الجامعة السعودية الالكترونية
Saudi Electronic University

دليل سياسة امن المعلومات

المسؤول: مدير أمن المعلومات

الملخص التنفيذي

تلعب سياسات أمن المعلومات دوراً اساسياً في توفير بيئة آمنة للعناصر الحيوية التي تبنى عليها نظم المعلومات والتي تعتمد عليها استمرارية الأعمال وخدمات المنظمات.

تهدف هذه الوثيقة الى تغطية المناطق المتعددة والمهمة المتعلقة بأمن المعلومات، فمع التطور السريع للتكنولوجيا وما يتطلبه ذلك من سياسات وتقنية امنية لتصل الي جميع نظم ومجالات المعلومات والتكنولوجيا،

تم اعداد هذه الوثيقة لتغطية متطلبات الجامعة السعودية الالكترونية من تدريس-ابحاث-الانشطة الجامعية-اعمال-اتصالات، لكل من طلاب الجامعة او اعضاء هيئة تدريس. نقدم هذه السياسة كحجر اساس لضبط كل ما هو مرتبط بعمل الجامعة، والتي تعرف أحيانا ب "مفاهيم الرعاية المحكمة والفائقة" .

إن في ضبط المعايير الامنية منع للعديد المشكلات مثل السطو، السرقة، التجسس، التدمير، الأخطاء، الحذف، بالإضافة الى نظام(الحجب). ومن ناحية اخرى فهذه السياسات تقوم بتحديد الضوابط الضرورية لمنع حدوث أي المشاكل القانونية، على سبيل المثال: التكذيب والانكار، الثغرات القانونية، حقوق الملكية. التعامل مع هذه المشكلات يحتاج الي مثل هذه الوثيقة لمنع اي خسائر غير ضرورية.

1. المقدمة

تنبثق هذه السياسة بشكل مباشر من رسالة الجامعة السعودية الإلكترونية، والتي تعرف الجامعة كجامعة حكومية الكترونية تستخدم التقنيات المتطورة، وبالتالي فإن دور أنظمة المعلومات في الجامعة لا يقتصر على المساعدة في إنجاز المهام فقط، ولكنه يتطور ليصبح عاملاً رئيسيا لنجاح الجامعة في توفير التعليم المتميز والتأهيل العصري لجميع شرائح المجتمع، وفق أعلى معايير الجودة وأفضل الممارسات العالمية. تم تقسيم هذه السياسات الى جزئيين:

أ- الجزء الاول: سياسات المستوى العالي:

نناقش هنا السياسات بشكل عام دون الخوض في التفاصيل ومنها:

- سياسات الإدارة العليا وامن المعلومات(العامة):

والتي تختص بالإدارة العليا، وتناقش أمن الشؤون الخارجية والاقسام العامة لكل من مدراء الإدارات والموظفين.

- سياسة الاستخدام المقبول:

وتلخص جميع المبادئ العامة لأمن المعلومات والتي يجب على جميع الموظفين الاحاطة بها.

ب- الجزء الثاني: والتي تناقش كل ما يختص عمل الجامعة من ناحية تقنية وتختص بتنظيم عمل مهندسين التقنيات، وتتم مراجعة هذا الجزء سنويا لمرة واحدة على الأقل او عند حدوث اي تغييرات بالجامعة.

الجزء الاول:

سياسات المستوى العالي

2. سياسة امن المعلومات العامة

متعلقة بالإدارة العليا، تنفذ على جميع الاقسام.

أ- الهدف:

تحديد المتطلبات لتقديم خطط تكنولوجية فائقة الامان.

ب- النطاق:

مدراء الإدارات، اعضاء هيئة التدريس من داخل او خارج الجامعة.

