سياسة أمن الشبكة والبنية التحتية

١,٠ الغرض :

لا يقصد بنوايا نشر سياسة البنية التحتية بشبكة الجامعة فرض قيود تتعارض مع النزاهة والثقة والانفتاح الثقافي للعمادة. تلتزم الجامعة بحماية موظفيها والشركاء ومن الأعمال غير المشروعة أو الضارة من قبل الأفراد سواًء عن علم أو عن جهل.

تعد الأنظمة ذات الصلة بالإنترانت/الإنترنت بما في ذلك على سبيل المثال وليس الحصر أجهزة الحاسوب والبرامج وأنظمة التشغيل ووسائط التخزين وحسابات الشبكات وتوفير البريد الإلكتروني، وتصفح الانترنت، جميعها ملك للجامعة. تستخدم هذه النظم في خدمة أغراض العمل لصالح الجامعة وعملائنا في أثناء العمليات العادية. يرجى مراجعة سياسات الموارد البشرية لمزيد من التفاصيل.

يعد الأمن الفعال جهد جماعي ينطوي على مشاركة ودعم كل موظف بالجامعة والأقسام التابعة لها. من مسؤولية كل مستخدم للحاسوب معرفة هذه المبادئ التوجيهية والقيام بالأنشطة وفقا لذلك.

يتمثل الغرض من هذه السياسة في تحديد الاستخدام المقبول لأجهزة الحاسوب بالجامعة حيث تحمي هذه القواعد الموظفين و الجامعة من الاستخدام غير اللائق الذي يعرض العمادة للمخاطر بما في ذلك هجمات الفيروسات وتعريض أنظمة الشبكات وخدماتها والمسائل القانونية للخطر.
كذلك تحديد المسؤوليات الخاصة بالاستخدام الأمثل للمعلومات.

٢,٠ النطاق :

تنطبق هذه السياسة على الموظفين والمقاولين والاستشاريين المؤقتين وغيرهم من العاملين في عمادة تقنية المعلومات والإتصالات ، بما في ذلك جميع الموظفين التابعين للأطراف الخارجية. تنطبق هذه السياسة على جميع المعدات التي تملكها أو تستأجرها الجامعة.

٣,٠ الأهداف :

تتمثل أهداف برنامج أمن المعلومات في ضمان سلامة البيانات وتوافرها وسريتها، بما يكفي من الدقة والوقت المناسب لتلبية احتياجات العمادة من دون التضحية بالمبادئ الأساسية المبينة في بيان السياسة.

وفيما يلي الأهداف على وجه التحديد:

- التأكد من أن بيئة الشبكة المحلية لديها أمان يتناسب مع الحساسية والحرجية وما إلى ذلك.
- ضمان أن يكون الأمن فعالا من حيث التكلفة على أساس نسبة التكلفة مقابل المخاطر.
- ضمان توفير الدعم المناسب لأمن البيانات في كل مجال وظيفي.
- ضمان المساءلة الفردية عن البيانات والمعلومات والموارد الحاسوبية الأخرى التي يمكن للأفراد الوصول إليها.
- ضمان قابلية التدقيق لبيئة الشبكة المحلية.
- ضمان توفير التوجيه الكافي للموظفين من اجل الإطلاع على مسؤوليات تتعلق بأمن المعلومات الآلي.
- التأكد من أن جميع الوظائف الحاسمة للشبكة المحلية لديها خطط طوارئ مناسبة لتوفير استمرارية التشغيل.
- التأكد من أن جميع السياسات التنظيمية المعمول بها. يتم تطبيقها والالتزام بها.

٤,٠ السياسة :

