الامن السيبراني

اعداد شعبة الموقع الالكتروني
جامعة النهرين

الإجراءات الوقائية للحد من حوادث الأمن السيبراني على مستوى جامعة النهرين

تشمل قائمة التحقق الأساسية لضمان أمان المؤسسة الجامعية مجموعة من التدابير التي تهدف إلى حماية الأجهزة والشبكات والبيانات المخزنة فيها من خلال تطبيق سياسات وإجراءات أمان صارمة كالتالي:

استخدام البريد الإلكتروني والصفحات الشخصية

١ .تثبيت برامج مكافحة البريد الإلكتروني الضار وتحديثها بشكل دوري لحماية المؤسسة من الهجمات الخبيثة.

٢ .لا تُحدّث كلمات المرور للبريد الإلكتروني الجامعي أو الصفحة الشخصية إلا بطلب رسمي موجه إلى مسؤول البريد الالكتروني الجامعي لمعالجة هذه الحالات.

٣ .يتم تحديث معلومات الصفحة الجامعية الخاصة بالتدريسي من قِبَله شخصيًا حفاظًا على خصوصية بياناته.

٤ .تفعيل ميزة التوثيق المتبادل عند استخدام تطبيقات الإنترنت مثلGmail ، لضمان إشعار المستخدم في حال فتح حسابه من جهاز آخر.

٥ .ينبغي أن لا تقتصر إدارة صفحات التواصل الاجتماعي الخاصة بالمؤسسة وفروعها على شخص واحد؛ بل يمكن تكليف واحد أو اثنين من الموظفين الموثوقين للقيام بهذه المهمة.

٦ .استخدام البريد الإلكتروني الجامعي حصريًا في جميع المعاملات الرسمية، بما في ذلك إرسال الأسئلة أو السعيات، وعدم استخدام التطبيقات الأخرى مثل WhatsApp أو Viber أو Telegram لهذا الغرض.

٧ .تجنب استخدام البريد الإلكتروني الجامعي في تفعيل حسابات التواصل الاجتماعي أو الحسابات البنكية والبطاقات الإلكترونية لتجنب المشاكل في حال تعطيل البريد بعد تخرج الطالب.

٨ .تشديد التنبيه على قسم التسجيل بعدم تسليم البريد الإلكتروني الجامعي للطلبة أو ممثليهم بشكل جماعي بصيغة ملفات أو صور تحتوي على الحسابات وكلمات المرور؛ لما لذلك من مخاطر أمنية.

٩ .تنظيم استخدام المساحة التخزينية للبريد الإلكتروني الجامعي وتجنب رفع الصور أو الملفات الخاصة على وحدة التخزين (Google Drive)أو مزامنة الصور تلقائيًا، وقصر استخدام البريد على الأمور الأكاديمية فقط. كما يجب تنبيه الحسابات التي تُلاحظ استخدامًا مفرطًا للتخزين عبر إرسال بريد إلكتروني رسمي لتوضيح حجم الاستخدام والسبب.

١٠ .تنبيه الأفراد إلى عدم فتح الروابط المشبوهة التي قد تصل عبر البريد الإلكتروني أو الرسائل النصية.

١١ .تبليغ فريق إدارة مخاطر الأمن السيبراني في حال فقدان أو سرقة أو تسريب المعلومات.

١٢ .عدم تسجيل البريد الإلكتروني المؤسسي في أي مواقع غير متعلقة بالعمل.

١٣ .يمنع فتح رسائل البريد الإلكتروني أو المرفقات المشبوهة أو غير المتوقعة حتى وإن بدت من مصادر موثوقة.

١٤. إبلاغ فريق الاستجابة لمخاطر الأمن السيبراني عند الاشتباه برسائل بريد إلكتروني تحتوي على محتوى قد يلحق الضرر بأنظمة المؤسسة.

الثقافة الأمنية الإلكترونية العامة

١ .اختيار موظفين يتمتعون بالنزاهة والخبرة للعمل على الأنظمة داخل المؤسسة، لضمان حمايتها من هجمات الأمن السيبراني.

٢ .تأمين أجهزة الكمبيوتر بقفل الشاشة أو تسجيل الخروج (Sign Out or Lock) قبل مغادرة المكتب، سواء لفترات قصيرة أو بعد انتهاء ساعات العمل.

٣ .يمنع تثبيت أي أدوات خارجية على أجهزة الحاسب الآلي دون إذن مسبق من رئاسة القسم أو المسؤول الأعلى.

٤ .وضع سياسات أمنية واضحة للمؤسسة والتأكد من تطبيقها بدقة.

٥ .تدريب الموظفين على الأمن السيبراني وكيفية التعامل مع الهجمات الإلكترونية، بالإضافة إلى التعرف على الرسائل الاحتيالية والبريد المشبوه وآليات التعامل الآمن مع البيانات الحساسة.

٦ .إجراء فحوصات دورية لاكتشاف الثغرات في أنظمة الحماية واتخاذ التدابير اللازمة لسدها فورًا.

٧ .تقتصر إدارة الأنظمة داخل المؤسسة الجامعية على المسؤول المعين، ولا يُسمح بتكليف أشخاص آخرين بهذه المهام.

٨ .يمنع استخدام برنامج Turnitin لأغراض غير رسمية أو مشاركة الحساب الرسمي مع أي شخص.

٩ .عدم ترك المطبوعات على الطابعات المشتركة دون متابعة أو رقابة.

١٠ .حفظ وسائط التخزين الخارجية في أماكن آمنة وبطريقة ملائمة.

