإلكتروني لأي مستخدم دون إذن مسبق ويستثنى من ذلك الذين تم ذكرهم آنفا.
- تخضع جميع رسائل البريد الإلكتروني بما في ذلك التي تحتوى على اتصالات شخصية لإجراءات فحص وفق القانون.
- تعتبر جميع رسائل البريد الإلكتروني المرسلة أو المستلمة والتي لا تتم حمايتها من قبل القانون وثائق عامة ويمكن الكشف عنها للعامة بموجب قانون حرية الوصول.

الحماية:

إن حماية البريد الإلكتروني هي مسؤولية مشتركة بين الموظفين التقنيين ومستخدمي البريد الإلكتروني. يجب على المستخدمين اتخاذ جميع الاحتياطات بما في ذلك حماية وتغيير كلمات المرور، لضمان منع استخدام حساب البريد الإلكتروني الخاص بهم من قبل أفراد غير مرخص لهم.

إدارة وحفظ اتصالات البريد الإلكتروني:

- **أ- رسائل البريد الإلكتروني والمرفقات:**

بما أن البريد الإلكتروني هو نظام تواصل، لذلك يجب عدم الاحتفاظ بالرسائل لفترات طويلة.
يجب على المستخدمين:

- إزالة أو أرشفة جميع رسائل البريد الإلكتروني حسب تاريخ الإرسال أو الاستلام.
- حذف السجلات العابرة أو التي ليست ذا قيمة بالنسبة للعمل.

- **ب- السجلات المرسلة عن طريق البريد الإلكتروني:**

إن البريد الإلكتروني الذي يتم إنشاءه في سياق عمل المنشأة ويتم الاحتفاظ به كمرجع رسمي للسياسات والإجراءات والقرارات أو المعاملات يعتبر بمثابة سجلات وتخضع لمتطلبات إدارة السجلات الموثقة في أرشيف الجامعة. لا بد من تحديد وإدارة وحماية والاحتفاظ بالسجلات التي ترسل باستخدام البريد الإلكتروني طالما انها ضرورية لتلبية متطلبات قانونية و حسابية وبحثية أو غيرها من المتطلبات.
إذا كانت هناك استفسارات معينة تتعلق بمتطلبات الاحتفاظ بالسجلات , يرجى الاتصال بوحدة التشغيل في قسم تقنية المعلومات, شعبة الأرشيف للحصول على المساعدة.

فيما يلي

- **أمثلة لبعض الرسائل المرسلة عن طريق البريد الإلكتروني التي تعتبر بمثابة سجلات :**
  - السياسات والتوجيهات
  - المراسلات أو المذكرات المتعلقة بالأعمال الرسمية
  - مواعيد العمل والمهام
  - جداول الأعمال ومحاضر الاجتماعات
  - مسودات الوثائق التي تم تعميمها للتعليق أو الموافقة
  - أي وثيقة تبدأ أو تفوض أو تنهي صفقة تجارية
  - التقارير أو التوصيات النهائية

- **فيما يلي أمثلة لبعض الرسائل المرسلة عن طريق البريد الإلكتروني التي لا تعتبر بمثابة سجلات :**
  - رسائل شخصية واعلانات
  - نسخ أو مقتطفات من الوثائق الموزعة كمرجع أو للترفيه.
  - ملاحظات رسائل الهاتف

الأدوار والمسؤوليات:

- ستقوم الإدارة التنفيذية بالتأكد من أن السياسة قد تم تنفيذها من قبل وحدة إدارة البرنامج ووحدة المشرفين.
- سوف يقوم مدراء ومشرفي الوحدة بتطوير و نشر ممارسات حفظ السجلات في نطاق مسؤولياتهم وسوف يقوموا بتدريب الموظفين على الاستخدام المناسب، بما في ذلك:

- الاستخدام الشخصي للبريد الإلكتروني الذي لا يؤدي إلى مشكلات في الأداء، وأن يكون مسؤولا عن ضمان حماية الأجهزة وكلمات السر.
- مسؤولي الشبكة و موظفي الرقابة الداخلية مسؤولون عن أمن البريد الإلكتروني والنسخ الاحتياطي.
- يجب على المستخدمين الالتزام بهذه السياسة.

الاستخدام الأمثل:

على جميع مستخدمي البريد الإلكتروني فهم هذه السياسة والالتزام بها وهي كالتالي:

- استيعاب أن الاستخدام الشخصي يجب أن يكون عرضيا فقط.
- الالتزام بسياسة وإجراءات ومعايير المنشأة ووحداتها.
- الالتزام بحماية أسرار الجامعة.
- إدراك أن إرسال أي بريد إلكتروني ذا طابع سياسي, هو ضد القانون ويخضع لعقوبات جنائية
- قم على الفور بحذف أي سلسلة من الرسائل الواردة من خلال نظام البريد الإلكتروني للجامعة.
- تأكد من الدخول للجامعة قبل إرسال أو إتلاف أي بريد إلكتروني.
- حماية كلمات المرور الخاصة بهم
- الحصول على موافقة من المشرف وإذن من الرئيس التنفيذي، أو مدير الجامعة، أو من ينوب عنه، قبل إرسال رسائل البريد الإلكتروني الخاصة بالجامعة على نطاق واسع.
- الرد على البريد الإلكتروني في الوقت المناسب
- عدم إرسال أو استخدام البريد الإلكتروني لنقل محتوى محظور ذا طابع جنسي
- حذف الرسائل التي قد تحتوي على مواد مسيئة وتقديم بلاغ إلى إدارة
- إزالة الرسائل الشخصية، والسجلات العابرة في الوقت المناسب
- عدم استخدام البريد الإلكتروني لنشاط تجاري ليس متعلقا بالجامعة أو تحقيق مكاسب شخصية
- التنبه إلى لوائح حقوق الطبع والنشر
- عدم استخدام البريد الإلكتروني لأي غرض غير قانوني.
- عدم استخدام البريد الإلكتروني لنشر التمييز على أساس العرق، أو الدين، أو الأصل أو الإعاقة أو التوجه الجنسي، والعمر، والحالة الزوجية، ونوع الجنس، أو الانتماء السياسي.
- عدم إنشاء بريد إلكتروني ذا طابع تشهيري.
-
- اتباع المعايير المقبولة للآداب
- يجب عدم استخدام نظام البريد الإلكتروني للترويج لأغراض ليس لها علاقة بالمنشأة.
- يجب عدم إرسال أو استقبال رسائل البريد الإلكتروني التي تحتوي على فيروسات عمدا.

انتهاكات هذه السياسة:

أي انتهاك لهذه السياسة يمكن أن يؤدي إلى اتخاذ إجراءات تأديبية، قد تصل إلى إنهاء الخدمة.

استعراض وتحديث السياسة:

سيقوم مكتب المدير التنفيذي للمعلومات بمراجعة دورية وتحديث لهذه السياسة بناء على التغييرات والتقنيات التي تطرأ على الجامعة وإذا كانت هناك أسئلة أو استفسارات متعلقة بهذه السياسة فيرجى التقدم بها إلى مكتب المدير التنفيذي.

سياسة جدار الحماية

تقوم عمادة تقنية المعلومات وخدمات الشبكة في جامعة المجمعة بتشغيل جدار الحماية من أجل تعزيز الحماية بين الإنترنت وشبكة الجامعة وذلك من أجل إنشاء شبكة موثوقة لأجهزة الكمبيوتر وموارد الشبكة في الجامعة.
كما يعتبر جدار حماية عنصر أساسي في البنية الامنية لشبكة الجامعة.
تقوم هذه السياسات والإجراءات بتنظيم عمل جدار الحماية على تنقية حزم البيانات بهدف تقليل المخاطر والخسائر المرتبطة بالأخطار الأمنية المحدقة بشبكة الجامعة ونظم المعلومات.
كما تسعى هذه هذه السياسات لتحقيق التوازن بين المخاطر التي يتم التعرض لها من جهة والحاجة للوصول للشبكة من جهة أخرى.

١- الهدف:

يعتبر جدار الحماية عنصر واحد من العناصر الأمنية في البنية التحتية. تهدف للتقليل من المخاطر الخارجية التي تهدد أنظمة الجامعة أو استخدام أنظمة الجامعة كنقطة عبور للدخول غير المشروع إلى أنظمة أخرى. ومع ذلك لا يمكن لجدار الحماية منع الأنشطة الضارة أو غير القانونية الحاصلة خلف الجدار.
تم تصميم هذه السياسات والإجراءات لحماية أجهزة حواسيب الجامعة سواءً الخوادم أو الخاصة بالمستخدمين وذلك ضد هجمات القرصنة والفيروسات عن طريق تقييد الوصول لهذه الأجهزة من الأشخاص الموجودين خارج الشبكة.

٢- النطاق:

تنطبق هذه السياسة على جميع مستخدمي شبكة تقنية المعلومات في جامعة المجمعة بما فيهم: الموظفين والمتعاقدين والموردين، والشركاء، والنظم والتطبيقات والشبكات.

٣- التعريفات:

- **جدار الحماية**

جدار الحماية هو عبارة عن جهاز مادي وبرمجي يتحكم في الوصول بين شبكتين. وهناك عدة آليات لتنفيذ هذا التحكم بالدخول ولكن النقطة الأساسية هي أن جدار حماية ينفذ سياسة أمن الشبكات.

- **نظام جدار الحماية:**

يتضمن نظام جدار الحماية كل من المنتج وضوابط إضافية، والتي قد تكون أو لا تكون متاحة كجزء من المنتج الأساسي لجدار الحماية. تشتمل هذه الإضافات عادة على حلول لمنع أو فحص المحتوى؛ على سبيل المثال منافذ البريد الإلكتروني المضادة للفيروسات، وأنظمة كشف التسلل، ومراجعة الحسابات, كود الجوال (ActiveX و Java).

٤. المسؤوليات:

يعد قسم أمن الشبكات في جامعة المجمعة المسؤول عن تنفيذ وصيانة جدار الحماية للشبكة .وبالتالي فهي مسؤولة عن الأنشطة المتصلة بهذه الإجراءات . كما أن مسؤولية حماية نظم المعلومات بشكل يومي هو مسؤولية كل موظف.
أما فيما يتعلق بإدارة طلبات الوصول والتدقيق الدوري, إضافة للتوجيهات والإرشادات فإنها تقع على عاتق إدارة أمن المعلومات في الجامعة.

٥. الإجراءات التشغيلية:

يسمح فقط لمدراء جدار الحماية بتسجيل الدخول لجدار الحماية.

- يجب أن تكون هناك رقابة مشددة للوصول إلى أجهزة جدار الحماية ويسمح لمسؤولي نظام جدار الحماية فقط بإنشاء حسابات على جهاز جدار الحماية.
- يجب على مسؤولي نظام جدار الحماية إنشاء حسابات شخصية، ولا يسمح بتسجيل الدخول من حساب واحد.
- لا يسمح بتوكيل شخص آخر للدخول بل يجب الدخول شخصيا.
- فقط الموظفين بالصلاحيات اللازمة من يمكنهم ضبط الإعدادات البرمجية والمادية و التحكم بالوصول.
- يجب أن تكون جميع التغييرات على جدار الحماية عن طريق تعبئة نموذج طلب فتح منفذ في جدار الحماية. كما يمكن إجراء تعديلات اضطرارية عن طريق اتصال هاتفي ويجب ارسال ايميل لاحقا بالإجراءات التي تمت على أن يتم تعديل ذلك في نظام ادارة المنافذ.
- يسمح فقط للموظفين التقنيين المصرح لهم في إدارات الجامعة بطلب فتح أو تغيير منافذ على جدار الحماية للجامعة.
- يقوم موظفين مصرح لهم في إدارة أمن المعلومات بدراسة و تقييم مخاطر فتح المنافذ المقدمة في هذه الطلبات. في حال قبول الطلب، يتم تنفيذه من قبل مدير جدار الحماية. أما إذا كانت المخاطر المرتبطة بالطلب غير محتملة، فسيتم تقديم شرح بالمخاطر المصاحبة للعملية لمقدم الطلب الأصلي وسيتم إقتراح حلول بديلة.
- في حال تبين خلال التنفيذ أن الطلب لا يلبي حاجة الجهة أو القسم صاحب الطلب وظيفياً, فإن المصرح لهم من إدارة أمن المعلومات في الجامعة لديه الصلاحية لرفض الطلب.
- يمكن لإدارة أمن المعلومات السماح خلال فترة قصيرة أن يتم فتح الوصول عبر جدار الحماية, على أن يتم على المدى البعيد بالعمل مع مقدم الطلب لتحديد المنافذ التي تلزم القسم لتلبية احتياجاتها.
- هناك بعض المهام الحساسة والتي تتطلب من شركات أو جهات أخرى من الخارج للحصول على دخول آمن ومحدود إلى موارد شبكة الجامعة. يجب أن تتم الموافقة مسبقاً على هذا الدخول من قبل إدارة أمن المعلومات ومن ثم إتباع إجراء تفعيل الدخول الآمن VPN لحساب يخصص للجهة طيلة فترة تنفيذ هذه المهام.
- إذا رأى مقدم الطلب الأصلي أن الحل غير مرضي، فيمكن استئناف الطلب مع عميد تقنية المعلومات.
- يتم التعامل مع الطلب العادي خلال ٣ ايام عمل من استلام طلب التغيير في جدار الحماية. وتشمل الخدمات عادة:
  - خدمة الملفات FTP
  - خدمة الإدارة الطرفية المشفر (SSH)
  - خدمة إتصال سطح مكتب بعيد (RDP)
  - خدمة البريد الإلكتروني SMTP
  - خدمة الويب HTTP/HTTPS
  - خدمة الاتصال بقواعد البيانات
- وسيتم التعامل مع أي طلب طارئ بأسرع وقت ممكن. يعتبر الطلب طارئاً حينما يرتبط الطلب بمشكلة أمنية حرجة.