ج- السياسة:

1. مسؤولية الادارة العليا التأكيد على امن وسرية المعلومات.
2. تقوم الادارة العليا بإمداد الدعم والمصادر الضرورية للوصول الى برنامج ناجح لأمن المعلومات.
3. امن المعلومات محدد بكفاءة وتوافر السياسات الامنية داخل الإطار العام والاجراءات الامنية.
4. مسؤول امن المعلومات يحدد مستوى المشكلات التي تتعامل معها الادارة العليا مباشرة، إذا دعت الضرورة.
5. تتم حماية المعلومات بثقة وامان وامكانية (C I A) اثناء الاستخدام والتخزين والانتقال بغض النظر عن وسيلة التخزين او الانتقال.
6. جميع ما يخص الشركة من (اجهزة-برامج-ادوات –بيانات) له حماية وتعريف خاص.
7. انتاج وتطوير البرامج يجب ان يتم في حماية امنية داخل موقع الانتاج.
8. تحتفظ الجامعة بحقوق توجيه مرور المعلومات عبر شبكتها، وذلك بحماية جميع الاجهزة والبرامج.
9. حماية امن الجامعة ضد اي تهديدات يلزمه برامج مضادة للفيروسات وجدار ناري، موانع اقتحام (IPS) وغيرها.
10. عند حدوث اي اختراقات او ثغرات امنية لابد من ارسال تقارير فورية الي مدير امن المعلومات.
11. وضع ضوابط صحيحة للعمل بتمكن وامان.
12. مدير امن المعلومات هو راعي برامج امن المعلومات.
13. تطوير المعالجات لجميع مناطق العمل.
14. وثائق امن المعلومات يتم مراجعتها سنوياً لمرة واحدة على الأقل.
15. وضع الضوابط صحيحة لإجراءات " التعامل مع المخاطر".
16. إلزام مدير امن المعلومات بتدريب الفريق المختص بالتعامل مع المخاطر (CIRT) وتدوين خطط الخاصة بإجراءات الاستجابة والتدخل السريع لأي خطر.

17. يتم تدوين جميع المخاطر والثغرات الامنية ورفعها فورا لمدير امن المعلومات (ISM) والذي بدوره سيقوم باتخاذ الإجراءات اللازمة للتعامل معها والحرص على عدم حدوثها مستقبلاً.
18. انشاء ادارة التامين ضد المخاطر.
19. سيتم تامين جميع الانظمة بما فيها نظام العمليات على مستوى المخاطر المحتملة.
20. الامن المادي والذي يجب أن يتضمن جميع المواقع الحيوية: المباني، غرف البيانات وغيرها.
21. على جميع الموظفين ارتداء بطاقات التعريف الخاصة بهم.
22. يمنع مناقشة اي معلومات خاصة بالجامعة في الأماكن العامة.
23. عند الانتهاء من الاجتماع يجب التأكد من ازالة اي معلومات او بيانات او جداول بالغرفه.
24. يجب اتباع سياسة المكتب النظيف بجميع انحاء الجامعة.
25. يمنع استخدام أجهزة الحاسب الخاصة بالجامعة في غير الأمور المتعلقة بالعمل.
26. اي اعلانات تختص بطلبات التوظيف او المساعدة يجب أن تكون خالية تماما من اي معلومات حساسة او خطط خاصة بأعمال الجامعة.
27. سياسة " الاستعانة بمتخصص " لأي استشارة خارجية مطلوبة.
28. ضرورة توافر الاجراءات القانونية.
29. الامن هو مسؤولية مشتركة بين الجميع، لذا يجب على جميع موظفين الجامعة اتباع السياسات الامنية المطلوبة منهم.
30. جميع مصادر الجامعة متوافرة للاستخدام الرسمي فقط.
31. على مدير امن المعلومات تقديم جميع الارشادات والسياسات الامنية.
32. يمنع التهاون في اتباع أي بند من بنود هذه السياسات.
33. جميع معلومات الجامعة سواء الصادرة او الواردة هي حقوق خاصة بالجامعة ويحق لها توجيهها والتحكم بها.
34. سيتم التعامل مع جميع المعلومات بسرية تامة الا المعلومات التي تندرج تحت بنود الاستخدام العام.
35. على جميع الموظفين حماية كلمات المرور الخاصة بهم ويمنع مشاركتها مع اي شخص اخر.
36. يجب حماية جميع أجهزة الحاسب الآلي (سطح المكتب/ المحمولة) بكلمات مرور قوية، ويجب ان يتم اغلاقها تلقائيا عند توقف نشاطها لمدة لا تزيد عن عشر دقائق.
37. يتم تخزين المعلومات الحساسة داخل أجهزة الحاسب الآلي بكلمة مرور خاصة.
38. لابد ان تعمل جميع الاجهزة بأحدث برامج الحماية من الفيروسات ولا يسمح لأي موظف تعطيل او ايقاف تلك البرامج.

