إدارة سياسات نظم إدارة أمن المعلومات(ISMS)

	عمادة التعاملات الإلكترونية والاتصالات إدارة البوابة الالكترونية	رقم الوثيقة	رقم الإصدار	اعتماد ادارة التطوير والجودة	اعتماد العميد
			1		
	سياسات وإجراءات إدارة المخاطر وأمن المعلومات				

2- هدف الوثيقة:

الغرض من هذه السياسة هو ضمان التزام جامعة الملك سعود نحو إدارة أمن المعلومات ونظام إدارة أمن المعلومات (ISMS) .و تعتبر الإدارة هي المسؤولة عن ضمان الاستعراضات الدورية ل ISMS والتحسينات استنادا إلى نتائج هذه الاستعراضات.

3- مجال التطبيق:

يتم توجيه هذه السياسة نحو إدارة جامعة الملك سعود إدارة عمادة التعاملات الإلكترونية والاتصالات.

4.2.1 إنشاء ISMS.
4.2.2 تنفيذ وتشغيل.
4.2.3 رصد واستعراض ISMS.
4.2.4 صيانة وتحسين ISMS.
4.3.2 التحكم بالوثائق ISMS.
4.3.3 التحكم بالسجلات.
5.1 التزام الإدارة.
5.2 ادارة الموارد.
6 التدقيق الداخلي.
7.2 مراجعة المدخلات ISMS.
7.3 مراجعة المخرجات.
8.1 استمرار التطوير.
8.2 إجراءات تصحيحية.
8.3 إجراءات الوقائية.

3- المسؤوليات:

إدارة عمادة التعاملات الإلكترونية والاتصالات هي المسؤولة عن دعم مبادرات أمن المعلومات من خلال ضمان توفير الموارد الكافية واستعراض دوري لفعالية التدابير الأمنية .وردت مفصلة في ISMS , الأدوار والمسؤوليات في منظمة سياسة أمن المعلومات .

4- سياسات العمل:

4.1. تصريحات عامة

4.1.1. نظام إدارة أمن المعلومات (ISMS)في جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات)، وجب انشأها و تنفيذها وتشغيلها ومراقبتها ومراجعتها عن طريق تحديد نطاقها وحدودها، وتعتبر سياسة(ISMS)، نهج تقييم المخاطر ومعايير القبول للخطر . تكون جميع وثائق (ISMS) تتطلب موافقة الإدارة.

4.1.2. تعريف المخاطر التي تتعرض لها أصول المعلومات الحرجة جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) والنظم الأساسية ليتم تحليلها وتقييمها مع الخيارات المتاحة لعلاج المخاطر.

4.1.3. يتم اختيار الضوابط المناسبة، ويجب الحصول على موافقة الإدارة المخاطر المتبقية والترخيص للتنفيذ وعمليات (ISMS).

4.1.4. يجب إعداد و استعراض بيان التطبيق (SOA).

4.1.5. يجب أن تستعرض سياسة أمن المعلومات لضمان تحقيق أهداف الأعمال والمتطلبات النظامية، و هي كافية و فعالة؛ والاتصالات لجميع الموظفين والأطراف الخارجية حسب الاقتضاء.

4.1.6. إعداد خطة لعلاج الخطر، ويجب تنفيذ الضوابط.

4.1.7. إنشاء و استعراض الاجراءات , لتمكين التنفيذ السليم و الحفاظ على الضوابط.

4.1.8. الحفاظ و استعراض على نظم إدارة المعلومات الموثقة , في سياق المهام و المخاطر لأعمال المنظمة العامة .

4.1.9. وتجرى عمليات التدقيق الداخلي ISMSعلى الأقل مرة واحدة في السنة ، لتحديد مدى فعالية وملاءمة أهداف المراقبة والضوابط والعمليات والإجراءات من ISMS.

4.1.10. فعالية ISMS يجب تحسينها باستمرار من خلال استخدام المعلومات السياسة الأمنية، والأهداف الأمنية ، ونتائج المراجعة والتحليل للأحداث رصد وقياس فعالية الضوابط "، والإجراءات التصحيحية والوقائية واستعراضات الإدارة.

