جامعة بيشة
University of Bisha
إدارة الأمن السيبراني

إدارة الأمن السيبراني

سياسة الاستخدام المقبول للأصول

التاريخ:	19/05/2024
الإصدار:	1.2
المرجع:	الضوابط الأساسية للأمن السيبراني (ECC-١: ٢٠١٨) الضابط الأساسي رقم ٢-١

● بنود السياسة

١- البنود العامة

١-١ يجب التعامل مع المعلومات حسب التصنيف المحدد، وبما يتوافق مع سياسة تصنيف البيانات وسياسة حماية البيانات والمعلومات الخاصة بجامعة بيشة بشكل يضمن حماية سرية المعلومات وسلامتها وتوافرها.

٢-١ يحظر انتهاك حقوق أي شخص، أو شركة محمية بحقوق النشر، أو براءة الاختراع، أو أي ملكية فكرية أخرى، أو قوانين أو لوائح مماثلة؛ بما في ذلك، على سبيل المثال لا الحصر، تثبيت برامج غير مصرح بها أو غير قانونية.

٣-١ يجب عدم ترك المطبوعات على الطابعة المشتركة دون رقابة.

٤-١ يجب حفظ وسائط التخزين الخارجية بشكل آمن وملائم، مثل التأكد من ضبط درجة الحرارة بدرجة معينة، وحفظها في مكان معزول وآمن.

٥-١ يمنع استخدام كلمة المرور الخاصة بمستخدمين آخرين، بما في ذلك كلمة المرور الخاصة بمدير المستخدم أو مرؤوسيه.

٦-١ يجب الالتزام بسياسة المكتب الآمن والنظيف، والتأكد من خلو سطح المكتب، وكذلك شاشة العرض من المعلومات المصنفة.

٧-١ يمنع الإفصاح عن أي معلومات تخص جامعة بيشة، بما في ذلك المعلومات المتعلقة بالأنظمة والشبكات لأي جهة أو طرف غير مصرح له سواءً كان ذلك داخلياً أو خارجياً.

٨-١ يُمنع نشر معلومات تخص جامعة بيشة عبر وسائل الإعلام، وشبكات التواصل الاجتماعي دون تصريح مسبق.

٩-١ يُمنع استخدام أنظمة جامعة بيشة وأصولها بغرض تحقيق منفعة وأعمال شخصية، أو تحقيق أي غرض لا يتعلق بنشاط وأعمال جامعة بيشة.

١٠-١ يُمنع ربط الأجهزة الشخصية بالشبكات، والأنظمة الخاصة بجامعة بيشة دون الحصول على تصريح مسبق، وبما يتوافق مع سياسة أمن الأجهزة المحمولة (BYOD).

١-١١ يُمنع القيام بأي أنشطة تهدف إلى تجاوز أنظمة الحماية الخاصة بجامعة بيشة، بما في ذلك برامج مكافحة الفيروسات، وجدار الحماية، والبرمجيات الضارة دون الحصول على تصريح مسبق، وبما يتوافق مع الإجراءات المعتمدة لدى جامعة بيشة.

١-١٢ تحتفظ إدارة الأمن السيبراني بحقها في مراقبة الأنظمة والشبكات والحسابات الشخصية المتعلقة بالعمل، ومراجعتها دورياً لمراقبة الالتزام بسياسات الأمن السيبراني ومعاييره.

١-١٣ يُمنع استضافة أشخاص غير مصرح لهم بالدخول للأماكن الحساسة دون الحصول على تصريح مسبق.

١-١٤ يجب ارتداء البطاقة التعريفية في جميع مرافق جامعة بيشة.

١-١٥ يجب تبليغ إدارة الأمن السيبراني في حال فقدان المعلومات أو سرقتها أو تسريبها.

١-١٦ يجب على المستخدمين المساهمة والمشاركة بنشاط في مبادرات وأنشطة الأمن السيبراني التي ترتبها إدارة الأمن السيبراني (مثل التدريب والتوعية في مجال الأمن السيبراني).

٢- حماية أجهزة الحاسب الآلي

٢-١ يُمنع القيام بأي نشاط من شأنه التأثير على كفاءة الأنظمة والأصول وسلامتها دون الحصول على إذن مسبق من إدارة الأمن السيبراني، بما في ذلك الأنشطة التي تُمكّن المستخدم من الحصول على صلاحيات وامتيازات أعلى.