المجموعات التالية مسؤولة عن تنفيذ وصون الأهداف الأمنية المنصوص عليها في هذه السياسة. يتم عرض مسؤوليات مفصلة في المسؤوليات لضمان أمن الشبكات المحلية.
١. المدراء : هم الذين لديهم برنامج أو مسؤولية وظيفية (ليس في مجال أمن الكمبيوتر) ضمن الجامعة هم المسؤولون عن إعلام الموظفين عن هذه السياسة، والتأكد من أن كل شخص لديه نسخة، والتفاعل مع كل موظف في القضايا الأمنية.
٢. شعبة إدارة الشبكة المحلية : هم الموظفين الذين يشاركون في الإدارة اليومية وعمليات شبكة الجامعة. وهي مسؤولة عن ضمان استمرار تشغيل الشبكة المحلية. و هي المسؤولة عن تنفيذ إجراءات أمن الشبكة المحلية المناسبة إمتثالاً لسياسة أمن المعلومات .
٣. مسؤولو قواعد البيانات : هم الموظفين المسؤولين عن ضمان حصول المستخدمين النهائيين على موارد الشبكة المحلية المطلوبة الموجودة على خوادمهم. وعن قواعد البيانات وضمان أن أمن خوادمهم الخاصة يتماشى مع سياسة أمن المعلومات بالجامعة.
٤. المستخدمين النهائيين : هم الموظفون اللذين لديهم حق الوصول إلى شبكة الجامعة وهم مسؤولون عن استخدام الشبكة المحلية وفقا لسياسة أمن المعلومات. وجميع مستخدمي البيانات مسؤولون عن الامتثال لسياسة أمن المعلومات ، وإبلاغ الإدارة عن أي مخالفة مشتبه فيها.

٥,٠ التطبيق :
في حالة انتهاك الموظف لهذه السياسة ، فإن ذلك يعرضه لإجراءات تأديبية صارمة.

٦,٠ السياسة :

٦,١. يجب أن يكون لكل جهاز كمبيوتر شخصي "مالك" أو "مدير نظام" يكون مسؤولا عن صيانه وامنه، واتباع جميع السياسات والإجراءات المرتبطة باستخدام الكمبيوتر. قد يقوم المستخدم الأساسي للكمبيوتر بملء هذا الدور. وينبغي تدريب هؤلاء المستخدمين وتوجيههم حتى يتمكنوا من متابعة جميع السياسات والإجراءات بصورة كافية.
٦,٢. من أجل منع الوصول غير المصرح به إلى البيانات والبرمجيات والموارد الأخرى الموجودة على الخوادم يجب أن تكون جميع آليات الأمن المعلوماتي تحت سيطرة حصرية من المسؤول المحلي والأفراد المعنيين من عمادة تقنية المعلومات والإتصالات.
٦,٣. من أجل منع انتشار البرامج الضارة والمساعدة في تنفيذ اتفاقيات ترخيص البرامج، يجب على المستخدمين التأكد من أن برامجهم مرخصة بشكل صحيح وآمنة.
٦,٤. ستكون جميع التغييرات البرمجية والنسخ الاحتياطية على الخوادم من مسؤولية عمادة تقنية المعلومات والإتصالات.
٦,٥. يجب تعيين إسم مستخدم وكلمة مرور لكل مستخدم ضمن الشبكة على ان لا يتم الاستخدام إلا بعد الانتهاء واكتمال الوثائق المناسبة. يجب على المستخدمين عدم مشاركة اسم المستخدم او كلمة المرور مع الاخرين .
٦,٦. يجب مصادقة المستخدمين على الشبكة المحلية قبل الوصول إلى موارد الشبكة المحلية.
٦,٧. يجب تعطيل اسم المستخم بعد فترة ٩٠ يوم من عدم الاستخدام.
٦,٨. يجب أن يكون استخدام أجهزة الشبكة المحلية مرخصا ومراقب من قبل عمادة تقنية المعلومات والإتصالات.
٦,٩. يجب على الموظفين المسؤولين عن إدارة عمليات واستخدام عمادة تقنية المعلومات والإتصالات تلقي التدريب على الوعي الأمني بالكمبيوتر وممارسات الكمبيوتر المقبولة. وينبغي تنفيذ التدريب على أمن الحاسوب في برامج التدريب القائمة مثل البرامج التوجيهية للموظفين الجدد، والدورات التدريبية التي تشارك في معدات نظم تكنولوجيا المعلومات وحزم البرمجيات.
٦,١٠. ويجب إعداد تقارير الأمن ومراجعتها على أساس يومي.