39. فرض سياسات لاستخدام البريد الإلكتروني والإنترنت.
40. يمنع استخدام نسخ لبرامج غير مصرح لها.
41. عند استخدام الفاكس للمراسلات الهامة يجب أن تتم عملية الارسال بتوازي لوقت الارسال والاستقبال.
42. يمنع السماح بعبور اي خادم خارجي او داخلي بدون أن يخضع للفحص والتدقيق.

د- الالزام:

يلتزم جميع الموظفين والطلاب باتباع هذه السياسات، وسيتم التعامل مع المخالفات حسب الإجراءات القانونية المتبعة.

هـ- المسؤولية:

تقع على جميع الموظفين والطلاب.

3. سياسة الاستخدام المقبول

أ- الهدف:

تهدف هذه السياسة إلى إدارة الدخول المنطقي والمادي، بحيث يقتصر على الاشخاص المفوضين والأجهزة المصرح بها فقط داخل الجامعة السعودية الإلكترونية.

ب- النطاق:

تشمل جميع الموظفين الدائمين او الاستشاريين.

ج- السياسة:

1. اتباع تعليمات الأمن والسلامة مسؤولية جماعية.
2. مصادر الجامعة مخصصة للاستخدام في حاجة العمل فقط ولا يحق لأي موظف استخدامها لأغراض شخصية.
3. تقوم ادارة امن المعلومات بوضع التعليمات وتغير السياسات حسب ما تدعو الية حاجة العمل.
4. يمنع التهاون في تطبيق أحد بنود هذه السياسات.
5. جميع معلومات الجامعة هي حق للجامعة في التوجيه والتعديل.
6. الحماية الحازمة لجميع المعلومات الحساسة، فيمنع نسخها او تعديلها او تداولها خارج نطاق العمل.
7. حماية كلمات المرور مسؤولية الموظف. فيمنع مشاركتها نهائيا مع اي شخص اخر.
8. تتغير كلمة المرور حسب السياسات الخاصة.
9. يجب حماية جميع أجهزة الحاسب الآلي (سطح المكتب/ المحمولة) بكلمات مرور قوية، ويجب ان يتم اغلاقها تلقائيا عند توقف نشاطها لمدة لا تزيد عن عشر دقائق.
10. يتم تخزين المعلومات الحساسة داخل أجهزة الحاسب الآلي بكلمة مرور خاصة.
11. لابد ان تعمل جميع الاجهزة بأحدث برامج الحماية من الفيروسات ولا يسمح لأي موظف تعطيل او ايقاف تلك البرامج.
12. فرض سياسات لاستخدام البريد الإلكتروني والإنترنت.
13. يمنع استخدام نسخ لبرامج غير مصرح لها.
14. عند استخدام الفاكس للمراسلات الهامة يجب أن تتم عملية الارسال بتوازي لوقت الارسال والاستقبال.
15. يمنع السماح بعبور اي خادم خارجي او داخلي بدون أن يخضع للفحص والتدقيق.

د- الالزام:

يلتزم جميع الموظفين والطلاب باتباع هذه السياسات، وسيتم التعامل مع المخالفات حسب الإجراءات القانونية المتبعة.

هـ- المسؤولية:

تقع على جميع الموظفين ومدراء الإدارات ومدير امن المعلومات عميد تقنية المعلومات وتكنولوجيا التعليم.