٦. ضبط الإعدادات:

يتم ضبط إعدادات جدار الحماية بأن يمنع الوصول لجميع المنافذ والخدمات عدا ما يسمح به.

- إذا لم تكن هناك قواعد محددة لعنوان شبكي معين في الجامعة، فيجب منع مرور البيانات من و إلى هذا العنوان.

- يجب أن يتم حظر الوصول إلى شبكة الجامعة أثناء إجراءات تشغيل جدار الحماية.
- يتم ضبط إعدادات نظام تشغيل جدار الحماية لأقصى درجات الأمان.
- يتم ضبط النظام المشغل لجهاز جدار الحماية لأقصى قدر من الأمان، بما في ذلك تعطيل أي خدمات غير مستخدمة.
- يجب أن يتواجد منتج جدار الحماية على أجهزة مخصصة ومكرسة لها.
- o لا ينبغي السماح بتشغيل أي تطبيقات من شأنها الإضرار وبالتالي التأثير سلباً على عمل جدار الحماية.
-
- يجب أن يتم توثيق عمليات الإنشاء وضبط الإعدادات لجدار الحماية بشكل كامل.
- يوفر هذا التوثيق قاعدة أساسية لنظام جدار الحماية والذي يتبع له جميع التغييرات الفرعية. مما يساعد على تتبع التغييرات وبالتالي ضمان استقرار الوضع.
-
- الحماية يجب أن لا تتأثر بسبب فشل أي مكون في جدار الحماية.
- في حال فشل أي مكون من جدار الحماية، فإن الرد المفترض سيكون منع أي وصول سواءً الصادرة أو الواردة من و إلى شبكة الجامعة-.
- إن عناصر جدار الحماية هي أي عتاد أو برمجية مرتبطة بنظام جدار الحماية. يعتبر الفشل مادياً عند حدوث عطل وظيفي أو عند إيقاف تشغيله. يعتبر الفشل برمجياً لأسباب عديدة مثل سوء صيانة قاعدة بيانات القواعد في جدار الحماية, أو تثبيت أو تحديث غير صحيح للبرامج.
- يجب تعطيل إعادة توجيه العناوين الشبكية IP على مستوى أنظمة التشغيل لحين إعادة برنامج جدار الحماية للعمل و تفعيل سياسة تنقيح العناوين IP.

٨. التدقيق والإمتثال :

يتم تنفيذ فحص دوري لجدار الحماية.

أ. يجب أن يتم فحص جدار الحماية بشكل منتظم بحثاً عن:

- أخطاء في الإعدادات و التي قد تمثل نقطة ضعف يمكن استغلالها من قبل أشخاص بنواياً سيئة.
- تناسق قواعد جدار الحماية، مثل التأكد من تطابق حالة القواعد مع ماهو موثق.
- سلامة تطبيق النظام الأساسي, مثل التحقق من سلامة جهاز جدار الحماية والتطبيقات باستخدام أداة تحقق بالسلامة.

ب. يجب أن يحتوي نظام جدار الحماية على نظام إنذار وإجراءات داعمة

ج. حينما يحصل حدث معين معرف مسبقاً، يجب أن يُرسل إنذار يصل لموظفي أمن الشبكات. كما لابد من وجود وثيقة إجراءات تسمح بالاستجابة الفعالة لمثل هذه الإنذارات الأمنية الخاصة بجدار الحماية.

د. في بعض الحالات يكون من الأفضل لنظام جدار الحماية الرد بطريقة آلية للأحداث الأمنية.

هـ. في حال أن جدار الحماية هو المستهدف لمحاولات إختراق, وكانت لدية القدرة على التصدي , ينبغي إيقاف وصول الخدمات ذات الصلة بهذه المحاولات بدلا من السماح بالوصول غير المنضبط إلى شبكة الجامعة.

- يجب أن يكون هناك نظام تدقيق أو تسجيل دخول لتحليل أنشطة جدار الحماية إما أثناء أو بعد الأحداث الأمنية.
- يجب إجراء عملية تدقيق كتجربة لتحديد ما إذا كانت هناك محاولات للالتفاف على جدار الحماية.
- يجب أن تكون عملية التدقيق التجريبية محمية ضد أي فقدان أو تعديل غير مصرح به.
- يجب أن يكون نظام الحماية قادرا على تسجيل الأحداث المرتبطة بسيل البيانات حينما يتم الكشف عن أي نشاط مشبوه.

٨. المراجعة الدورية للإجراءات الأمنية لجدار الحماية:

يتم مراجعة الإجراءات الأمنية لجدار الحماية على الأقل سنويا. في حال كون هناك تغييرات كبيرة في متطلبات الشبكة فإن هذا قد يستدعي تغييرات على إجراءات جدار الحماية الأمنية.

٩. إرشادات توجيه البيانات:

يسمح جدار الحماية بمرور البيانات الصادرة والواردة في الحالات التالية:

- حركة البيانات الصادرة- السماح بمرور جميع إتصالات الانترنت إلى الخدمات والأجهزة خارج شبكة جامعة المجمعة بإستثناء الثغرات الأمنية المعروفة. هذا يسمح لأي شخص متصل بشبكة جامعة المجمعة الاستفادة من جميع الخدمات على شبكة الإنترنت باستثناء نقاط الضعف المعروفة.
- حركة البيانات الواردة -
- يسمح فقط لخدمات معينة تدعم مهام أعمال جامعة المجمعة من الوصول لشبكة الجامعة عبر الانترنت.

يوضح الجدول أدناه الخدمات الأكثر استخداما في التواصل عبر الإنترنت في شبكة جامعة المجمعة

من شبكة جامعة المجمعة إلى الإنترنت: الخدمات التي لا يسمح بها	من الإنترنت إلى شبكة جامعة المجمعة: الخدمات التي يسمح بها
• خدمات الويب المشفر (HTTPS) لبرمجيات الجامعة الرسمية. • خدمة البريد المشفر (SMTPS) للبريد الرسمي للجامعة. • خدمة الشبكة الوهمية الخاصة المشفر (VPN) الرسمية للجامعة.	• خدمات مايكروسوفت السحابية Office٣٦٥ المتضمنة: -البريد الإلكتروني. -حزمة البرامج المكتبية Office٣٦٥ -تخزين الملفات • خدمات الويب. • خدمة التعليم الإلكتروني (Blackboard) • مصادر تحديث أنظمة التشغيل. • خدمة الاتصال الطرفي (SSH) • خدمات الإتصال بنظام عن بعد (RDP, VNC) • البحث في الفهارس المكتبية

سياسة المستخدم الزائر

١. الهدف:
هناك العديد ممن هم في حاجة لاستخدام شبكة جامعة المجمعة مثل للطلاب والشركات والبائعين والمدققين. ومن أجل تقديم خدمات لهؤلاء المستخدمين , فإن عمادة تقنية المعلومات تمنح للضيوف والزوار الحق في استخدام موارد تقنية طبقا لسياسات وإجراءات عمادة تقنية المعلومات في جامعة المجمعة. وهؤلاء الأشخاص المصرح لهم يعتبروا بمثابة مستخدمين زائرين ويبقوا كذلك إلى انتهاء مدة التصريح المعطى لهم.

٢. النطاق:
تنطبق هذه السياسة على أي مستخدم زائر ولا تشمل موظفي الجامعة.

٣. السياسة:
يعتبر المستخدم الزائر عبارة عن مستخدم مصرح له عند استخدام موارد عمادة تقنية المعلومات وفقا لسياسات جامعة المجمعة ومادام أن الاستخدام في نطاق الصلاحيات المعطاة للمستخدم الزائر. يمكن أيضا إعطاء الصلاحية للمستخدم الزائر باستخدام أجهزة الكمبيوتر في الجامعة بالإضافة إلى بعض البرامج التي يتم اختيارها. كما يسمح أيضا للزوار بالدخول لمناطق معينة من تقنية المعلومات والشبكات بجامعة المجمعة.

٤. تطبيق القانون:
في حالة انتهاك هذه السياسة من قبل أي مستخدم مرخص له, فإنه يعتبر غير مرخص له ويخضع لإجراءات تأديبية وفقا لبند تطبيق القانون الموجود في سياسة الاستخدام الغير مرخص به.

سياسة الأمن للتحكم بمنطقة العمل

الهدف:

تهدف هذه السياسة إلى وضع معايير لتكوين قاعدة أو مرجع يستند إليه في إدارة منطقة العمل التابعة أو التي يتم تشغيلها من قبل الجامعة. وفي حال تم تنفيذ هذه السياسة بشكل جيد فإن ذلك سيؤدي إلى التقليل من الدخول الغير مصرح به إلى شبكة تقنية المعلومات وغيرها من المعلومات السرية والتقنية.

٢. النطاق:

تنطبق هذه السياسة على جميع أجهزة عمادة تقنية المعلومات الموجودة في منطقة العمل والتي تملكها أو تشغلها الجامعة. كما تنطبق هذه السياسة أيضا على محطات العمل المسجلة تحت أي شبكة داخلية تملكها المنشأة.

٣. السياسة:

الملكية والمسؤوليات

يجب أن تكون جميع مناطق العمل في عمادة تقنية المعلومات هي مسؤولية مجموعة تشغيلية وأن تكون مسؤولة أيضا عن إدارة أجهزة الكمبيوتر. كما يجب إنشاء ومتابعة المعايير المعتمدة لمنطقة العمل من قبل كل قسم بناء على احتياجات العمل. كما يجب على المجموعات التشغيلية مراقبة مطابقة المعايير وطلب موافقة خاصة لأية استثناءات تم ملاحظتها. كما يجب على كل مجموعة تشغيلية إنشاء عملية لتغيير معايير التكوين، والتي تشمل مراجعة وموافقة من قبل موظفي أمن المعلومات.

١. يجب تسجيل مناطق العمل ضمن نظام الجرد للجامعة. ويتعين توفر المعلومات التالية كحد أدنى لتحديد نقطة الاتصال:

- أسماء محطة العمل، والمكان، وأسماء النسخ الاحتياطية
- الأجهزة وأرقام إصدارات نظام التشغيل (OS)
- الوظائف الرئيسية والتطبيقات، إن وجدت

٢. يجب أن تبقى المعلومات الموجودة في نظام الجرد لتقنية المعلومات في الجامعة.

٣. يجب أن تكون التغييرات لإعدادات مناطق العمل متوافقة مع سياسة التغيير للإدارة.

معايير الإعدادات العامة :

- يجب أن تتطابق إعدادات نظام التشغيل مع المعايير المعتمدة من قبل أمن المعلومات.
- يجب تعطيل الخدمات والتطبيقات الغير مستخدمة . في حال الاستثناءات يجب إشعار وأخذ موافقة من قبل موظفي أمن المعلومات.
- يجب حماية الوصول إلى الخدمات من خلال استخدام طرق التحكم بالدخول (على سبيل المثال wrappers TCP)، إذا كان ذلك ممكنا.
- يجب تثبيت ال (Patches) الأحدث والأكثر أمنية على النظام في أقرب وقت ممكن ويستثنى من ذلك تعارض التطبيق الفوري مع متطلبات العمل.
- إن علاقات الثقة بين الأنظمة تشكل خطرا أمنيا، وينبغي تجنب استخدامها، خاصة إذا كانت هناك طريقة أخرى كافيه للاتصال.
- يجب أن يتم استخدام مبدأ الحماية لتقليل صلاحية الدخول لأكبر قدر ممكن عند القيام بوظيفة معينة.
- إذا وجدت منهجية لاتصال القناة الآمنة (أي ممكن من الناحية التقنية)، فإنه يجب تقديم الدخول بامتيازات على القنوات الآمنة (مثل اتصال الشبكة المشفر باستخدام IPSec أوSecure Shell).

المراقبة:

يجب إبلاغ موظفي أمن المعلومات عن الأحداث المتعلقة بالحماية و القيام بمراجعة سجلات الحوادث ورفع تقرير لموظفي الإدارة في قسم خدمات تقنية المعلومات وسيتم توصيف التدابير التصحيحية حسب الحاجة. وتشمل الأحداث المتعلقة بالحماية التالي :

- هجمات منفذ الماسح الضوئي
- وجود أدلة على دخول غير مصرح به إلى حسابات أو بيانات مميزة
- أحداث غريبة لا ترتبط بتطبيقات محددة على المضيف

المطابقة:

- يتم تنفيذ عمليات التدقيق بشكل منتظم من قبل جهات مرخص لها داخل الجامعة.
- تتم إدارة عمليات التدقيق من قبل مجموعة من المراجعين الداخليين للجامعة أو موظفي أمن المعلومات، وفقا لسياسة التدقيق الموثقة. يتم تصفية النتائج التي لا علاقة لها بمجموعة تنفيذية معينة من قبل موظفي أمن المعلومات، ومن ثم عرضها على موظفي الدعم المناسب لمعالجتها أو إيجاد مبررات لها.
- يتم بذل جهود كافية لمنع عمليات التدقيق من التسبب في فشل أو تعطيل عملية التشغيل .