4.1.11. ال ISMS في جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) يجب أن تتوافق مع جميع التطبيقات من القانونية والتعاقدية الدستورية والتنظيمية

4.2. تأسيس الISMS

4.2.1. تحديد النطاق والحدود لISMS في جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات)، وتتم مراجعتها سنويا نظرا للأعمال ، والمتطلبات التعاقدية والالتزامات القانونية .ويمكن تبرير أي استثناء من نطاق وتوثيقه.

4.2.2. المنهجية محددة مسبقا لتحديد العمليات التجارية الهامة و أصول المعلومات ذات الصلة ، وتقييم المخاطر، وتقييم الخيارات العلاجية للخطر ، يجب أن يتبع معايير لقبول المخاطر وتحديد مستويات مخاطر مقبولة.

4.2.3. إعداد بيان التطبيق (SOA) وتحديثها بعد النظر في الضوابط التي تنفذ حاليا، أهداف المراقبة والضوابط المحددة لمعالجة المخاطر استنادا إلى منهجية تقييم المخاطر والأعمال التجارية والمتطلبات القانونية مع مبرر لاستبعاد أي أهداف مراقبة أو ضوابط.

4.2.4. وتوضع السياسات والإجراءات الأمنية /المحدثة /المعدلة لمعالجة الضوابط المحددة واللازمة لتنفيذها.

4.2.5. يجب وضع سياسة أساسية للأصول وإجراء تقييم تفصيلي للمخاطر التي لا حاجة لها.

4.3. تنفيذ وتشغيل ISMS

4.3.1. يتم تشكيل فريق تنفيذ المعلومات الأمنية (ISIT) لتنفيذ وتشغيل وصيانة نظام إدارة أمن المعلومات ISMS .

4.3.2. تنفذ الضوابط المحددة على أساس (SOA)بعد وضع خطة العلاج وتحديد المخاطر الإجراءات الإدارية، والموارد والمسؤوليات والإطار الزمني للتنفيذ.

4.3.3. يجب وضع تدابير مناسبة لفعالية الضوابط أو مجموعة من الضوابط لتقييماتها.

4.3.4. وجوب تنظيم برامج التوعية والتدريب الأمني بشكل دوري , على سبيل المثال للموظفين الجدد خلال فترة التوظيف يعطى هذا التدريب .

4.3.5. على مدير نظام إدارة أمن المعلومات إدارة العمليات و موارد نظم ادارة أمن المعلومات (ISMS).

4.4. المراقبة و المراجعة ل ISMS

4.4.1. يجب تنفيذ إجراءات للكشف عن الحادث المطالبة، والإبلاغ والاستجابة والتصعيد.

4.4.2. رصد واستعراض الإجراءات والضوابط الأخرى كحد أدنى مرة واحدة في السنة للكشف عن الأخطاء والثغرات الأمنية، والحوادث، لتحديد ما إذا كان يتم تنفيذ الرقابة كما هو متوقع وفعالية الإجراءات المتخذة لتسوية الخروقات الأمنية.

4.4.3. يجب أن يجرى التدقيق الداخلي ل ISMS على الاقل مرة واحدة في السنة.

4.4.4. تقاس فعالية ISMS سنويا من مدخلات المراجعة الداخلية ومراجعة الحسابات الأمنية، وحوادث، وقياس فعالية الرقابة والاقتراحات والملاحظات من جميع الأطراف المهتمة.

4.4.5. يجرى تقييم المخاطر على أساس سنوي، ومستوى المخاطر المتبقية ومخاطر مقبولة، يجب مراجعة النظر في إجراء تغييرات في التنظيم، والتكنولوجيا، والأعمال التجارية، والبيئة الخارجية)القانونية والتعاقدية ، والاجتماعية(، والتهديدات التي تم تحديدها وفعالية الضوابط المنفذة.

4.4.6. يجب صيانة سجل الإجراءات والأحداث التي تؤثر على ISMS.

4.5. صيانة و تحسين الISMS

4.5.1. يجب تنفيذ التحسينات التي تم تحديدها في ISMS.