الجزء الثاني:

تفاصيل السياسات سياسة حماية البيانات والملكية

4. سياسة حماية البيانات

أ- الهدف:

تصنيف البيانات حسب المالك الأصلي لها، وتكليفه بالمهام والمسؤوليات التي تعنى بحمايتها.

ب- النطاق:

تقع على جميع الموظفين المفوضين بالتعامل مع البيانات ويجب عليهم معرفه طريقة استخدامها والتعامل معها.

ج- السياسة:

1. مسؤول البيانات يتم تعيينه على حسب التخصص. فهو الشخص المسؤول والقائد لوحدة العمل على سبيل المثال: مدير الإدارة المالية يمتلك جميع البيانات المالية ولا علاقة له ببيانات إدارة شؤون الموظفين.
2. مسؤول البيانات مرتبط بالبيانات واهميتها وحساسيتها، والتحكم والتوجيه بكل ما هو متعلق بهذه البيانات.
3. لا يتم التعامل مع البيانات دون الرجوع لمسؤول البيانات.
4. على مسؤول البيانات التأكد من وجود نسخة احتياطية من البيانات في مكان امن.
5. مسؤول البيانات عليه حماية البيانات من اي مخاطر.
6. يتم عمل نسخة احتياطية لبيانات الخادم.
7. يجب على مسؤول البيانات التأكد من الضوابط الامنية اللازمة.
8. يجب تزويد مسؤول البيانات بجميع الوثائق المتعلقة بجميع النشاطات للبيانات.
9. يتم اشعار مالك البيانات من قبل مسؤول البيانات في حال حدوث أي تجاوزات او مخاطر تم حدوثها.

د- الالزام:

يلتزم جميع الموظفين باتباع هذه السياسة، وسيتم التعامل مع المخالفات حسب الإجراءات القانونية المتبعة.

هـ- المسؤولية:

مالك البيانات، مسؤول البيانات، إدارة امن المعلومات، عميد تقنية المعلومات وتكنولوجيا التعليم.

5. سياسة امن المعلومات

أ- الهدف:

تحديد ضوابط حماية المعلومات وكيفية استخدامها وتخزينها والتعامل معها داخل الشبكة.

ب- النطاق:

امدادات المعلومات بغض النظر عن الوسيلة المستخدمة للتخزين او التواصل.

ج- السياسة:

1. يحدد مالك الحاسوب اهمية المعلومات والنسخ الاحتياطية للبيانات ومدى بقاءها.
2. يتم تحديد الخادم وتزويده بالنسخ الاحتياطية على حسب رغبة صاحب البيانات وعميد تقنية المعلومات وتكنولوجيا التعليم بالإضافة لمدير امن المعلومات.
3. يتم التأكد من تخزين النسخ الاحتياطية.
4. صاحب البيانات يقوم بتحديد مدة الاحتفاظ بالبيانات.
5. عدم استخدام برامج مقرصنة او غير قانونية.
6. يمنع تحميل اي برامج يتم شرائها من قبل جهات خارجية قبل الحصول على إذن رسمي من قبل مدير امن المعلومات.
7. يتم اختبار جميع البرامج داخل البيئة الافتراضية اولاً قبل نشرها على النطاق العام.
8. يتم اتخاذ الاجراءات الأمنية للحماية من التهديدات الداخلية والخارجية مثل: تركيب البرامج مضادة للفيروسات، الجدار الناري،IDS .

د- الالزام:

يلتزم جميع الموظفين والطلاب باتباع هذه السياسات، وسيتم التعامل مع المخالفات حسب الإجراءات القانونية المتبعة.

هـ- المسؤولية:

تقع على جميع الموظفين ومدراء الإدارات ومدير امن المعلومات وعميد تقنية المعلومات وتكنولوجيا التعليم.