٤. تطبيق القانون:

في حالة انتهاك هذه السياسة من قبل أي مستخدم مرخص له, فإنه يعتبر غير مرخص له ويخضع لإجراءات تأديبية وفقا لبند تطبيق القانون الموجود في سياسة الاستخدام الغير مرخص به .

سياسة الإتصال بالإنترنت

١. نظرة عامة:

تحتوي هذه السياسة على مكونات سياسة المستخدم وسياسة تقنية المعلومات الداخلية ويحدد قسم سياسة المستخدم كيفية السماح للمستخدمين الاتصال بالإنترنت ويزود المستخدم ايضا بكافة الشبكات التي يمكن الاتصال بها سواء عن طريق جهاز المودم أو الشبكة اللاسلكية بالإضافة إلى المتطلبات الأساسية للحصول على إذن الاستخدام مثل عمليات جدار الحماية من أجل حماية الاتصال.

تتطلب سياسة الاتصال بالإنترنت من المستخدمين استخدام الانترنت لأمور العمل فقط، وتجنب الذهاب إلى مواقع مشبوهة يمكن أن تهدد أمن الشبكة. كما تذكر السياسة بأنه قد يتم تسجيل ورصد نشاطات المستخدم . كما تحدد السياسة أي نظام سيتم استخدامه لمنع الوصول إلى مواقع غير مسموح بها وأي نظام سيقوم بتسجيل نشاط استخدام الإنترنت. بالإضافة إلى تحديد ما إذا كان سيتم استخدام ملقم وكيل لاستخدام وكيفية حماية الشبكة من أجل منع المستخدمين من الوصول إلى مواقع مشبوهة.

٢. الهدف:

تم صياغة هذه السياسة لحماية موارد الجامعة من أي اختراق من قبل برمجيات ضارة والتي يمكن أن تتسلل إلى الشبكة من قبل المستخدمين في حال استخدامهم لشبكة الانترنت. كما تهدف لمنع الاتصالات غير المصرح بها وغير المحمية بشبكة الإنترنت والتي قد تسمح لمجموعة من المحتويات غير الآمنة للدخول إلى شبكة الجامعة والتي قد تضر بأمن الشبكة وسلامة البيانات .

٣. الاتصال المادي بالأنترنت:

يجب اعتماد جميع الاتصالات بالأنترنت أو أي شبكات أخرى من قبل قسم تقنية المعلومات. معظم المستخدمين يقومون بالاتصال بالإنترنت من خلال شبكات الاتصال في المكاتب المعدة من قبل قسم تقنية المعلومات. أما بالنسبة لأي اتصالات إضافية فيجب اعتمادها من قبل قسم تقنية المعلومات وهي كالتالي:

- اتصال مودم من كمبيوتر أو جهاز الاتصالات والذي قد يسمح للاتصال بالشبكة.
- يجب فحص أي طابعة أو جهاز فاكس متعدد الأغراض ومتصل بالشبكة من قبل عمادة تقنية المعلومات.
- لا يسمح الوصول إلى نقاط الشبكة اللاسلكية أو أجهزة لاسلكية إلا بعد اعتمادها من قبل قسم تقنية المعلومات. كما يجب إغلاق أجهزة الكمبيوتر أو الأجهزة الأخرى التي لديها قدرة لاسلكية قبل اتصالها بالشبكة ما لم تتم الموافقة عليها من قبل قسم تقنية المعلومات عند الاتصال بالشبكة.

يجب مراجعة أي اتصالات بالأنترنت غير مدعومة من قبل قسم تقنية المعلومات والموافقة عليها، وعادةً ما تتطلب أي اتصالات إضافية من شبكة الجامعة لشبكة الانترنت أو أي شبكة أخرى الأمور التالية.

- جدار حماية معتمد من قبل قسم تقنية المعلومات يعمل في جميع الأوقات بشكل جيد.
- قد تتطلب بعض الاتصالات تشفير خلال الاتصال يخضع لمراجعة البيانات من أجل انتقالها عن طريق قسم تقنية المعلومات.

٤. استخدام الإنترنت:

- يجب على جميع الموظفين استخدام الإنترنت لأغراض العمل فقط.
- يمكن مراقبة وتسجيل استخدام الموظف للأنترنت بما في ذلك جميع المواقع التي تمت زيارتها ومدة هذه الزيارات وكمية البيانات التي تم تحميلها وأنواع البيانات التي تم تحميلها.
- على جميع الموظفين توخي الحذر عند زيارة مواقع الإنترنت غير المعروفة، والإبقاء على إعدادات المتصفح الموحدة والمعتمدة من قبل تقنية المعلومات من أجل الحماية من المواقع الضارة. وسيتم تدريب الموظفين على أحدث المعايير المعتمدة من تقنية المعلومات للحماية من البرمجيات الضارة.

٥.التحكم بالأنترنت ونظام التسجيل:

لابد من توافر الإمكانيات التالية لأي نظام يعمل على الشبكة:

- القدرة على منع المستخدمين من زيارة مواقع الويب غير الملائمة أو الإباحية، أو الخطرة، وأن يكون لديها قاعدة بيانات للمواقع المصنفة يتم تحديثها بانتظام.

- القدرة على تسجيل نشاط الإنترنت للمستخدم بما في ذلك:
  - وقت نشاط الإنترنت.
  - مدة النشاط.
  - المواقع التي تم زيارتها.
  - نوع البيانات التي تم تحميلها
  - قدرة النظام على تخزين صفحات الويب لزيادة سرعة الاتصال بشبكة الانترنت وهذا يتطلب ملقم وكيل.

- معرفة ما إذا كان النظام سيقوم بطلب (معرف / أولا) لتسجيل دخول الشبكة الحالية لتعريف المستخدمين. .

إن النظام المستخدم لمنع المستخدمين من زيارة مواقع الويب غير الملائمة أو الإباحية أو الخطرة هو SRVPROXY٠١. هذا النظام لا يحتاج إلى معرف تسجيل دخول إضافي وسوف يستخدم Active Directory لتحديد مستخدمي الإنترنت. هذا النظام قادر على تسجيل وقت نشاط الإنترنت، ومدة النشاط، والمواقع التي تم زيارتها، وأنواع البيانات التي تم تحميلها بالإضافة إلى تخزين صفحات الويب.

٦.تطبيق القانون:

بما أن الاستخدام غير المناسب لأجهزة الكمبيوتر المتنقلة يمكن أن يجلب برامج ضارة قد تضر بسلامة موارد الشبكة والأنظمة، لذلك فإن منع هذه البرامج أمر مهم لأمن الجامعة ومنسوبيها وجميع الأفراد، وأي موظف لا يلتزم بهذه السياسة قد يخضع لإجراءات تأديبية معتمدة من قبل الإدارة العليا.

سياسة شراء معدات تقنية المعلومات ومنع الفشل

١. نظرة عامة:
تحتوي هذه السياسة على توجيهات بخصوص شراء أجهزة لتقنية المعلومات تقوم بدعم الخدمات المهمة للجامعة. كما تذكر هذه السياسة الخدمات الأساسية و المبادئ التوجيهية لشراء التقنيات التي تتمتع بكفاءة عالية ولا تحتمل الأخطاء.

٢. الهدف:
إن الهدف من هذه السياسة هو ضمان عدم تعثر الخدمات الأساسية بسبب أي خطأ. بالإضافة إلى توفير مبادئ توجيهية موحدة تضمن أن أداء الأجهزة التي تم شراءها للخدمات الأساسية لتقنية المعلومات وذلك من أجل ضمان عدم انقطاعها عن تقديم الخدمات الأساسية.

٣. النطاق:
تشمل هذه السياسة أي أجهزة كمبيوتر يمكن أن توفر خدمات أساسية للجامعة.

٤. الخدمات الأساسية:
إن الخدمات الأساسية المطلوبة من أجل عمل الجامعة هي كما يلي:
- خدمة مشاركة الملفات على خادم مشاركة الملفات.
- خدمات الإنترنت و شبكة الإنترنت
- خدمات البريد الإلكتروني
- خدمات قواعد البيانات للمستخدمين الداخليين والتطبيقات الخارجية المهمة.
- خوادم التطبيقات الخارجية المهمة.
- خوادم وحدة التحكم بالمجال او السيرفر.
- توصيل هذه الخدمات إلى شبكة الإنترنت عن طريق جدار الحماية.

يجب على جميع الخادمات أو الأجهزة التي تقوم بدعم هذه الخدمات المهمة أن تكون مطابقة لهذه السياسة بما في ذلك أجهزة الاتصال من الانترنت الى هذه الخدمات.

٥. متطلبات الأجهزة:
بجب عند شراء معدات تقنية المعلومات ومنع الفشل الاستفادة من جميع التقنيات بما في ذلك:
- امدادات الطاقة المزدوجة على كافة الملقمات التي توفر الخدمات الأساسية.
- مصفوفة أقراص RAID لمنع فشل قرص واحد من تعطيل الخدمات.
- مزودات الطاقة التي لا تنقطع والتي يمكن أن توفر الطاقة لمدة لا تقل عن ساعة إلى الخوادم التي تقدم خدمات أساسية في حال انقطاع التيار الكهربائي.

٦. متطلبات إضافية:
بالنسبة للخدمات التي تعتبر بالغة الأهمية للدخل أو العمليات التي لا يمكن توقفها فإنه ينصح بالتقنيات التالية:
- مولد احتياطي لضمان ان انقطاع التيار الكهربائي على المدى الطويل لا يؤدي إلى قطع الخدمة.
- توافر أكثر من خادم لنفس الخدمة حيث يتم استخدام تقنية توزيع

سياسة جهاز الحاسب المحمول

١. نظرة عامة

تحدد هذه السياسة استخدام أجهزة الحاسب المحمول في الجامعة وهي كالتالي:.

- العمليات التي يجب أن يمر بها الحاسب المحمول لمغادرة شبكة الجامعة. يجب حماية كل من الجهاز وأي بيانات حساسة باستخدام كلمة مرور.
- كيفية حماية أجهزة الحاسب المحمول والأجهزة الأخرى أثناء عملها خارج شبكة الجامعة.
- العمليات التي يجب أن تمر بها أجهزة الحاسب المحمول من أجل الدخول لشبكة الجامعة في حال تم إحضارها إلى مبنى تملكه الجامعة.

٢. الهدف:

إن الهدف من هذه السياسة هو حماية البيانات السرية التي يمكن تخزينها على أجهزة الحاسب المحمول، بالإضافة إلى حماية شبكة الجامعة من أي هجوم عدائي عند إعادة أجهزة الحاسب المحمول. كما تأخذ هذه السياسة الدخول اللاسلكي في عين الاعتبار.

٣. النطاق:

تشمل هذه السياسة جميع أجهزة الحاسب التي يتم إحضارها إلى الجامعة أو تكون متصلة بشبكة الجامعة باستخدام أي وسيلة اتصال ومن هذه على سبيل المثال سطح المكتب لأجهزة الحاسب والأجهزة المحمولة.

ملاحظة: يجب الأخذ في الاعتبار عند كتابة هذه السياسة حساسية البيانات المخزنة والمعروضة على جهاز الكمبيوتر المحمول بما في ذلك:

- البريد الإلكتروني
- البيانات المخزنة محليا ويعمل عليها المستخدم.
- البيانات المخزنة مؤقتا محليا، مثل البيانات المخزنة مؤقتا من متصفح المستخدم. يسمح ويندوز إكس بي بتشفير الملفات المخزنة مؤقتا باستخدام ملف تشفير.
- نظام (EFS).
- بيانات من الشبكة الداخلية التي يمكن للمستخدم الوصول إليها أثناء تواجد الكمبيوتر خارج الشبكة.
- أسماء المستخدمين وكلمات المرور المخزنة محليا.

كما ينبغي التنبه إلى فقدان البيانات جراء التالي:

- السرقة - هل تم تشفير البيانات المخزنة محليا؟
- فشل القرص الصلب

٤. المسؤولية:

على المستخدم للحاسب المحمول القبول بتحمل المسؤولية عن طريق اتخاذ احتياطات السلامة اللازمة الخاصة بالحاسب المحمول وأن يوافق على الالتزام بهذه السياسة. لن يمنح أي مستخدم صلاحيات إدارية إلا في حال منحه استثناء خاص من قبل مسؤول الشبكة. كما يجب على مستخدم الكمبيوتر الموافقة على عدم استخدام الكمبيوتر المحمول لأغراض تجارية خاصة .وأن يلتزم بسياسة استخدام الكمبيوتر للجامعة.