4.5.2. يجب أن تتخذ الإجراءات التصحيحية والوقائية لتصحيح نقاط الضعف في بيئة الرقابة وأي مستقبل غير المطابقة.

4.5.3. الأخذ بالإعتبار الخبرات الأمنية للمنظمات أخرى لتحسين نظم ادارة أمن المعلومات (ISMS) عمادة التعاملات الإلكترونية والاتصالات .

4.5.4. يجب على اللجنة التوجيهية ل ISMS ضمان تحقيق التحسينات أهدافها المرجوة.

4.6. التوثيق

4.6.1. مقابل كل الوثائق .ISMSيجب التحكم و تأمين السياسات والأهداف والنطاق والإجراءات ومنهجية تقييم المخاطر، تقرير تقييم المخاطر، وخطة علاج المخاطر لISMS ، وفقا للأدلة لمتطلبات ISMSوالعمليات ، وبيان التطابق.

4.6.2. يتعين على كل قسم /شعبة الاحتفاظ بالسجلات لتقديم أدلة على المطابقة لل ISMSوبالنسبة لجميع الأحداث الهامة من الحوادث الأمنية ذات الصلة ISMS.

4.6.3. يجب الإلتزام بضوابط الموثقة لتحديد وتخزين وحماية واسترجاعها والاحتفاظ بها والتخلص من السجلات .

4.7. مسؤولية الإدارة

4.7.1. ترأس مدير ISMS اللجنة التوجيهية لتأسيس نظام إدارة أمن المعلومات (ISMS) في جامعة الملك سعود من ، تنفيذ وتشغيل ومراقبة ومراجعة وصيانة وتحسين ISMSوتقديم أدلة على التزامها.

4.7.2. تستعرض سياسة وأهداف وخطط ISMS على الأقل مرة واحدة في السنة لتتضمن التغييرات على الأعمال التجارية ، والمتطلبات التعاقدية والقانونية.

4.7.3. شكلت اللجنة التوجيهية ISMS لضمان توفير موارد كافية لإنشاء وتنفيذ وتشغيل وصيانة ISMS.

4.7.4. جميع الأفراد الذين تم تعيينهم بمسؤوليات لأمن المعلومات أن تكون مختصة لأداء المهام الضرورية .يجب توفير التدريب الكافي، إذا يجب أن يعمل الأفراد أو تدريبهم اللازمة لتلبية هذه الاحتياجات.

4.7.5. يجب أن يكون جميع الافراد المعنيين على بينة من أهمية دورها بأنشطة أمن المعلومات ومساهمتها في تحقيق أهداف ISMS.

4.8. المراجعة الداخلية ل ISMS

4.8.1. مراجعة الداخلية لل ISMSجامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) على الاقل مرة واحدة كل عام للتأكد من الامتثال لجميع السياسات والإجراءات و ISMS والوثائق الخاصة به لتحديد الغير مطابقة منها في التنفيذ والتشغيل.

4.8.2. المراجعة الداخلية تتطلب النظر في متطلبات المعايير الدولية، والتنظيم ، ووضع وأهمية العمليات التي سيجري تدقيقها، وكذلك نتائج عمليات مراجعة الحسابات السابقة.

4.8.3. يقوم مدير نظام إدارة أمن المعلومات بتحديد الأهداف والمعايير والنطاق ووتيرة وأساليب التدقيق الداخلي.

4.8.4. يجب ضمان نزاهة واستقلالية عملية مراجعة الحسابات .يجب عدم مراجعة المدققين الداخليين لأعمالهم.

4.8.5. يكون مدير الإدارة مسؤولا عن المنطقة التي تم مراجعتها ويجب ضمان اتخاذ إجراءات سريعة لإزالة الاكتشافات الغير المطابقة ومعرفة أسبابها.

4.8.6. يجب اللجنة التوجيهية ل ISMS اتخاذ الإجراءات للقضاء على سبب عدم المطابقة وتحديد إجراءات للوقاية من عدم التطابق في المستقبل بتنفيذ وتشغيل ISMS.