سياسة برامج المضادة للفيروسات والقرصنة

6. سياسة مكافحة الفيروسات ورسائل البريد الالكتروني الغير مرغوب بها

أ- الهدف:

تهدف هذه السياسة الى وضع الضوابط لبرامج مكافحة البرمجيات الضارة مثل: الفيروسات –الديدان – حصان طروادة – وغيرها.

ب- النطاق:

تطبق على جميع وسائل الاتصالات الالكترونية، بالإضافة الى وسائط التخزين والتي قد تكون عرضة لبرامج السرقة والقرصنة.

ج- السياسة:

- سياسة مقاومة الفيروسات:

1. جميع الاجهزة المستخدمة يتم تشغيلها بأحدث برامج مكافحة الفيروسات بعد موافقة عمادة تقنية المعلومات وتكنولوجيا التعليم.
2. يمنع فتح رسائل البريد الالكتروني والتي تحتوي على مرفقات مشبوهة او المرسلة من مصادر مجهولة ويتم حذفها بشكل مباشر.
3. يجب على جميع الموظفين التحقق من هوية المرسل قبل توجيه الرسائل البريدية او الرد عليها.
4. يجب فحص الوسائط الغير ثابتة (القرص المرن وغيره) قبل الاستخدام.
5. يمنع استخدام البرامج المقرصنة على شبكة الجامعة.
6. في حالة اكتشاف فيروس يجب اخطار مدير امن المعلومات فورا. وبناء على ذلك سيقوم مدير امن المعلومات باتخاذ الاجراءات الامنية اللازمة لتجنب حدوثه مستقبلاً.
7. يمنع محو اي فيروس بدون الرجوع لمدير امن المعلومات.
8. جميع أدوات التشفير سيتم فحصها وفك شيفرتها للتأكد من خلوها من اي فيروسات قبل الاستخدام.
9. يتم تزويد خادم البريد الالكتروني ببرامج مضادة للفيروسات وفحص جميع الرسائل الالكترونية وملحقاتها قبل ارسالها الى صندوق البريد.
10. جميع البرامج المضادة للقرصنة سيتم تحديثها اليا من الشبكة او من الخادم المركزي.

- قائمة فحص الرسائل الالكترونية المصنفة كتهديد:

يجب اتباع التالي:

1- يتم تصنيف الرسائل الالكترونية حسب احتمالية كونه "بريد غير مرغوب به".
2- التأكد من كونه بريد غير مرغوب به.
3- على الإدارة المختصة اتباع إجراءات الحماية وفرز الرسائل الالكترونية التي تم التأكد من كونها رسائل تهديدية او رسائل مشتبه بها ثم القيام بحذفها.

- يتم مراجعه البريد المشتبه به يوميا كأجراء أمني.
- على الإدارة المختصة تحديد الادوات والبرامج للتعامل مع مثل هذه الرسائل الالكترونية للفحص الالي لأي رسائل مشتبه بها تم تمريرها للمستخدم.
- الرسائل ذات العناوين الخطرة يجب حظرها فورا من الوصول الى العناوين البريدية التابعة للجامعة. ويتم حفظ هذا العناوين بالقائمة السوداء.
- آليات التعرف على الرسائل الخطرة يجب ان تحتوي على اجراءات اضافية لمنع الرسائل النظيفة من أن تصنف كرسائل تهديد وذلك بان يتم عمل قائمة بيضاء لعناوين المراسلات السليمة.
- على الإدارة المعنية تقديم مقترحات حول عناوين المراسلات السليمة لإضافتها الى القائمة البيضاء.
- على الإدارة المعنية ان تقوم بفحص محتويات البريد الالكتروني للتأكد من خلوها من اي برامج مصابة او مقرصنة.

د- الالزام:

يلتزم جميع الموظفين والطلاب باتباع هذه السياسات، وسيتم التعامل مع المخالفات حسب الإجراءات القانونية المتبعة.

هـ- المسؤولية:

تقع على جميع الموظفين وإدارة البنية التحتية وإدارة امن المعلومات عميد تقنية المعلومات وتكنولوجيا التعليم.