٥. شروط الاتصال:

- يجب تحديد مدى منفعة الأجهزة المتصلة بشبكة الجامعة وليس وجودها من أجل راحة مدير تقنية المعلومات.
- يجب تحديد جميع الأجهزة النقالة التي تملكها الجامعة أو المسموح بها على شبكة المنشأة بعنوان MAC تقنية المعلومات قبل اتصالها. (من الممكن طلب عنوان IP الثابت)
- يجب أن يستوفي الجهاز معايير الاتصال بالكمبيوتر كما هو موضح في القسم التالي.
- يجب تعريف مشغل الجهاز باسم ومعلومات الاتصال لقسم تقنية المعلومات.
- يجب أن يكون مشغل جهاز الكمبيوتر متوافق مع سياسة الاستخدام المقبول للجامعة.
- لابد أن تخضع الأجهزة التي لا تملكها المنشأة لمراجعة برامجها في أي وقت للتأكد من عدم وجود برامج يمكن أن تهدد أمن الشبكة.
- لا يمكن نقل صلاحية الوصول إلى شبكة الجامعة لشخص آخر حتى لو كان هذا الشخص يستخدم جهاز مصرح به.

٦. حماية جهاز الكمبيوتر المحمول

١. يجب إجراء التالي على أي كمبيوتر محمول للجامعة في جميع الأوقات من أجل حماية الجهاز :

- استخدام برنامج مكافحة الفيروسات TrendMicro مع أحدث التحديثات للبرنامج إن أمكن. يجب أن يتم ضبط إعدادات البرنامج للحصول على حماية دائمة ومستمرة طوال الوقت وذلك من أجل استرجاع التحديثات بشكل يومي، وإجراء فحص للفيروسات والبرامج الضارة مرة واحدة على الأقل أسبوعيا.
- استخدام جدار الحماية TrendMicro IDF مع أحدث التحديثات للبرنامج إن أمكن. يجب أن يعمل البرنامج في جميع الأوقات التي يكون فيها جهاز الكمبيوتر متصل بشبكة غير موثوق بها بما في ذلك شبكة الانترنت لحماية الكمبيوتر من البرامج الضارة.
- يجب تفعيل برامج إضافية لحماية أجهزة الكمبيوتر وفقا لسياسة مكافحة الفيروسات والبرامج الضارة.
- يجب أن تكون مستويات تصحيح التطبيق ونظام التشغيل متماشية مع مستويات التصحيح الحالية للجامعة والمماثلة للأجهزة وأنظمة التشغيل. كما يجب تعطيل الاتصال اللاسلكي لجميع أجهزة الكمبيوتر المحمول في الجامعة. أما في حالة استخدام الاتصال اللاسلكي، فيجب وضع بروتوكولات معينة للتشفير اللاسلكي وضبط الإعدادات. كما تجب ملاحظة جميع فئات البيانات الحساسة للكمبيوتر بناء على أمنية الدخول اللاسلكي وغيرها من خصائص الكمبيوتر.

٢. سياسة أجهزة الكمبيوتر المحمولة المملوكة للجامعة والتي تم استخدامها خارج أوقات العمل من قبل الموظفين المصرح لهم للعمل من المنزل.

- يجب أن تستوفي هذه الأجهزة الشروط المذكورة في ٦,٠,١ أعلاه.
- في حال فشل الكمبيوتر في استيفاء المتطلبات المذكورة في ٦,٠,١ أعلاه، فإنه يتعين على الموظف إبلاغ إدارة أمن المعلومات والتي بدورها يتوجب عليها القيام بفحص الكمبيوتر بشكل مماثل لأي جهاز كمبيوتر غير آمن تم إدخاله إلى المبنى.
- يجب التأكد من أن الأشخاص غير المرخص لهم لا يمكنهم الوصول إلى جهاز الكمبيوتر من دون اسم مستخدم وكلمة مرور صحيحة. كما لا يمكن استخدام أنظمة التشغيل التي لا تدعم هذه العملية في أجهزة الكمبيوتر المحمول. إن قسم أمن تقنية المعلومات سيقوم بتحديد الأدوات المناسبة لاستخدامها للمصادقة والتحكم بالدخول.
- سيتم تقييم البيانات التي يتم تخزينها على الكمبيوتر للنظر في مدى

حساسية البيانات وفقا لوثيقة عملية تقييم البيانات. وسيتم تخزين البيانات التي تعتبر حساسة بتنسيق مشفر، وقد يتم استخدام نظام تشفير الملفات (EFS). كما يجب أن تحدد السياسة أداة التشفير المستخدمة وكيفية الحفاظ عليه.

- يجب فحص جهاز الكمبيوتر أسبوعيا من قبل أفراد عمادة تقنية المعلومات في أوقات معينة عند إدخال الكمبيوتر إلى منطقة أمنية قرب المبنى. وسوف يشمل الفحص البرمجيات الضارة واختبار تحديد ما إذا كان الكمبيوتر يحتوي على دوده. كما سيتم فحص حالة البيانات الحساسة المخزنة للتأكد من تشفيرها وما إذا كان تم تخزين بيانات ذات مستوى عالي من الأمنية على جهاز الكمبيوتر. كما يجب إزالة أية برامج ضارة على الكمبيوتر إذا تم الكشف عنها وتسجيل معلومات حول أي برامج ضارة إن وجدت. كما يجب تسجيل أي معلومات عن البيانات التي تم تخزينها بشكل غير صحيح.

٣. سياسة أجهزة الكمبيوتر التي تستخدم للسفر - إن حماية هذه الحواسيب يكون عن طريق تشفير كافة البيانات الحساسة ويشترط الحصول على معرف مستخدم صالح لتشغيل الكمبيوتر.

٤. يجب استيفاء الشروط المذكورة في ٦,٠,١ أعلاه. وإذا كان هناك داعي لتثبيت برامج إضافية، فيجب أن يتم ذلك قبل أن يتم إخراج الحاسب من المبنى.

٥. يجب التأكد من أن الأشخاص غير المرخص لهم لا يمكنهم الوصول إلى جهاز الكمبيوتر من دون اسم مستخدم وكلمة مرور صحيحة. كما لا يمكن استخدام أنظمة التشغيل التي لا تدعم هذه العملية في أجهزة الكمبيوتر المحمول. إن قسم أمن تقنية المعلومات سيقوم بتحديد الأدوات المناسبة لاستخدامها للمصادقة والتحكم بالدخول.

٦. سيتم تقييم البيانات التي يتم تخزينها على الكمبيوتر للنظر في مدى حساسية البيانات وفقا لوثيقة عملية تقييم البيانات. وسيتم تخزين البيانات التي تعتبر حساسة بتنسيق مشفر، وقد يتم استخدام نظام تشفير الملفات (EFS). كما يجب أن تحدد السياسة أداة التشفير المستخدمة وكيفية الحفاظ عليه. وسيتم إزالة أية بيانات لا تعتبر آمنة على جهاز الكمبيوتر باستخدام برنامج معين للتأكد من أنه تمت إزالتها بشكل نهائي بحيث لا يمكن قراءتها باستخدام تقنية خاصة في وقت لاحق. وسوف تكون هناك قائمة للبيانات الحساسة الموثقة بما في ذلك مواقع تخزين كافة البيانات الحساسة المخزنة على الكمبيوتر. وسيتم إنشاء هذه القائمة قبل أن يتم إخراج الكمبيوتر من المبنى.

٧. إذا كان هناك مجال من رؤية المستخدم لبيانات حساسة باستخدام متصفح الويب أو غيرها من البرنامج، فإن ذلك يحتاج إلى تشفير البيانات المخزنة مؤقتا. سيتم تشفير البيانات التي تم تخزينها مؤقتا محليا مثل البيانات المخزنة مؤقتا في متصفح المستخدم عن طريق استخدام نظام تشفير الملفات (EFS) وهذا يتطلب Windows XP أو بعض برامج محايده. قد يتم تنفيذ ذلك باستخدام نظام التشغيل Windows XP، وذلك عن طريق الإجراء التالي:

١. افتح «جهاز الكمبيوتر»
٢. انقر على «أدوات» وحدد «خيارات المجلد».
٣. حدد على التبويب «الملفات دون اتصال»
٤. ضع علامة في المربع بجانب «تشفير الملفات دون اتصال لتأمين البيانات».
٥. انقر على زر «موافق» للخروج.

٨. إذا كان الكمبيوتر سيستقبل بيانات مهمة، فيجب على مستخدم الكمبيوتر إخطار عمادة تقنية المعلومات بحيث يمكن إجراء الترتيبات اللازمة لطريقة لدعم الاحتياطي للبيانات.

- **سياسة أجهزة الكمبيوتر المستخدمة من قبل المتعاقدين**
- سيتم فحص جهاز الكمبيوتر للتأكد من استيفاءه للشروط المذكورة في القسم ٦,٠١ أعلاه.
- سيتم فحص الكمبيوتر بحثا عن برامج ضارة واختباره لتحديد ما إذا كان الكمبيوتر يحتوي على دودة. كما يجب إزالة أي برامج ضارة على الكمبيوتر إذا تم اكتشافها وتسجيل معلومات حول أي برامج ضارة إن وجدت.
- إذا كان جهاز الكمبيوتر متوافق مع القسم ٦,٠١ ولا يحتوي على أي برمجيات ضارة، فيجب على المتعاقد الإبلاغ عن أي بيانات حساسة متعلقة بالجامعة والتي من المتوقع أن يتم تخزينها على جهاز الكمبيوتر.
- سيتم تقييم البيانات التي يتم تخزينها على الكمبيوتر للنظر في مدى حساسية البيانات وفقا لوثيقة عملية تقييم البيانات. وسيتم تخزين البيانات المخزنة على الكمبيوتر والتي تعتبر حساسة بتنسيق مشفر، وقد يتم استخدام نظام تشفير الملفات (EFS). كما يجب أن تحدد السياسة أداة التشفير المستخدمة وكيفية الحفاظ عليه.
- يجب تسجيل معرف الكمبيوتر ومصادقته للاستخدام على شبكة الجامعة.
- يجب فحص جهاز الكمبيوتر أسبوعيا من قبل أفراد قسم أمن تقنية المعلومات في أوقات معينة عند إدخال الكمبيوتر إلى منطقة أمنية قرب المبنى. وسوف يشمل الفحص البرمجيات الضارة واختبار تحديد ما إذا كان الكمبيوتر يحتوي على دوده. كما سيتم فحص حالة البيانات الحساسة المخزنة للتأكد من تشفيرها وما إذا كان تم تخزين بيانات ذات مستوى عالي من الأمنية على جهاز الكمبيوتر. كما يجب إزالة أية برامج ضارة على الكمبيوتر إذا تم الكشف عنها وتسجيل معلومات حول أي برامج ضارة إن وجدت وتسجيل معلومات حول أي بيانات لم يتم حفظها بشكل جيد . كما يجب مراجعة شهادة الكمبيوتر في حال عدم حفظ البيانات بشكل جيد.

لا. حماية الشبكة:

يتطلب عند اتصال أجهزة الكمبيوتر المحمول بشبكة الجامعة استيفاء المتطلبات التالية:

١. إذا كان جهاز الكمبيوتر مملوكا للجامعة ويتم استخدامه بانتظام من قبل الموظفين وفقا ل ٤,٠ أعلاه، فيجب فحص جهاز الكمبيوتر وفقا لذلك الجزء من السياسة.

٢. إذا كان جهاز الكمبيوتر مملوكا للجامعة وتم إعادته بعد أن تم استخدامه من قبل موظف في السفر ,فيجب تنفيذ الاجراءات التالية:

- يجب التأكد من أن برنامج مكافحة الفيروسات محدث، ويحتوي على أحدث تعريفات الفيروسات، بالإضافة إلى ضبط الإعدادات وأن البرنامج يعمل بشكل صحيح. إذا فشل الكمبيوتر في استيفاء الشروط السابقة أو لم يتم فحصه خلال الأسبوع الماضي، فيجب فحصه بشكل كامل قبل أن يتم استخدامه في المبنى.
- يجب اختبار جهاز الكمبيوتر وفحصه للتأكد من الفايروسات مثل

adware أو برامج التجسس لتحديد ما إذا كان الكمبيوتر يحتوي على دودة أو لا.

- يجب اختبار حالة البيانات الحساسة المخزنة للتأكد من تشفيرها.
- يجب إزالة أية أي برامج ضارة على الكمبيوتر إذا تم الكشف عنها وتسجيل معلومات حول أي برامج ضارة إن وجدت. بالإضافة إلى تسجيل أي معلومات عن البيانات التي لم يتم تخزينها بشكل صحيح.

٣. إذا كان الجهاز ملكا للجامعة فيجب عمل التالي.

- يتطلب على الجامعة الاتفاق خطيا على السماح لمسح البرامج الضارة من أجهزة الكمبيوتر الخاصة به والموافقة على دفع أي تكاليف إذا تم العثور على برامج ضارة في أجهزة الكمبيوتر.
- يجب عمل فحص كامل للفيروسات.
- يجب اختبار جهاز الكمبيوتر وفحصه للتأكد من الفايروسات مثل adware أو برامج التجسس لتحديد ما إذا كان الكمبيوتر يحتوي على دودة أو لا.
- يجب إزالة أية أي برامج ضارة على الكمبيوتر إذا تم الكشف عنها وتسجيل معلومات حول أي برامج ضارة إن وجدت. قد يتم فرض رسوم على المنشأة الخارجية لأي خدمات بناء على سياسة الجامعة.

٨. تطبيق القانون:

بما أن الاستخدام غير السليم لأجهزة الكمبيوتر المحمول قد يعرض الشبكة لكثير من الهجمات والاختراقات، لذلك فإن الاستخدام السليم والمرخص له لأجهزة الكمبيوتر المحمول يعتبر أمر مهم لأمن الجامعة وجميع أفرادها فإن الموظفين الذين لا يلتزمون بهذه السياسة قد يتعرضون لإجراءات تأديبية قد تصل في بعض الاحيان إلى الفصل.