4.9. الاستعراض الإداري ل ISMS

4.9.1. يجب على اللجنة التوجيهية ISMS استعراض ISMSعلى الأقل مرة واحدة في السنة لضمان استمرار ملاءمة وكفاية وفعالية، وتحسين وتغيير ISMSحيثما كان ذلك ممكنا بما في ذلك الأهداف الأمنية /السياسات /الإجراءات .سوف يتم توثيق محاضر الاجتماعات والسجلات.

4.9.2. سوف يتم توثيق هذه الاستعراضات ويجب الحفاظ على سجلاتها للتحقق منها.

4.9.3. مدخلات لمراجعة الإدارة - نتائج مراجعة الحسابات ل ISMS، الاستعراضات ، التقييمات من الأطراف المعنية، ووضع الإجراءات الوقائية والتصحيحية، ونقاط الضعف والتهديدات التي لم تعالج بالشكل المناسب، ونتائج قياسات الفعالية ، وإجراءات المتابعة من مراجعات الإدارة السابقة ، أي تغييرات في وبيئة الأعمال التي يمكن أن تؤثر ISMSوتوصيات لتحسين أن يكون أساسا لمراجعة الإدارة.

4.9.4. مخرجات مراجعة الإدارة --تحسين فعالية ISMS، تحديث تقييم المخاطر /العلاج خطة لتغطية التغيرات في الإعداد / بيئة، والتغييرات المطلوبة لسياسات /الإجراءات بما يتماشى مع التغيرات في متطلبات العمل والعمليات ، والمتطلبات التعاقدية والقانونية، ومستويات الخطر أو المخاطرة معايير القبول، والاحتياجات من الموارد وتحسين فعالية لقياس السيطرة.

4.10. تحسين ال ISMS

4.10.1. بناء على تقارير المراجعة الداخلية، وتقارير فعالية الضوابط وتقارير إدارة الحادثة واللجنة التوجيهية ISMSاتخاذ إجراءات للقضاء على أسباب عدم المطابقة، وتحديد الإجراءات اللازمة للحماية ضد عدم المطابقة المحتملة المرتبطة بتنفيذ وعمليات ISMS.

4.10.2. يجب اتخاذ إجراءات وقائية تكون ملائمة لتأثير المشاكل المحتملة أو بناء على نتائج تقييم المخاطر أو على تحديد المخاطر يطرأ تغيير كبير عليها.

4.10.3. تنفذ الإجراءات الوقائية / التصحيحية والتحسينات التي تم تحديدها في ISMS من شخصية مسؤولة لتسجيل الإجراءات المتخذة.

4.10.4. يجب التحقق من الإجراءات الوقائية التي اتخذها مدير ISMS / ISOوإبلاغ النتائج إلى اللجنة التوجيهية ل ISMS.

4.10.5. يجب على اللجنة التوجيهية ل ISMS استعراض الإجراءات التصحيحية والوقائية المتخذة لعدم المطابقة حاليا وفي المستقبل، وضمان تحقيق تحسينات أهدافها المرجوة.

4.10.6. يجب على أصحاب الأصول المعنية تتولى مسؤولية بتحديد السبب الجذري لعدم مطابقة ، إغلاقها وتطبيق الضوابط المناسبة لمنع تكرار حدوث عدم المطابقة.

4.10.7. يجب أن يسعى أعضاء منظمة الأمن لتعلم الدروس من تجارب المنظمات الأخرى وتحسين ISMS في جامعة الملك سعود(عمادة التعاملات الإلكترونية والاتصالات).

4.10.8. تتم مراجعة سياسات أمن المعلومات أو إجراءات لإزالة أوجه الضعف في نظم الرقابة وتحسين الوضع الأمني للمنظمة.

5- الانطباق والتنفيذ :

5.1. يحق لجميع الموظفين جامعة الملك سعود(عمادة التعاملات الإلكترونية والاتصالات). بما في ذلك الاستشاريين والموظفين من جهات أخرى والزوار طرف ثالث تلتزم هذه السياسة.

5.2. عدم الامتثال لهذه السياسة من قبل أي موظف يخضع لإجراءات تأديبية ، قد تشمل إنهاء الخدمة.

6- الوثائق المرتبطة :

- منظمة سياسة أمن المعلومات
- سياسات وإجراءات أمن المعلومات
- منهجية إدارة المخاطر