٧,٠ مسؤوليات محددة لضمان أمن الشبكات المحلية :

٧,١. المستخدمين

يتوقع من المستخدمين أن يكونوا على دراية والتزام بالسياسات الأمنية الخاصة بالجامعة ، والقوانين والسياسات والإجراءات الأخرى المعمول بها. المستخدمين هم المسؤولون في نهاية المطاف عن سلوكهم. وعلى وجه التحديد، يتحمل المستخدم مسؤولية ما يلي:

١. مسؤول عن فهم واحترام القوانين ذات الصلة، سياسات وإجراءات الإدارة وسياسات وإجراءات الجامعة ، وغيرها من السياسات الأمنية المطبقة والممارسات المرتبطة بها لعمادة تقنية المعلومات والإتصالات.
٢. مسؤول عن توظيف آليات الأمن المتاحة لحماية سرية وسلامة المعلومات الخاصة بهم
٣. اتباع إجراءات الموقع لأمن البيانات الحساسة.
٤. استخدام آليات حماية الملفات للحفاظ على التحكم في الوصول إلى الملفات المناسبة.
٥. إنشاء كلمات مرور قوية . الحصول على إرشادات بشأن اختيار كلمة مرور جيدة. لا تكتب كلمات المرور بأسفل الشاشة، أو تكشف عنها للآخرين. لا تشارك حساباتك مع الاخرين.
٦. مسؤول عن تقديم المشورة إلى الآخرين الذين لا يستخدمون بشكل مناسب آليات الأمن المتاحة. المساعدة في حماية ممتلكات الأفراد الآخرين. إخطارها بالموارد (مثل الملفات والحسابات) التي لم يتم حمايتها.
٧. مسؤول عن إخطار المسؤول أو الإدارة إذا كان قد لوحظ مخالفة أمنية أو فشل أو الكشف عنها.
٨. مسؤول عن عدم استغلال نقاط ضعف النظام.
a. لا تقم بتعديل المعلومات أو تدميرها أو قراءتها أو نقلها عمدا بطريقة غير مصرح بها. لا تسمح لغير المخولين بالوصول إلى موارد الشبكة المحلية والمعلومات أو استخدامها.
b. قدم معلومات الهوية والمصادقة الصحيحة عند الطلب ولا تحاول افتراض او معرفة هوية طرف آخر.
٩. مسؤول عن ضمان أن يتم إجراء النسخ الاحتياطية للبيانات والبرمجيات على محرك الأقراص الثابتة الخاصة بمحطة العمل الخاصة بهم.
١٠. مسؤول عن معرفة كيفية عمل البرمجيات الخبيثة، والأساليب التي يتم إدخالها ونشرها، ومواطن الضعف التي يتم استغلالها من قبل البرامج الضارة والمستخدمين غير المصرح لهم.
١١. مسؤول عن معرفة واستخدام السياسات والإجراءات المناسبة لمنع واكتشاف وإزالة البرامج الضارة.
١٢. مسؤول عن معرفة كيفية مراقبة أنظمة محددة والبرمجيات للكشف عن علامات النشاط غير الطبيعي .
١٣. مسؤول عن استخدام الضوابط الفنية التي أتيحت لحماية النظم من البرامج الضارة.
١٤. مسؤول عن معرفة واستخدام إجراءات الطوارئ لاحتواء والتعافي من الحوادث المحتملة.

٧,٢ المدراء الوظيفيون

المدراء الوظيفيون (والإدارة العليا) مسؤولين عن وضع وتنفيذ سياسات أمنية فعالة تعكس أهدافا محددة للجامعة. وهم مسؤولون في نهاية المطاف عن ضمان أن يكون أمن المعلومات والإتصالات قد تحقق، ولا يزال، هدفا بارزا في العمليات اليومية. والمدراء على وجه التحديد مسؤولون عما يلي:

١. عن تنفيذ إدارة فعالة للمخاطر من أجل توفير أساس لصياغة سياسة ذات مغزى. وتتطلب إدارة المخاطر تحديد الأصول التي يتعين حمايتها، وتقييم أوجه الضعف، وتحليل مخاطر الاستغلال، وتنفيذ ضمانات فعالة من حيث التكلفة.
٢. ضمان حصول كل مستخدم، كحد أدنى، على نسخة من سياسة الأمن وكتيب الموقع (إن وجد) قبل إنشاء حساب للمستخدم.
٣. تنفيذ برنامج التوعية الأمنية للمستخدمين لضمان معرفة سياسة أمن الموقع والممارسات المتوقعة.
٤. ضمان إطلاع جميع الموظفين داخل الكليات والوحدة التشغيلية على هذه السياسة والمسؤولين عن إدراجها في جلسات الإحاطة الأمنية وبرامج التدريب. مسؤول عن إعلام المسؤول المحلي وعمادة تقنية المعلومات والإتصالات من تغيير في صلاحيات أي موظف داخل الكليات.
٥. ضمان أن المستخدمين على فهم طبيعة البرامج الضارة، وكيف ينتشر بشكل عام، والضوابط الفنية لاستخدامها للحماية.
٦. إجراء عمليات التدقيق في الوقت المناسب من سجلات الخادم.
٧. البقاء على علم بالسياسات الخارجية والممارسات الموصي بها وعند الاقتضاء، وإعلام المستخدمين المحليين وتقديم المشورة للإدارة من التغييرات أو التطورات الجديدة.
٨. ممارسة السلطات والامتيازات الاستثنائية المتأصلة في واجباتهم بحكمة. يجب أن تكون خصوصية المستخدمين دائما من الاعتبارات الرئيسية.
٩. وضع الإجراءات المناسبة وإصدار التعليمات لمنع واكتشاف وإزالة البرامج الضارة بما يتفق مع المبادئ التوجيهية الواردة في هذه الوثيقة.
١٠. اخذ نسخ من جميع البيانات والبرمجيات على الخوادم في الوقت المناسب.
١١. التوصية بحزم البرمجيات للكشف عن البرامج الضارة وإزالتها.
١٢. تطوير الإجراءات التي تسمح للمستخدمين بالإبلاغ عن فيروسات الكمبيوتر وغيرها من الحوادث ومن ثم مسؤول عن إخطار الأطراف التي يحتمل أن تتأثر من التهديد المحتمل.
١٣. إخطار على الفور أفراد الأمن المعلوماتي أو فريق الاستجابة للحوادث لجميع الحوادث الأمنية الخاصة بالأمن المعلوماتي بما في ذلك البرمجيات الخبيثة.
١٤. تقديم المساعدة في تحديد مصدر البرامج الضارة.
١٥. تقديم المساعدة لإزالة البرامج الضارة.
١٦. إجراء استعراضات دورية لضمان اتباع الإجراءات الأمنية المناسبة، بما في ذلك الإجراءات المصممة للحماية من البرامج الضارة.

٧,٣قسم امن المعلومات – مسؤولو الشبكة وقواعد البيانات :

١. مسؤول عن إدارة جميع امتيازات وصول المستخدمين إلى البيانات والبرامج والوظائف.
٢. مسؤول عن رصد جميع الأحداث المتعلقة بالأمن ومتابعة أي انتهاكات فعلية أو مشتبه فيها عند الاقتضاء. وعندما يكون ذلك ملائما، يكون مسؤولا عن إبلاغ قسم امن المعلومات. والتنسيق معه عن رصد الأحداث ذات الصلة بالأمن أو التحقيق فيها.
٣. الحفاظ على كلمات المرور آمنة وعدم تقاسم الحسابات. يتحمل المستخدمين المخولين مسؤولية أمن كلمات المرور والحسابات الخاصة بهم. يتعين تغيير كلمات مرور المستخدم كل ثلاثة أشهر.
٤. مسح الشبكة ببرامج مكافحة الفيروسات على فترات منتظمة.
٥. تعيين هوية مستخدم فريدة من نوعها وكلمة مرور (أو غيرها من معلومات الهوية أو بيانات التوثيق) لكل مستخدم فقط بعد الانتهاء من الوثائق المناسبة.
٦. إخطار موظفي الأمن أو فريق الاستجابة للحوادث على وجه السرعة بجميع الحوادث الأمنية المتعلقة بالحواسيب، بما في ذلك البرامج الضارة؛
a. إخطار قسم امن المعلومات إذا كان هناك اختراق في التقدم، ومساعدة المسؤولين المحليين الآخرين في الاستجابة لانتهاكات الأمن.
b. التعاون مع الإداريين المحليين الآخرين و قسم امن المعلومات. في العثور على المنتهكين والمساعدة في جهود الإنفاذ.
٧. مسؤول عن تقديم المساعدة في تحديد مصدر البرامج الضارة ومدى التلوث.