جمهورية العراق

وزارة التعليم العالي والبحث العلمي

جامعة واسط

دليل سياسة واقع الامن السيبراني في جامعة واسط

Email/quality@uowasit.edu.iq

سياسة الأمن السيبراني في جامعة واسط

مقدمة

تُعدّ سياسة الأمن السيبراني هذه وثيقة أساسية تُحدد قواعد وإجراءات حماية أنظمة المعلومات والبيانات الحساسة في الجامعة من المخاطر والتهديدات الإلكترونية. تهدف هذه السياسة إلى ضمان استمرارية عمل الجامعة وحماية خصوصية أعضاء هيئة التدريس والموظفين والطلاب.

أهداف سياسة الأمن السيبراني

•حماية الأصول المعلوماتية: تشمل البنية التحتية لتقنية المعلومات، والبيانات والبرامج والتطبيقات من الهجمات الإلكترونية.

•ضمان توافر الخدمات الإلكترونية: ضمان استمرارية عمل أنظمة الجامعة الإلكترونية مثل البريد الإلكتروني ومنصات التعلم الإلكتروني وسجلات الطلاب.

•حماية الخصوصية: حماية المعلومات الشخصية لأعضاء هيئة التدريس والموظفين والطلاب من الوصول غير المصرح به أو الاستخدام غير القانوني.

•التوعية بمخاطر الأمن السيبراني: نشر ثقافة الأمن السيبراني بين جميع أعضاء مجتمع الجامعة.

نطاق تطبيق سياسة الأمن السيبراني

تُطبق هذه السياسة على جميع أعضاء مجتمع الجامعة بما في ذلك أعضاء هيئة التدريس والموظفين والطلاب وتشمل جميع الأجهزة والأنظمة الإلكترونية المتصلة بشبكة الجامعة بما في ذلك أجهزة الكمبيوتر المحمولة والأجهزة اللوحية والهواتف الذكية وأجهزة إنترنت الأشياء.

المسؤوليات

•إدارة الجامعة: تلتزم إدارة الجامعة بتوفير الموارد اللازمة لتنفيذ هذه السياسة وتشكيل فريق متخصص للأمن السيبراني للإشراف على تطبيقه.

•أعضاء هيئة التدريس والموظفين: يلتزمون باتباع قواعد وإجراءات الأمن السيبراني وحماية المعلومات الحساسة والإبلاغ عن أي مشكلات أمنية.

•الطلاب: يلتزمون باتباع قواعد وإجراءات الأمن السيبراني واستخدام أنظمة الجامعة الإلكترونية بشكل مسؤول.

عناصر سياسة الأمن السيبراني

•إدارة هويات الدخول: استخدام كلمات مرور قوية وفريدة من نوعها وتغييرها بشكل دوري.

•التحكم في الوصول: تحديد مستوى الوصول إلى المعلومات والأنظمة الإلكترونية بناءً على مبدأ الحاجة إلى المعرفة.

•التوعية والتدريب: تقديم برامج توعية وتدريب حول مخاطر الأمن السيبراني وأفضل الممارسات لحماية المعلومات.

•الاستجابة للحوادث: وضع خطة للاستجابة للحوادث الإلكترونية وتحديد الأدوار والمسؤوليات في حالة حدوث أي هجوم.

•التدقيق والمراجعة: مراجعة سياسة الأمن السيبراني بشكل دوري للتأكد من ملاءمتها وفعاليتها.

اعتماد سياسة الأمن السيبراني

يجب اعتماد هذه السياسة من قبل الإدارة العليا للجامعة ونشرها على نطاق واسع لجميع أعضاء مجتمع الجامعة. ان سياسة الأمن السيبراني هي أداة أساسية لحماية الجامعة من المخاطر والتهديدات الإلكترونية. يجب أن تُعتمد هذه السياسة من قبل الإدارة العليا للجامعة وأن تُطبق بشكل فعال من قبل جميع أعضاء مجتمع الجامعة.

تُعدّ الإجراءات التقنية والإدارية ضرورية لضمان تطبيق سياسة الأمن السيبراني بشكل فعال يجب أن تُستكمل هذه الإجراءات بتوثيق واضح ودقيق، وأن تُراجع بشكل دوري للتأكد من ملاءمتها وفعاليتها.

أولاً/ الإجراءات التقنية:

•برامج مكافحة الفيروسات: يجب تثبيت برامج مكافحة الفيروسات على جميع الأجهزة المتصلة بشبكة الجامعة وتحديثها بشكل دوري.

•جدران الحماية: يجب استخدام جدران الحماية لمنع الوصول غير المصرح به إلى أنظمة الجامعة الإلكترونية.