سياسة السرية للجامعة

١. الهدف:

إن الاطلاع على معلومات سرية من قبل موظفي جامعة المجمعة ممكن ويعتمد ذلك على علاقة الموظف بالجامعة.

٢. النطاق:

يجب على جميع المستخدمين المصرح لهم ممن لديهم صلاحية الاطلاع على المعلومات السرية الإبقاء عليها بشكل جيد وعدم اطلاع الآخرين. تتضمن المعلومات السرية على سبيل المثال الأنواع التالية من المعلومات:

- معلومات تربوية وخاصة بالموظف بالإضافة إلى معلومات خاصة.
- كتيبات العمليات وممارسات الجامعة و الخطط الدراسية، والتقنيات والمواد، وخطط التنمية، والمعلومات المالية
- قوائم مرتبات الموظفين وسجلات الرواتب والسجلات المتعلقة بالبائعين والموردين وغيرها من المعلومات بشأن الشؤون التجارية أو الممارسات التشغيلية للجامعة.

٣. السياسة:

يجب عدم الإفصاح عن أي معلومات سرية، أو إزالتها من مقر الجامعة أو نسخها أو نقلها أو حتى استخدامها بأي طريقة أخرى من قبل المستخدمين المصرح لهم لأي أغراض خارج نطاق العمل. كما لا يجب كشف المعلومات السرية لغير موظفين الجامعة من دون موافقة خطية من قبل موظفي الإدارة. إن المعلومات المخزنة على شبكة تقنية المعلومات تعتبر سرية ولا يجوز نشرها خارج الجامعة إلا في سياق العمل أو بتفويض من موظفي الإدارة. كما لا يمكن للمستخدمين المرخص لهم إزالة أو استعارة أي أجهزة كمبيوتر أو أقراص، أو منتجات متعلقة بالتكنولوجيا ما لم يرخص لهم بذلك.

٤. تطبيق القانون:

في حالة انتهاك هذه السياسة من قبل أي مستخدم مرخص له, فإنه يعتبر غير مرخص له ويخضع لإجراءات تأديبية وفقا لبند تطبيق القانون الموجود في سياسة الاستخدام الغير مرخص به.

إجراءات كلمة المرور

١. نظرة عامة

يجب على جميع الموظفين والعاملين الذين لديهم القدرة على الدخول على أنظمة كمبيوترالجامعة الالتزام بإجراءات كلمة المرور الموضحة أدناه من أجل حماية أمن الشبكة، وحماية سلامة البيانات، وحماية أنظمة الكمبيوتر.

٢. الهدف:

تم تصميم هذه الإجراءات لحماية موارد الجامعة على الشبكة عن طريق طلب كلمات مرور قوية بالإضافة إلى حماية كلمات المرور هذه، ووضع حد أدنى من الوقت لتغيير كلمات المرور.

٣. النطاق:

تنطبق هذه الإجراء على جميع الموظفين الذين لديهم حساب على كمبيوتر والذي يتطلب كلمة مرور على شبكة الجامعة بما في ذلك حساب المجال (domain) وحساب البريد الإلكتروني.

٤. حماية كلمة المرور:

- عدم تدوين كلمة المرور أبدا.
- عدم إرسال كلمة المرور عن طريق البريد الإلكتروني.
- عدم إدراج كلمة المرور في وثيقة مخزنة بدون تشفير.
- عدم إخبار أي أحد عن كلمة المرور.
- لا تكشف كلمة المرور الخاصة بك عبر الهاتف.
- لا نترك أي تلميح حول شكل كلمة المرور الخاصة بك.
- لا تكشف أو تلمح إلى كلمة المرور الخاصة بك على شبكة الانترنت.
- لا تستخدم خاصية «تذكر كلمة المرور» لبرامج التطبيقات مثل انترنت اكسبلورر، و برنامج البريد الإلكتروني الخاص بك، أو أي برنامج آخر.
- لا تستخدم كلمة مرور الشبكة أو الجامعة الخاصة بك على أي حساب عبر الانترنت لا يحتوي على تسجيل دخول آمن بحيث يبدأ عنوان متصفح الويب ب https:// بدلا من http://
- الإبلاغ عن أي اشتباه في اختراق كلمة المرور الخاصة بك لإدارة أمن المعلومات في الجامعة.
- إذا سألك أي شخص عن كلمة المرور الخاصة بك, يرجى إبلاغ إدارة أمن المعلومات في الجامعة.
- لا تستخدم اختصارات شائعة كجزء من كلمة المرور.
- لا تستخدم الكلمات الشائعة أو هجاء عكسي للكلمات كجزء من كلمة المرور.
- لا تستخدم أسماء الأشخاص أو الأماكن كجزء من كلمة المرور.
- لا تستخدم جزءا من اسم تسجيل الدخول الخاص بك في كلمة السر.
- لا تستخدم أرقام سهلة التذكر مثل أرقام الهاتف، رقم الهوية الشخصية، أو عناوين الشوارع كجزء من كلمة المرور.
- كن حذرا من السماح للآخرين من رؤيتك أثناء كتابة كلمة المرور الخاصة بك.

٥.متطلبات كلمة المرور (قابلة للتغيير):

يجب على من يقومون بوضع متطلبات كلمة المرور تذكر أن جعل القواعد صعبة جدا قد يقلل من الأمنية نظرا لأن المستخدمين قد يجدون أنها صعبة التنفيذ أو مستحيلة. إذا كان من المتطلبات أيضا تغيير كلمة المرور بشكل متكرر، فإن المستخدمين قد يميلون إلى تدوين كلمة المرور أو اختيار كلمة مرور مقاربة أو مشتقة من كلمة المرور القديمة والذي سيجعلها سهلة الاختراق. سيتم تعيين متطلبات كلمة المرور التالية من قبل إدارة أمن المعلومات:

١.لا يجب أن يقل طول كلمة المرور عن ٨ أحرف.
٢.لا يوجد حد أعلى لعدد الأحرف.
٣.تعقيد كلمة المرور:
- يجب أن تتضمن كلمة المرور أنماط الأحرف التالية:
  - أحرف صغيرة.
  - أحرف كبيرة.
  - أرقام.
  - رموز (مثل: !@ # $٪ ^ & * () {} []).

- تحدد طول كلمة المرور المستخدمة الحد الأدنى من عدد الأنماط أعلاه اللازم توفرها, وذلك على الشكل التالي:
- من ٨ – ١١ حرف: يتطلب جميع الأنماط.
- من ١٢ – ١٥ حرف: يتطلب الثلاث أنماط الأولى فقط.
- من ١٦ – ١٩ حرف: يتطلب النمطين الأوليين فقط.
- ٢٠ وما فوق: لا توجد شروط.

- عدم استخدام أي كلمات واردة في القواميس والمعاجم في حال كان طول الكلمة أقل من ١٦ حرف.

٤.تاريخ كلمة المرور:
-لا يسمح بإعادة استخدام كلمة مرور سابقة الا بعد ١٢ تغيير للكلمة.
-الحد الأعلى لعمر كلمة المرور: يجب تغيير كلمة المرور بعد مرور ٩٠ يوم على عمر الكلمة.
-الحد الأدنى لعمر كلمة المرور: لا يسمح بتغيير كلمة المرور قبل مرور يوم واحد على تاريخ الكلمة.

٥.في حال الرغبة بتخزين كلمات المرور بتشفير قابل للفك, ينبغي أخذ الموافقة المسبقة من عمادة تقنية المعلومات لأن ذلك من شأنه أن يقلل من أمن كلمة المرور للمستخدم.

٦.إقفال الحساب (Account Lockout):

a.يجري إقفال الحساب المستخدم بعد ٤ محاولات فاشلة لتسجيل للدخول.
b.لا يتم إعادة احتساب تكرار المحاولات الدخول الخاطئة قبل أن تمر ٢٠ دقيقة بعد كل محاولة. فعلى سبيل المثال, في حال حصول ثلاث محاولات فاشلة خلال ٢٠ دقيقة, سيتم إقفال الحساب في حال كانت المحاولة الرابعة قبل انتهاء هذه المدة.
c.يتم إعادة فتح الحساب المغلق بعد ٣٠ دقيقة من آخر محاولة دخول فاشلة.

٧.يتم إغلاق سطح مكتب لأجهزة الجامعة بعد مضي ٥ دقائق على عدم استخدام الجهاز. وسوف يحتاج المستخدم لإعادة تسجيل دخوله في النظام. بكل الأحوال يجب على جميع المستخدمين عدم ترك جهازه مفتوح, ويمكن إغلاق سطح المكتب بشكل سريع من خلال الضغط على مفاتيح الاختصار معاً (L + ⊞)

إن القواعد الخاصة بكلمات المرور أعلاه أيضاً تنطبق على جمل المرور (Passphrases) والتي تستخدم في المصادقة بالمفاتيح الخاصة و العامة (Public/Private key authentication).

إن القواعد الخاصة بكلمات المرور أعلاه أيضاً تنطبق على جمل المرور (Passphrases) والتي تستخدم في المصادقة بالمفاتيح الخاصة و العامة (Public/Private key authentication).

٦. سياسة التحكم بكلمة المرور:

٦,١ حساب المدير الرئيسي للأنظمة و الأجهزة والخدمات (Root, Admin, Administrators)

- ٦,١,١ يجب عدم استخدام هذه الحسابات في الأعمال اليومية مع الأنظمة والأجهزة, كما لا ينبغي أن يكون معروفاً لدى أي شخص كان.
- ٦,١,٢ يتم إعطاء هذه الحسابات كلمات مرور بطول لا يقل عن ٢٠ حرف, ويتم تخزين هذه الكلمات السرية في مستند داخل ظرف مختوم محفوظ داخل خزنة وتكون بعهدة عميد تقنية المعلومات ووكيل العمادة.
- ٦,١,٣ تستخدم هذه الحسابات فقط في الحالات الطارئة كحالات الاستعادة.

٦,٢ يتم منح حسابات الموظفين المصرح لهم للعمل مع هذه الأجهزة والأنظمة والخدمات صلاحيات إدارية حسب ما يلزم لتأديته الأعمال الموكلة له.

٦,٣ تبادل كلمات المرور:
يمنع تبادل كلمات المرور الإدارية بأي شكل سواءً ورقي أو رقمي. في حال تم منح حساب جديد لأول مرة, يتم منح الحساب للموظف بكلمة مرور مؤقتة مع تفعيل خيار تغيير كلمة المرور عند أول عملية تسجيل دخول.

٦,٤ إلغاء كلمات المرور
يجب تغيير جميع كلمات المرور للموظفين في موقع معين فور استقالة موظف من هذا الموقع أو انتقاله لقسم آخر.

لا تطبيق القانون:

بما أن كلمة المرور أمر هام وحساس لأمن الجامعة والجميع، لذلك فإن أي موظف لا يلتزم بهذه الإجراءات سوف يخضع لإجراءات تأديبية.

سياسة الأمن المادي

١. نظرة عامة:
الأمن المادي يعني توفير حماية بيئية والتحكم بالوصول إلى الأجهزة والبيانات على شبكة تقنية المعلومات للجامعة من أجل حماية موارد تقنية المعلومات من الاستخدام الغير مرخص به، سواء من حيث الأجهزة أو البيانات.

٢. الغرض:
الغرض من هذه السياسة هو وضع معايير لمنح ومراقبة وإنهاء أي وصول فعلي إلى شبكة تقنية المعلومات من أجل حماية الأجهزة الموجودة في شبكة تقنية معلومات من العوامل البيئية.

٣. النطاق:
تنطبق هذه السياسة على قسم شبكة تقنية المعلومات بأكمله، بما في ذلك على سبيل المثال غرف وقاعات العرض، حجرات الشبكة، ومركز عمليات خدمات تقنية المعلومات.

٤. السياسة:
الحماية البيئية
- يجب تشغيل تكييف الهواء بشكل كاف في مرافق شبكة تقنية المعلومات والتي تضم موارد تقنية المعلومات لمنع تأثير الحرارة على المدى الطويل على تعطيل الأجهزة.
- يجب توفير أجهزة إطفاء الحريق في مرافق شبكة تقنية المعلومات وفحصها من قبل موظفي منظمة السلامة العامة.
- يجب أن تكون جميع موارد تقنية المعلومات في عمادة تقنية المعلومات مزودة بعازل حماية لمنع ارتفاع الطاقة والأضرار اللاحقة التي قد تصيب البيانات والأجهزة.
- يجب أن يتم ربط جميع موارد تقنية المعلومات بمزود طاقة (UPS) لا ينقطع أبدا وذلك لمنع ارتفاع الطاقة، والاضاءة، والأضرار اللاحقة التي قد تصيب البيانات والأجهزة.
- يجب ألا يتم الضغط على مأخذ التيار الكهربائي من خلال ربط العديد من الأجهزة. كما يجب مراجعة الاستخدام السليم والعملي لتمديد الأسلاك بشكل سنوي.
- يجب وضع جهاز استشعار الماء تحت أي منطقة مرتفعة.