١١ .يمنع الإفصاح عن أي معلومات تخص الجامعة، بما في ذلك تفاصيل الأنظمة والشبكات، لأي جهة أو طرف غير مصرح له داخليًا أو خارجيًا.

١٢ .يحظر استخدام أنظمة المؤسسة وأصولها لتحقيق منافع شخصية أو لأي غرض لا يتعلق بنشاطات المؤسسة.

١٣ .في حالة إنشاء مجموعات طلابية، يجب أن تكون تحت إشراف التدريسي نفسه وتدار من قبله دون إشراك الطلاب في إدارتها.

١٤ .تقييد المحادثات في المجموعات الطلابية بحيث تقتصر على التبليغات فقط.

١٥ .عدم مشاركة معلومات بطاقة الراتب مع أي شخص لتجنب الاستغلال أو السرقة.

١٦ .الامتناع عن تنزيل أو تحميل التطبيقات من مصادر غير معروفة.

١٧ .متابعة التنبيهات الأمنية التي يصدرها مصنعو الهواتف.

١٨ .الحرص على عدم نشر بيانات الاتصال الشخصية على مواقع أو منصات غير موثوقة.

١٩. تعلم كيفية ضبط الإعدادات الصحيحة للأمان.

حماية الخوادم والشبكات

١ .السماح فقط للمسؤول المخول بدخول غرفة الخوادم لضمان سرية وأمان بيانات المؤسسة.

٢ .تحديث البرامج والأنظمة وترقيتها بشكل منتظم لتصحيح الثغرات الأمنية وضمان سلامة الأنظمة.

٣ .تحديد مسؤوليات الأفراد من خلال تخصيص صلاحيات الوصول إلى المعلومات الحساسة بناءً على مهامهم.

٤ .استخدام كلمات مرور قوية وآمنة لحسابات المؤسسة (البريد الإلكتروني الجامعي والحسابات الشخصية للتدريسيين) وشبكات Wi-Fi، وتغييرها بشكل دوري. يُنصح باستخدام كلمات مرور مختلفة عن الحسابات الشخصية وعدم مشاركتها بأي وسيلة.

٥ .حماية البيانات الحساسة المخزنة على خوادم الجامعة من خلال تثبيت جدران الحماية وتحديثها دوريًا وتشفير قواعد البيانات باستخدام خوارزميات قوية. يُنصح بتجنب تخزين البيانات على خوادم خارجية.

٦ .تصنيف الأنظمة والبيانات حسب نوع الشبكة المستخدمة للوصول إليها (الداخلية أو الخارجية).

٧ .التأكد من تفعيل أدوات كشف الاختراق وإبلاغ فريق الاستجابة عند اكتشاف أي مشكلة.

٨ .فحص الخوادم بانتظام للتأكد من خلوها من الأجهزة أو البرامج الضارة غير المصرح بها.

٩ .تثبيت برامج الحماية ومكافحة الفيروسات بنسخ أصلية وتحديثها بشكل دوري لحماية الأجهزة والشبكات.

١٠ .استخدام التخزين السحابي الآمن أو الأقراص الصلبة الخارجية لحفظ نسخ احتياطية من البيانات بشكل دوري.

١١ .أرشفة البيانات باستمرار ورفعها على التخزين السحابي بشكل منتظم.

١٢ .تجنب فتح الروابط أو الرسائل المريبة إلا بعد التحقق من مصدرها.

١٣ .في حال تعرض الأجهزة للاختراق، يُمنع الاستجابة لطلبات المهاجمين، ويجب إبلاغ الفريق المختص بسرعة.

١٤ .استخدام البرمجيات والأنظمة المرخصة على أجهزة المؤسسة.

١٥ .ضمان وجود كاميرات مراقبة في مباني المؤسسة وربطها مركزيًا، مع تسجيل البيانات لمدة لا تقل عن ٣٠ يومًا وتأمين مصدر طاقة بديل.

١٦ .التشجيع على استخدام الحواسيب المكتبية لبعض المهام لضمان بقائها في المؤسسة وتقليل المخاطر المرتبطة بالحواسيب المحمولة.

١٧ .استخدام الرمز التعريفي (الباركود) في الوثائق الرسمية لتسهيل التحقق من سلامتها.

١٨ .إبلاغ فريق الأمن السيبراني عند ملاحظة مواقع أو روابط مشبوهة لاتخاذ الإجراءات المناسبة.

١٩ .الحرص على عدم انتهاك حقوق الملكية الفكرية للباحثين داخل المؤسسة.

٢٠ .حظر استخدام التقنيات التي تتجاوز جدار الحماية للوصول إلى الإنترنت.

٢١ .منع استخدام الإنترنت لأغراض غير متعلقة بالعمل مثل تنزيل الوسائط أو استخدام برامج مشاركة الملفات.

٢٢ .الإبلاغ الفوري لفريق الأمن السيبراني عند الاشتباه بوجود مخاطر، والتعامل بحذر مع الرسائل المشبوهة.

٢٣ .منع أي جهة خارجية من إجراء فحص أمني أو اختبار اختراق دون موافقة قيادة المؤسسة وفريق الأمن السيبراني.

٢٤ .حظر استخدام مواقع مشاركة الملفات دون تصريح من القيادة العليا وفريق إدارة الأمن السيبراني.

٢٥ .منع زيارة المواقع المشبوهة مثل مواقع تعليم الاختراق لاحتوائها على أكواد ضارة.

٢٦ .حظر استخدام برامج غير مصرح بها لعقد الاجتماعات المرئية أو إجراء الاتصالات.

٢٧. منع استضافة البيانات على خوادم خارجية دون علم وموافقة القيادة وفريق الأمن السيبراني.