•التشفير: يجب تشفير البيانات الحساسة عند نقلها أو تخزينها.

•التحديثات الأمنية: يجب تطبيق تحديثات الأمان بشكل دوري على جميع أنظمة الجامعة الإلكترونية.

•نظام الكشف عن الاختراق: يجب استخدام نظام الكشف عن الاختراق لاكتشاف أي نشاط مشبوه على شبكة الجامعة.

ثانياً/ الإجراءات الإدارية:

•سياسة كلمات المرور: يجب وضع سياسة قوية لكلمات المرور تحدد متطلبات طولها وتعقيدها.

•التحكم في الوصول: يجب تحديد مستوى الوصول إلى المعلومات والأنظمة الإلكترونية بناءً على مبدأ الحاجة إلى المعرفة.

•التوعية والتدريب: يجب تقديم برامج توعية وتدريب حول مخاطر الأمن السيبراني وأفضل الممارسات لحماية المعلومات.

•التحقيق في الحوادث: يجب التحقيق في جميع الحوادث الإلكترونية وتحديد سببها واتخاذ الإجراءات اللازمة لمنع تكرارها.

•التدقيق والمراجعة: يجب مراجعة سياسة الأمن السيبراني بشكل دوري للتأكد من ملاءمتها وفعاليتها.

استراتيجية الأمن السيبراني لجامعة واسط

تُعدّ استراتيجية الأمن السيبراني ضرورية لحماية المعلومات والأنظمة الإلكترونية لجامعة واسط من المخاطر والتهديدات الإلكترونية. فيما يلي العناصر الأساسية لاستراتيجية الأمن السيبراني لجامعة واسط:

١. تقييم المخاطر:

•إجراء تقييم شامل للمخاطر لتحديد نقاط الضعف في أنظمة الجامعة الإلكترونية.

•تحديد المخاطر الأكثر احتمالًا للحدوث وأكبر تأثيرًا على الجامعة.

٢. وضع خطة عمل:

•وضع خطة عمل لِتحسين سياسة الأمن السيبراني لِتَتوافق مع أفضل الممارسات العالمية.

•تحديد الأهداف والغايات المراد تحقيقها من خلال استراتيجية الأمن السيبراني.

٣. التوعية والتدريب:

•نشر الوعي بين اعضاء الهئية التدريسية والموظفين والطلاب حول مخاطر الأمن السيبراني وأفضل الممارسات للحماية من هذه المخاطر.

•تقديم تدريب منتظم لاعضاء الهئية التدريسية والموظفين والطلاب حول كيفية استخدام أنظمة الجامعة الإلكترونية بشكل آمن.

٤. التكنولوجيا والأدوات:

•استخدام أحدث التقنيات والأدوات لِحماية أنظمة الجامعة الإلكترونية من المخاطر والتهديدات الإلكترونية.

•تحديث أنظمة الجامعة الإلكترونية بشكل دوري لِضمان أمنها.

٥. المراقبة والاختبار:

•مراقبة أنظمة الجامعة الإلكترونية بشكل مستمر لِكشف أي نشاط مشبوه.

•إجراء اختبارات اختراق دورية للتأكد من فعالية سياسة الأمن السيبراني.

٦. الإدارة والاستجابة:

•إنشاء فريق عمل متخصص بالأمن السيبراني لِإدارة سياسة الأمن السيبراني والرد على الحوادث الإلكترونية.

•وضع خطة استجابة للحوادث الإلكترونية لِتحديد كيفية التعامل مع هذه الحوادث.

٧. التعاون:

•التعاون مع الجهات ذات الصلة، مثل وزارة الداخلية و هيئة الاتصالات والإعلام لِتحسين الأمن السيبراني في العراق.

بِمُتابعة هذه العناصر الأساسية يمكن لجامعة واسط تطوير استراتيجية أمن سيبراني فعّالة لِحماية المعلومات والأنظمة الإلكترونية من المخاطر والتهديدات الإلكترونية.

المصادقة والختم

تمت المصادقة على وثيقة سياسة جامعة واسط لتطبيق تقييم واقع الامن السيبراني والعمل بموجبها اعتباراً من تاريخ إقرارها وهي ملزمة لكافة الكليات والتشكيلات المشمولة.

حررت هذه الوثيقة استناداً إلى القوانين والتعليمات النافذة وتخضع للمتابعة والتقييم الدوري من قبل الجهات المختصة في الجامعة.

الاسم :.....

الصفة: رئيس جامعة واسط

الأستاذ الدكتور
رئيس جامعة واسط

التوقيع :.....

التاريخ : ... / ... / ...