الوصول المادي
- يجب أن تكون جميع أنظمة الأمن المادي لشبكة تقنية المعلومات مطابقة لجميع اللوائح، بما في ذلك، قوانين البناء وقوانين الوقاية من الحريق.
- يجب توثيق الدخول إلى جميع مرافق شبكة تقنية المعلومات وإدارتها من قبل خدمات تقنية المعلومات.
- حماية جميع مرافق شبكة تقنية المعلومات بما يتناسب مع أهمية وظيفتها.
- سيتم السماح لبعض موظفي تقنية المعلومات باستخدام مرافق شبكة تقنية المعلومات ممن تتطلب مسؤولياتهم ذلك.
- يجب أن تتم المصادقة على عملية السماح لموظفي شبكة تقنية المعلومات باستخدام مرافق شبكة تقنية المعلومات من قبل مدير خدمة تقنية المعلومات.
- يجب عدم مشاركة أجهزة الدخول الأمنية (مثل بطاقات الدخول والمفاتيح، والأرقام السرية، الخ) مع أي مستخدم غير مصرح له.
- يجب إعادة أجهزة الدخول الأمنية التي لم تعد هناك حاجة إليها إلى عمادة تقنية المعلومات، وتسجيلها بشكل مناسب قبل أن يتم إعادة تخصيصها لمستخدم آخر.
- يجب الإبلاغ عن أي أجهزة مسروقة أو مفقودة خاصة بأمنية الدخول إلى موظفي أمن المعلومات.
- يجب على الموظفين المسؤولين عن مرافق شبكة تقنية المعلومات إزالة أجهزة الدخول الأمنية من الأشخاص الذين لم يعد يتطلب منهم الدخول.
- يجب مرافقة ومراقبة الزوار والمدعوين إلى عمادة تقنية المعلومات أثناء زيارتهم لمرافق القسم.
- ١١. يجب على الموظفين المسؤولين عن مرافق شبكة تقنية المعلومات مراجعة سجلات الدخول وسجلات الزوار للقسم بشكل دوري.
- يجب أن تبقى جميع الأماكن التي تتواجد بها موارد تقنية المعلومات مقفلة عندما لا يتم شغلها من قبل الموظف، وذلك من أجل الحد من وقوع الدخول غير المصرح به.
- يجب تأمين أي جهاز من أجهزة شبكة تقنية المعلومات التي تتواجد في منطقة عامة بجهاز مثبط السرقة. كما يجب تأمين أجهزة الكمبيوتر المحمولة التابعة لشبكة تقنية معلومات عن طريق جهاز مثبط للسرقة.

٥. تطبيق القانون:
في حالة انتهاك هذه السياسة من قبل أي مستخدم مرخص له, فإنه يعتبر غير مرخص له ويخضع لإجراءات تأديبية وفقا لبند تطبيق القانون الموجود في سياسة الاستخدام الغير مرخص به.

سياسية الضوابط الأمنية للخوادم

١. الهدف:

تهدف هذه السياسية لتكون مرجع يستند إليه في إدارة الضوابط الأمنية للخوادم التابعة أو التي يتم تشغيلها من قبل الجامعة. وفي حال تم تنفيذ هذه الإجراءات بشكل جيد فإن ذلك سيؤدي إلى التقليل من الدخول الغير مصرح به إلى شبكة تقنية المعلومات وغيرها من المعلومات السرية والتقنية.

٢. النطاق:

تنطبق هذه السياسية على جميع الخوادم المادية والوهمية التابعة لجامعة المجمعة، سواءً المملوكة لها في مركز بيانات الجامعة أو المستأجرة في منشآت أخرى.

الملكية والمسؤوليات

يجب أن تخضع الخوادم الداخلية المشغلة في الجامعة لمسؤولية الفريق المختص من قسم نظم التشغيل بالإضافة للأفراد المصرح لهم بذلك من قبل وكالة الشؤون الفنية لعمادة تقنية المعلومات. كما يجب لكل قسم اتباع المعايير المعتمدة لإعدادات الخوادم حسب احتياجات العمل. كما يجب على الفريق الفني مراقبة امتثال إعدادات الضبط و الطلبات المعتمدة بشكل خاص حول أية استثناءات تم ملاحظتها. كما يجب على الفريق الفني قبل إجراء تغيير لمعايير إعدادات ضبط الخوادم، إعلام إدارة أمن المعلومات للمراجعة والموافقة.

٣. معايير ضبط الخوادم

- يجب تسجيل الخوادم ضمن نظام إدارة الحماية الخاص بالجامعة. ويتعين توفر المعلومات التالية كحد أدنى:
  - أ. أسماء الخوادم، والمكان، وأسماء النسخ الاحتياطية.
  - ب. رقم إصدار الجهاز و إصدار نظام التشغيل (OS).
  - ت. الخدمات الرئيسية والتطبيقات.
  - ث. إعدادت الشبكة (المنافذ, نوع وسائط الاتصال, الموقع في خريطة الشبكة)
- يجب أن تبقى المعلومات الموجودة في نظام إدارة الحماية محدثة.
- يجب أن تكون التغييرات لإعدادات للخوادم متوافقة مع سياسة التغيير.

معايير الإعدادات العامة

- يجب أن تتطابق إعدادات نظام التشغيل مع المعايير المعتمدة من قبل إدارة أمن المعلومات.
- يجب تعطيل الخدمات والتطبيقات الغير مستخدمة . في حال وجود أي استثناء يجب إشعار وأخذ موافقة إدارة أمن المعلومات.
- يجب حماية الخوادم برمجياً من خلال منتج الحماية المخصص للخوادم في الجامعة, وشبكياً من خلال وضعه في مجال شبكي مخصص للخوادم حسب طبيعة عمله مثل نطاق الخوادم الداخلي Servers Farm, والمنطقة المعزولة DMZ.
- تسجيل ومتابعة السجلات والأحداث الأمنية للخوادم مثل عمليات الوصول والمصادقة في الخوادم, من خلال نظام المراقبة الأمنية SIEM.
- يجب تثبيت البرمجيات الترقيعية (Security Patches) حالما تكون متاحة, الاستثناء الوحيد يكون للتطبيقات الهامة حينما تضر بمصلحة العمل.
- يعتبر الاتصال بين الأنظمة مبني على علاقات الثقة (Trust Relationship) خطرا أمنيا، ويجب الامتناع عن استخدامها خصوصاً إن توفرت أساليب أتصال أخرى.
- يجب على المستخدمين استخدام أقل الصلاحيات التي تكفي لتنفيذ وظيفة معينة مع الخوادم.
- الاتصال في الخادم يجب أن يتم من خلال قنوات إتصال آمنة (مثل الإتصال بإستخدام بروتوكول IPSec أو بروتوكول Secure Shell)
- يمنع على المستخدمين المصرح لهم من التعامل مع الخوادم في أماكن مكتبية لا تخضع للتحكم (مثال: جهاز مكتبي خارج النطاق الآمن للجامعة).

المراقبة:

- يجب تسجيل جميع الأحداث الأمنية الخاصة بالأنظمة الحساسة أو الهامة من قبل موظفي أمن المعلومات وحفظ عمليات التدقيق والتحليل كما يلي:
- أيجب حفظ جميع الأحداث المسجلة والمتعلقة بالحماية كما هو مذكور في معايير إعدادات الخادم أعلاه - البند ٤.
- يجب استعادة النسخ الاحتياطية اليومية كما هو مذكور في الوثيقة المحددة لمعايير الخادم.
- يجب استعادة النسخ الاحتياطية الأسبوعية كما هو مذكور في الوثيقة المحددة لمعايير الخادم.
- يجب استعادة النسخ الاحتياطية الشهرية كما هو مذكور في الوثيقة المحددة لمعايير الخادم.

٢. يجب إبلاغ موظفي أمن المعلومات عن الأحداث المتعلقة بالحماية الذين بدورهم يقومون بمراجعة سجلات الحوادث ورفع تقرير لوكالة الشؤون الفنية في عمادة تقنية المعلومات و لفريق الإستجابة للحوادث وسيتم توصيف التدابير التصحيحية حسب الحاجة.

قد تشمل الأحداث الأمنية ولكن غير محدودة بما يلي:

- هجمات فحص المنافذ.
- دلائل دخول غير مصرح بها إلى حسابات أو بيانات ذات إمتيازات معينة.
- أحداث غريبة لا ترتبط بتطبيقات محددة في المضيف.

الامتثال:

- يتم تنفيذ عمليات التدقيق بشكل منتظم من قبل مدقق أمني مصرح له في الجامعة.
- تتم إدارة عمليات التدقيق من قبل مجموعة المراجعين الداخليين التابعين لإدارة أمن المعلومات في الجامعة، وفقا لسياسة التدقيق الموثقة. كما يتم تصفية النتائج التي لا علاقة لها بالفريق الفني من قبل موظفي إدارة أمن المعلومات، ومن ثم عرضها على الفريق الفني المناسب لمعالجتها أو إيجاد مبررات لها.
- يتم بذل الجهود اللازمة لمنع عمليات التدقيق من التسبب في فشل أو تعطيل العمل.

٤. تطبيق القانون:

في حالة انتهاك هذه الإجراءات من قبل أي مستخدم مصرح له في الجامعة, فإنه سيعتبر غير مصرح له ويخضع لإجراءات تأديبية وفقا لبند تطبيق القانون الموجود في سياسة الاستخدام الغير المصرح.

سياسة استخدام الشبكة اللاسلكية

تعد سياسة الاستخدام للشبكة اللاسلكية أمر ضروري لأمن الكمبيوتر في وقتنا الحاضر نظرا للحاجة الماسة لوجود شبكة لاسلكية في أي منشأة. لذلك من الأفضل وضع شروط وتحديد أجهزة معينة تتم الموافقة عليها لاستخدام الشبكة اللاسلكية من أجل تقليل المخاطر الأمنية المرتبطة بالشبكة اللاسلكية.

١. نظرة عامة:

تحدد هذه السياسة استخدام الأجهزة اللاسلكية في الجامعة وتحديد كيفية ضبط إعدادات هذه الأجهزة عند الاستخدام.

٢. الهدف:

تم إعداد هذه السياسة لحماية موارد الجامعة من أي استخدام قد يؤدي لاختراق الشبكة عن طريق الشبكة اللاسلكية.

٣. النطاق:

تنطبق هذه السياسة على جميع الأجهزة اللاسلكية التي تستخدمها الجامعة أو أي شخص يقوم بالاتصال على شبكة الجامعة عن طريق جهاز لاسلكي.

٤. تقييم المخاطر:

إن استخدام تقنية اللاسلكي تسبب مخاطر أمنية لأي جامعة وذلك لأنها تعتبر أسهل نقطة دخول يمكن من خلالها الدخول على شبكة الجامعة. بالإضافة إلى ذلك فإنه يمكن قراءة البيانات المرسلة عبر تقنية اللاسلكي في بعض الأحيان حتى عند تشفيرها نظرا لضعف نظام التشفير المستخدم. لذلك فإن هذه السياسة تقوم بتقييم المخاطر في أي وقت يتم فيه إضافة نوع جديد من الأجهزة اللاسلكية إلى الشبكة. يجب تقييم عدة بنود منها:

- هل هذه تقنية جديدة؟
- هل هذا الجهاز يستخدم التشفير وإلى أي مدى تم اختبار بروتوكول التشفير؟
- ما هي تكلفة تنفيذ بروتوكول التشفير الآمن؟
- هل تم استخدام هذا النوع من الأجهزة من قبل على الشبكة؟
- هل يمكن ضبط إعدادات الجهاز للسماح للمستخدمين المصرح لهم فقط بالدخول للجهاز أو الشبكة؟
- إلى أي مدى يمكن لأي شخص التحايل على الجهاز للدخول بشكل غير نظامي؟ ماهي الطرق التي يمكن استخدامها؟
- ما هي إجراءات الحماية المتوفرة و ماهي تكلفة تنفيذها وصيانتها؟
- إلى أي مدى سيكون عمليا استخدام الشبكة اللاسلكية من ناحية السعر واحتمالية الخسائر؟

المصادقة أو التحقق

يجب أن يتم فحص آليات مصادقة كافة الأجهزة اللاسلكية المستخدمة بشكل دقيق. كما ينبغي أن تستخدم آلية المصادقة لمنع الدخول غير المصرح به إلى الشبكة. كما يجب اختبار طريقة واحدة للمصادقة ومراعاة التالي:

- إلى أي مدى تعتبر آلية المصادقة آمنة لاستخدامه؟
- ماهي تكلفة آلية المصادقة التي سيتم استخدامها ؟

أ-التشفير

يجب أن يتم فحص آليات التشفير لكافة الأجهزة اللاسلكية المستخدمة بشكل دقيق. كما ينبغي أن تستخدم آلية التشفير لحماية البيانات اثناء انتقالها في الهواء. كما يجب مراعاة التالي:

- إلى أي مدى تعتبر آلية التشفير آمنة لاستخدامه؟
- ماهي مدى حساسية البيانات التي تنتقل عبر الجهاز اللاسلكي؟
- ماهي تكلفة آلية التشفير التي سيتم استخدامها ؟

ب- إعدادات الضبط

يجب أن يتم ضبط إعدادات جهاز SSID اللاسلكي بطريقة معينة بحيث لا تحتوي أو تشير إلى أي معلومات عن الجامعة أو أقسامها، أو موظفيها بما في ذلك اسم الجامعة، أواسم القسم، أو اسم الموظف أو رقم هاتف الموظفين وعناوين البريد الإلكتروني، أو معرفات المنتج.

ج- نقاط الدخول

يجب تسجيل واعتماد جميع نقاط الدخول اللاسلكية والأجهزة اللاسلكية المتصلة بشبكة الجامعة من قبل ممثل في قسم تقنية المعلومات. جميع الأجهزة اللاسلكية خاضعة لعمليات مراجعة الحسابات واختبارات الإختراق من قبل تقنية المعلومات دون إشعار.

إن أعلى سلطة لشخص في عمادة تقنية المعلومات لديه السلطة النهائية بخصوص إدارة وأمن الأجهزة اللاسلكية والشبكات اللاسلكية. هذا الشخص له الحق في تفويض من يراه مناسبا ويكون مسؤولا عن تشغيل الشبكة.

٥. فصل الشبكة:

تتطلب هذه السياسة فصل أجزاء من الشبكة التي تحتوي وتدعم أجهزة لاسلكية بشكل مباشر (الشبكة اللاسلكية) عن جزء من الشبكة التي لا تدعم الاتصالات اللاسلكية. وسيعتبر الجزء الذي يدعم الأجهزة أو الاتصالات اللاسلكية أقل وثوقا من الجزء الآخر. سيتم فصل كل خوادم الملفات والمجال الداخلي المتحكم بالخوادم من الشبكة اللاسلكية عن طريق استخدام جدار الحماية. وسوف يتم وضع جهاز كاشف للاختراقات أو أكثر لمراقبة الشبكة اللاسلكية لأي حالة اختراق وتسجيل الاحداث . وسيتم تحديد نوع الأحداث المسجلة من قبل مسؤول الشبكة.

٦. الاستخدامات المسموح بها في الشبكة اللاسلكية :

- يسمح فقط باستخدام الأجهزة اللاسلكية المعتمدة.
- يجب فحص إعدادات جميع الأجهزة اللاسلكية من قبل قسم تقنية المعلومات قبل أن يتم وضعها للاستخدام.
- يجب فحص إعدادات أو مشاكل التحميل لجميع الأجهزة اللاسلكية المستخدمة بشكل شهري.

٧. تطبيق القانون:

بما أن الاستخدام غير السليم لتقنية اللاسلكية والاتصالات اللاسلكية قد يعرض الشبكة لكثير من الهجمات والاختراقات، لذلك فإن الاستخدام السليم والمرخص له لتقنية اللاسلكية يعتبر أمر مهم لأمن الجامعة وجميع منسوبيها. إن الموظفين الذين لا يلتزمون بهذه السياسة قد يتعرضون لإجراءات تأديبية قد تصل في بعض الاحيان إلى الفصل.

سياسة الدعم الفني

١. نظرة عامة:
تحتوي هذه السياسة على آلية صيانة الأجهزة المكتبية والمحمولة، ومعامل الحاسب الآلي بالجامعة. وتثبيت برامج التشغيل. وذلك تحت إجراءات وآليات متبعة بقسم الدعم الفني – بعمادة تقنية المعلومات

٢. الهدف:
إن الهدف من هذه السياسة هو وضع معايير واشتراطات لتقديم كافة خدمات الدعم الفني لمنسوبي الجامعة .

٣. النطاق:
تشمل هذه السياسة أي أجهزة مكتبية أو محمولة تكون خاصة بأعضاء هيئة التدريس والموظفين والطلاب داخل الجامعة.

٤. السياسات:
١ - سياسة طلب الدعم الفني:
-يتم طلب الدعم الفني عبر تقديم طلب إلكتروني من خلال الخدمات الإلكترونية. – الدعم الفني.
-يجب أن يكون الطلب المرسل يخص مقدم الطلب والجهاز نفسه، ولا يمكن أن تتم خدمة أكثر من جهاز عبر طلب واحد إلا في حالة صيانة المعامل فقط.
-لا يمكن استقبال أي جهاز في مقر وحدة الدعم الفني بعمادة تقنية المعلومات إلا بعد الاتصال به من قبل موظفي وحدة الدعم الفني.

٢ - سياسة مدة صيانة الأجهزة:
- يتم تقدير مدة صيانة الأجهزة من قبل وحدة الدعم الفني على ألا تتجاوز مدة الصيانة ٣ أيام عمل.
- في حالة حاجة الجهاز لمدة صيانة أكثر يتم إبلاغ مقدم الطلب بذلك أثناء فترة الفحص والصيانة.
- لا تتحمل وحدات الدعم الفني أي مسؤولية تجاه الأجهزة التي يتأخر صاحب الطلب في استلامها لمدة تتجاوز أسبوع واحد.

٣- سياسة صيانة الأجهزة:
- يجب على صاحب الطلب أخذ نسخة من كافة ملفاته قبل إحضار الجهاز للصيانة.
- وحدات الدعم الفني غير مسؤولة عن أي بيانات أو معلومات لم يتم إبلاغ موظفي الصيانة بضرورة المحافظة عليها قبل البدء في عملية صيانة الجهاز.
- أي جهاز يتم تسليمه لوحدات الدعم الفني سيتم ربطه بالمجال الجامعي دون الرجوع لصاحب الطلب.
-يتم تنزيل البرامج الأساسية فقط والتي يتم تحديدها من قبل وحدة الدعم الفني، وتخضع البرامج والتطبيقات الأخرى لطلبات خاصة يتم النظر فيها في حينها.
- لوحدة الدعم الفني الحق في قبول أو رفض أي طلب تبديل جهاز وذلك وفق التقارير الفنية الخاصة بالجهاز.
- لا يتم عمل أي أعمال فنية (صيانة، فورمات، تحديث، تثبيت برامج) لأي جهاز شخصي ليس ملكاً للجامعة.

٤ - صيانة المعامل:
- يتم طلب صيانة أجهزة المعامل عن طريق نظام الاتصالات الإدارية (إرسال خطاب يتضمن طلب الصيانة).
- يتطلب لصيانة أجهزة المعامل رفع طلب صيانة قبل أسبوعين كحد أدنى من تاريخ الصيانة المطلوب.
- يجب على كل جهة تحديد منسق للجهة في خطاب طلب الصيانة وذلك ليتم التواصل معه من قبل فريق الدعم الفني.

٥. إخلاء مسؤولية:
تبذل عمادة تقنية المعلومات أقصى جهودها لتحقيق مستوى عالي من الجودة والدقة في الدعم الفني، إلا أنها لا تتحمل أي مسئولية أو تبيعات قد تنتج إثر مخالفة السياسات المبيّنة أعلاه.

٦-تطبيق القانون:
في حال انتهاك هذه السياسة من قبل أي مستخدم مصرح له، فإنه يعتبر غير مصرح له ويخضع لإجراءات تأديبية وفقاً لبند تطبيق القانون الموجود في سياسة الاستخدام الغير مصرح له.

سياسة الاستخدام للاتصال الصوتي والمرئي

١. نظرة عامة:
تحتوي هذه السياسة على آلية صرف الهواتف الشبكية وتفعيل الخدمات، وذلك تحت إجراءات وآليات متبعة بقسم الاتصال الصوتي والمرئي-بعمادة تقنية المعلومات-

٢. الهدف:
إن الهدف من هذه السياسة هو وضع معايير واشتراطات لصرف واستخدام أجهزة الاتصال وذلك لتنظيم العمل.

٣. النطاق:
تشمل هذه السياسة أي أجهزة اتصال بالشبكة داخل الجامعة كالهواتف وأجهزة الفيديو كونفرنس وكذلك أجهزة الفاكس.

٤. السياسات:
-الهاتف الشبكي:

١- سياسة طلب هاتف شبكي: يتم طلب هاتف شبكي عن طريق تعبئة نموذج طلب هاتف من خلال بوابة الخدمات الالكترونية، علماً أنه لا يتم صرف جهازين لموظف واحد إلا في حالة كونه يشغل منصبين وفي مكانين مختلفين.

٢- سياسة نقل عهدة الهاتف الشبكي: يتم نقل العهدة من موظف لآخر وذلك عبر تعبئة نموذج نقل عهدة هاتف شبكي من بوابة الخدمات الالكترونية وفي حال تلف أو فقدان للعهدة فإنه يتم التعامل معها حسب ما يقتضيه النظام.

٣- سياسة الحصول على خدمة الصفر: يتم تفعيل الصفر الداخلي والخارجي لوكلاء الجامعة والعمداء ومستشارين معالي مدير الجامعة ومدراء الإدارات العامة المرتبطة بمعالي مدير الجامعة، ويتم تفعيل الصفر الداخلي لوكلاء العمداء ومدراء مكاتب وكلاء الجامعة ومدراء إدارات الشؤون الإدارية والمالية ومدراء مكاتب العمداء، وكذلك الحالات المستثناة التي على تواصل دائم مع جهات خارج الجامعة.

٤- سياسة صرف التحويلات والأرقام المميزة: تم تحديد نطاق لكل إدارة وكل إدارة يتم الصرف لها بناء على النطاق المحدد لها ويتم صرف الأرقام المميزة لأصحاب المناصب كالعمداء والوكلاء ومدراء العموم علماً أن الأرقام المميزة تبقى للمنصب.

-الفاكس الإلكتروني:

يتم طلب خدمة الفاكس الالكتروني عبر مخاطبة عمادة تقنية المعلومات موضحاً فيه الحاجة لخدمة الفاكس الالكتروني. وكل إدارة يتم الصرف لها بناء على النطاق المحدد لها ويتم صرف الأرقام المميزة لأصحاب المناصب كالعمداء والوكلاء ومدراء العموم علماً أن الأرقام المميزة تبقى للمنصب.

٥. الفيديو كونفرنس:
هي خدمة تتيح التواصل الصوتي والمرئي بين جهتين أو أكثر داخل الجامعة أو خارجها ولطلب جهاز الفيديو كونفرنس عبر مخاطبة عمادة تقنية المعلومات .وعليه يتم تسجيل عهدة الفيديو كونفرنس على مسؤول الجهة الطالبة للجهاز (كلية ، عمادة ، إدارة)وتنتقل العهدة للمسؤول التالي في حال انتقال أو اعفاء المسؤول الأول من منصبه وفي حال فقدان أو تلف جهاز الفيديو كونفرنس بسبب سوء الاستخدام فإنه يتعامل مع هذه الحالات حسب ما يقتضيه النظام، كذلك يوجد لدى قسم الاتصال الصوتي والمرئي خدمة نقل فعالية من جهة لباقي الجهات ولطلب نقل الفعالية

يجب مراعات الآتي :

١- يتم تعبئة نموذج طلب نقل فعالية عبر الخدمات الالكترونية وذلك قبل موعد الفعالية بأربع أيام.

٢- اشعار الجهات المطلوب نقل الفعالية لها من اختصاص الجهة الطالبة لنقل الفعالية وليس من اختصاص عمادة تقنية المعلومات.

٣- لابد من تعيين منسقين للجهات المطلوب لنقل الفعالية لها حتى يتم التواصل معهم قبل موعد نقل الفعالية بيوم أو يومين، للتأكد من جودة الصوت والصورة في الجهات الأخرى.

٦- تطبيق القانون:
في حال انتهاك هذه السياسة من قبل أي مستخدم مصرح له، فإنه يعتبر غير مصرح له ويخضع لإجراءات تأديبية وفقاً لبند تطبيق القانون الموجود في سياسة الاستخدام الغير مصرح له.

سياسة الدخول عن بعد

١. نظرة عامة:
تحدد هذه السياسة المعايير اللازمة للاتصال بشبكة الجامعة والمعايير الأمنية لأجهزة الكمبيوتر التي يسمح لها بالاتصال بشبكة الجامعة.
وتحدد أيضا الطريقة التي يمكن من خلالها للمستخدمين عن بعد الاتصال بالشبكة الرئيسية للجامعة ومتطلبات الأنظمة قبل أن يتم السماح لهم بالاتصال. بالإضافة، تعرّف هذه السياسات والإجراءات الطرق التي يجب على المستخدمين اتباعها للاتصال عن بعد عبر الانترنت بشبكة الجامعة الداخلية (Intranet).

٢. الهدف:
إن الغرض من هذه السياسة هو منع وصول الضرر إلى شبكة الجامعة بالإضافة إلى منع فقدان البيانات.

٣. الموافقة:
يشترط للوصول إلى موارد الجامعة وشبكتها الداخلية عن بعد (عبر الانترنت) الاتصال بالشبكة الخاصة الظاهرية (Virtual Private Network - VPN) الخاصة بالجامعة. وهي تقنية لبناء اتصال خاص بين شبكة الجامعة و جهاز المستخدم عبر الانترنت يمكن من خلالها الوصول للموارد الداخلية للشبكة.
للحصول على حساب VPN من الجامعة, يجب توفر ما يلي:

١. يجب أن يكون المستخدم أحد الفنيين المصرح لهم بإدارة موارد ضمن شبكة الجامعة الداخلية, سواءً كان المستخدم موظف رسمي بالجامعة أو يتبع لطرف ثالث أو شركة لديها عقد مع الجامعة. يمكن منح الوصول لغير فني في حالات استثنائية تتم مراجعتها من قبل عمادة تقنية المعلومات وإدارة أمن المعلومات.

٢. يجب تقديم طلب تفعيل حساب VPN في نظام إدارة أمن المعلومات الإلكتروني ليتم مراجعته واعتماده من قبل إدارة أمن المعلومات.

٣. يجب أن تكون إعدادات الضبط لحسابات جميع الموظفين تمنع أي دخول عن بعد بشكل إفتراضي. وعليه لا يسمح بتغييرهذه الإعدادات للسماح بالدخول عن بعد دون الرجوع وأخذ موافقة إدارة أمن المعلومات.

٤. متطلبات جهاز الحاسب عن بعد:
١. يجب أن يملك المستخدم حساب VPN فعال ومعتمد للاتصال عن بعد بشبكة الجامعة الداخلية.

٢. يجب استخدام برنامج Forticlient الخاص بالجامعة لإجراء اتصال VPN.

٣. يجب التأكد من حصول برنامج Forticlient على آخر التحديثات لمكتبة مكافحة الفيروسات ومكتبة الثغرات الأمنية.

٤. في حال قام البرنامج بالتنبيه حول ثغرة ما أو ملف ضار في الجهاز, ينبغي إجراء مسح وتنظيف الجهاز من الملفات الضارة قبل معاودة الاتصال.

٥. متطلبات الاتصال عن بعد:
١. يجب على المستخدم للوصول إلى موارد الجامعة الداخلية بإستخدام الإتصال الآمن SSL-VPN وذلك من أجل إجراء قناة إتصال آمنة ضد هجمات التنصت ونحوها.

٢. يجب عدم استخدام حساب اتصال VPN لمستخدم آخر في الجامعة, وعليه يجب اتباع إجراءات تفعيل حساب VPN للحصول على حساب خاص.

٣. يجب عدم استخدام حساب اتصال VPN للوصول إلى موارد في الجامعة غير مصرح للمستخدم بإدارتها.

٦-المراقبة:
تتم مراقبة عمليات الاتصال التي يتم إجراءها عبر ال VPN مثل عمليات الدخول والخروج للموارد الداخلية, ويتم من خلالها التدقيق والتأكد من إمتثال هذه العمليات للإجراءات المنصوص عليها في هذه الوثيقة.

٦-مخالفة السياسات الإساءة استخدام::
تتضمن مخالفة السياسة, ولا تنحصر, بما يلي:
١. الوصول لموارد داخلية غير مصرح للفرد بها.
٢. الوصول لموارد داخلية من خلال حساب غير مصرح للفرد به.
٣. السماح لفرد بالوصول لموارد داخلية غير مصرح له بها.
٤. الوصول لموارد داخلية من خلال جهاز كمبيوتر لا يحقق متطلبات الأمان.

٦-تطبيق القانون:
في حال انتهاك هذه السياسة من قبل أي مستخدم مصرح له، فإنه يعتبر غير مصرح له ويخضع لإجراءات تأديبية وفقاً لبند تطبيق القانون الموجود في سياسة الاستخدام الغير مصرح له.

سياسة الدعم الفني بالإدارة النسائية

نظرة عامة:
تحتوي هذه السياسة على آلية تقديم الدعم الفني بالأقسام النسائية بجامعة المجمعة. من صيانة الأجهزة المكتبية والمحمولة، ومعامل الحاسب الآلي بالجامعة. وتثبيت برامج التشغيل وحل مشاكل البريد الالكتروني والهاتف الشبكي، وجميع الخدمات الالكترونية المقدمة من قبل عمادة تقنية المعلومات وذلك تحت إجراءات وآليات متبعة بالإدارة النسائية.

١. الهدف:
إن الهدف من هذه السياسة هو وضع معايير واشتراطات لتقديم خدمات الدعم الفني لكافة منسوبات الجامعة.

٢. النطاق:
تشمل هذه السياسة أي أجهزة مكتبية أو محمولة او بريد الكتروني او هاتف شبكي يكون خاص بأعضاء هيئة التدريس والموظفات والطالبات داخل الجامعة.

٣. متطلبات جهاز الحاسب عن بعد:
١. يجب أن يملك المستخدم حساب VPN فعال ومعتمد للاتصال عن بعد بشبكة الجامعة الداخلية.

٢. يجب استخدام برنامج Forticlient الخاص بالجامعة لإجراء اتصال VPN.

٣. يجب التأكد من حصول برنامج Forticlient على آخر التحديثات لمكتبة مكافحة الفيروسات ومكتبة الثغرات الأمنية.

٤. في حال قام البرنامج بالتنبيه حول ثغرة ما أو ملف ضار في الجهاز, ينبغي إجراء مسح وتنظيف الجهاز من الملفات الضارة قبل معاودة الاتصال.

٤. السياسات:
أ- سياسة طلب الدعم الفني:
- يتم طلب الدعم الفني عبر تقديم طلب إلكتروني من خلال بوابة الدعم الفني الإلكترونية.
- يجب أن يكون الطلب المرسل يخص مقدم الطلب والجهاز نفسه، ولا يمكن أن تتم خدمة أكثر من جهاز عبر طلب واحد إلا في حالة صيانة المعامل فقط.
- لا يمكن استقبال أي جهاز في مقر وحدة الدعم الفني بعمادة تقنية المعلومات إلا بعد التنسيق من قبل موظفي وحدة الدعم الفني.

ب- سياسة مدة صيانة الأجهزة:
- يتم تقدير مدة صيانة الأجهزة من قبل وحدة الدعم الفني على ألا تتجاوز مدة الصيانة ٣ أيام عمل.
- في حالة حاجة الجهاز لمدة صيانة أكثر يتم إبلاغ مقدم الطلب بذلك أثناء فترة الفحص والصيانة.
- لا تتحمل وحدات الدعم الفني أي مسؤولية تجاه الأجهزة التي يتأخر صاحب الطلب في استلامها لمدة تتجاوز أسبوع واحد.

ج- سياسة صيانة الأجهزة:
- يجب على صاحب الطلب أخذ نسخة من كافة ملفاته قبل إحضار الجهاز للصيانة.
- وحدات الدعم الفني غير مسؤولة عن أي بيانات أو معلومات لم يتم إبلاغ موظفات الصيانة بضرورة المحافظة عليها قبل البدء في عملية صيانة الجهاز.
- أي جهاز يتم تسليمه لوحدات الدعم الفني سيتم ربطه بالدومين الجامعي بشكل مباشر دون الرجوع لصاحب الطلب.
- يتم تنزيل البرامج الأساسية فقط والتي يتم تحديدها من قبل وحدة الدعم الفني، وتخضع البرامج والتطبيقات الأخرى لطلبات خاصة يتم النظر فيها في حينها.
- لوحدة الدعم الفني الحق في قبول أو رفض أي طلب تبديل جهاز وذلك وفق التقارير الفنية الخاصة بالجهاز.
- لا يتم عمل أي أعمال فنية (صيانة، فورمات، تحديث، تثبيت برامج) لأي جهاز شخصي ليس ملكاً للجامعة.

د- صيانة المعامل:
- يتم طلب صيانة أجهزة المعامل عن طريق نظام الاتصالات الإدارية (إرسال خطاب يتضمن طلب الصيانة).
- يتطلب لصيانة أجهزة المعامل رفع طلب صيانة قبل أسبوعين كحد أدنى من تاريخ الصيانة المطلوب.
- يجب على كل جهة تحديد منسق للجهة في خطاب طلب الصيانة وذلك ليتم التواصل معه من قبل فريق الدعم الفني.

ه- تقديم الدعم الفني للبريد الالكتروني:
- يتم تقديم طلب الدعم للبريد الالكتروني في حال تعذر انشاءه او الارسال او الاستقبال من خلاله او تعذر استعادة كلمة المرور.
- يتم عمل اللازم والرفع لقسم البيانات لحل المشكلة وإبلاغ المستخدم بذلك.

ل- تقديم الدعم الفني للهاتف الشبكي:
- في حالة وجود مشكلة في طلب الهاتف الشبكي يتم التواصل مع الادارة النسائية عن طريق نظام الدعم الفني وشرح المشكلة.
- يتم تحويل المشكلة للقسم المختص في الهاتف الشبكي
- يتم عمل اللازم وحل المشكلة وإبلاغ المستفيد بذلك

م- تقديم الدعم الفني لنقاط الانترنت :
- في حال تعطل نقطة الانترنت او في حالة الاحتياج لنقاط انترنت اضافية يتم الرفع بها من قبل المستفيد عبر نظام الدعم الفني.
- يتم تحديد مكان العطل او الاحتياج بشكل واضح في الطلب مع توضيح المكان وترميزه والحاجة منه
- يتم فحص النقطة والتأكد من تعطلها او احتياج المكان لذلك
- يتم الرفع بها لقسم الشبكات لإتمام اللازم وإبلاغ المستفيد.

٥. إخلاء مسؤولية:
تبذل عمادة تقنية المعلومات أقصى جهودها لتحقيق مستوى عالي من الجودة والدقة في الدعم الفني، إلا أنها لا تتحمل أي مسئولية أو تبيعات قد تنتج إثر مخالفة السياسات المبيّنة أعلاه.

٦. تطبيق القانون:
في حال انتهاك هذه السياسة من قبل أي مستخدم مصرح له، فإنه يعتبر غير مصرح له ويخضع لإجراءات تأديبية وفقاً لبند تطبيق القانون الموجود في سياسة الاستخدام الغير مصرح له.

سياسة خدمة المستفيدين

١. نظرة عامة:
تهتم عمادة تقنية المعلومات بجامعة المجمعة بالعناية بالمستفيدين من خدماتها من منسوبي الجامعة (أعضاء هيئة التدريس – الموظفين – الطلاب) وكذلك الجهات الخارجية. ويعمل قسم العناية بالمستفيدين ليكون حلقة الوصل بين منسوبي الجامعة وعمادة تقنية المعلومات عبر تخصيصها الرقم الداخلي (٥٥٥٥)، لإيجاد الحلول للمشكلات والاستفسارات وتحويلها على الجهة المختصة ومتابعة الطلب الى ان يتم انتهائه. وقياس رضى المستفيد.

٢. الهدف:
تهدف هذه السياسة لتقديم خدمات متميز للمستفيدين من خدمات العمادة من منسوبي الجامعة (أعضاء هيئة التدريس – الموظفين – الطلاب) وكذلك الجهات الخارجية. بكل اتقان وسرعة وذلك لإنجاز معاملاتهم ومتابعة طلباتهم والحرص على مواصلة التطوير في العمل وقياس رضاء المستفيدين بعد حل مشاكلهم.

٣. النطاق:
تنطبق هذه السياسة جميع منسوبي جامعة المجمعة الجامعة (أعضاء هيئة التدريس – الموظفين – الطلاب) وكذلك الجهات الخارجية.

٤. السياسات:
سياسة طلب دعم فني:

يتم طلب دعم فني عن طريق تعبئة نموذج طلب دعم فني من خلال بوابة الخدمات الالكترونية، وتظهر نافذة لتعبئة البيانات المهمة كالاسم – الموضوع – تفاصيل الطلب ويتم تحويل الطلب للجهات ذات العلاقة، في حال انتهاء الطلب يتم الاتصال بالمستفيد لقياس رضاه عن الخدمات المقدمة.

علماً أنه لا يتم صرف جهازين لموظف واحد إلا في

سياسة استقبال المكالمات عبر التحويلة (٥٥٥٥):

تم تخصيص التحويلة الداخلية (٥٥٥٥) لاستقبال المكالمات الواردة للعمادة من الساعة ٧,٣٠ صباحاً حتى الساعة ٢,٣٠ ظهراً، ويقدم قسم العناية بالمستفيدين كافة الدعم لضمان حل المشكلة والرد على الاستفسارات والشكاوى وتقييم رضى المستفيد.

٦- تطبيق القانون:
في حالة انتهاك هذه السياسة من قبل أي مستخدم مرخص له، فإنه يعتبر غير مرخص له ويخضع لإجراءات تأديبية وفقا لبند تطبيق القانون الموجود في سياسة الاستخدام الغير مرخص به.

سياسة الاستخدام الغير مصرح به

١. الهدف:
إن الهدف من هذه السياسة هو تحديد سياسة الجامعة بشأن الاستخدام الغير مصرح به لشبكة تقنية المعلومات بجامعة المجمعة.

٢. النطاق:
تغطي هذه السياسة جميع أنواع الاستخدام الغير مصرح به لشبكة تقنية المعلومات، سواء من قبل شخص غير مصرح له أو حتى من قبل مستخدم مرخص له ولكنه مخالف لقوانين الجامعة. لذلك فمصطلح « مستخدم غير مصرح له» يرمز إلى كلا المستخدمين.

٣. السياسة:
يمنع جميع المستخدمين الغير نظاميين من استخدام شبكة تقنية المعلومات لجامعة المجمعة لأي غرض كان. كما يمنع جميع المستخدمين النظاميين من استخدام شبكة تقنية المعلومات في أمور تتجاوز صلاحية استخدامهم.

٤. تطبيق القانون:
أي مستخدم غير مصرح له قد يتعرض لمحاكمة جنائية و / أو دعاوى مدنية يحق من خلالها لجامعة المجمعة أن تطالب فيها بتعويضات قانونية. وأي موظف من جامعة المجمعة قد يخضع لإجراءات تأديبية في حال مخالفته للأنظمة وقد تصل العقوبة إلى إنهاء خدماته.