٢-٢ يجب تأمين الجهاز قبل مغادرة المكتب وذلك بقفل الشاشة، أو تسجيل الخروج (Sign out or Lock)، سواء كانت المغادرة لفترة قصيرة أو عند انتهاء ساعات العمل.

٢-٣ يُمنع ترك أي معلومات مصنفة في أماكن يسهل الوصول إليها، أو الاطلاع عليها من قبل أشخاص غير مصرح لهم.

٢-٤ يُمنع تثبيت أدوات خارجية على جهاز الحاسب الآلي دون الحصول على إذن مسبق من الإدارة العامة للاتصالات وتقنية المعلومات.

٢-٥ يجب تبليغ إدارة الأمن السيبراني عند الاشتباه بأي نشاط قد يتسبب بضرر على أجهزة الحاسب الآلي الخاصة بجامعة بيشة أو أصولها.

٣- الاستخدام المقبول للإنترنت والبرمجيات

٣-١ يجب إبلاغ إدارة الأمن السيبراني في حال وجود مواقع مشبوهة ينبغي حجبها.

٣-٢ يجب ضمان عدم انتهاك حقوق الملكية الفكرية أثناء تنزيل معلومات أو مستندات لأغراض العمل.

٣-٣ يُمنع استخدام البرمجيات غير المرخصة أو غيرها من الممتلكات الفكرية.

٣-٤ يجب استخدام متصفح آمن ومصرح به للوصول إلى الشبكة الداخلية أو شبكة الإنترنت.

٣-٥ يُمنع استخدام التقنيات التي تسمح بتجاوز الوسيط (Proxy) أو جدار الحماية (Firewall) للوصول إلى شبكة الإنترنت.

٣-٦ يُمنع تنزيل البرمجيات والأدوات أو تثبيتها على أصول جامعة بيشة دون الحصول على تصريح مسبق من الإدارة العامة للاتصالات وتقنية المعلومات.

٣-٧ يُمنع استخدام شبكة الإنترنت في غير أغراض العمل، بما في ذلك تنزيل الوسائط والملفات واستخدام برمجيات مشاركة الملفات.

٣-٨ يجب تبليغ إدارة الأمن السيبراني عند الاشتباه بوجود أخطار سيبرانية، كما يجب التعامل بحذر مع الرسائل الأمنية التي قد تظهر خلال تصفح شبكة الإنترنت أو الشبكات الداخلية.

٣-٩ يُمنع إجراء فحص أمني لغرض اكتشاف الثغرات الأمنية، ويشمل ذلك إجراء اختبار الاختراقات، أو مراقبة شبكات جامعة بيشة وأنظمتها، أو الشبكات والأنظمة الخاصة بالجهات الخارجية دون الحصول على تصريح مسبق من إدارة الأمن السيبراني.

٣-١٠ يُمنع استخدام مواقع مشاركة الملفات دون الحصول على تصريح مسبق من إدارة الأمن السيبراني.

٣-١١ يُمنع زيارة المواقع المشبوهة بما في ذلك مواقع تعليم الاختراق.

٣-١٢ يُمنع استخدام أنظمة الجامعة لتخزين بيانات يمكن تفسيرها على أنها منحازة (على سبيل المثال، سياسًيا أو دينًيا أو عرقًيا أو ثقافيا، الخ) أو معالجتها أو تنزيلها أو نقلها.

٣-١٣ يُمنع إيقاف تشغيل حزمة برامج الكشف عن الفيروسات المعتمدة من الجامعة، أو استخدام أي حزمة برامج لمكافحة فيروسات أخرى دون موافقة كتابية من الإدارة العامة للاتصالات وتقنية المعلومات.

٤- الاستخدام المقبول للبريد الإلكتروني ونظام الاتصالات

١-٤ يعتبر البريد الالكتروني الرسمي قناة رسمية معتد بها للتواصل وانهاء المعاملات.

٢-٤ يُمنع استخدام البريد الإلكتروني، أو الهاتف، أو الفاكس، أو الفاكس الإلكتروني في غير أغراض العمل، وبما يتوافق مع سياسات الأمن السيبراني ومعاييره.

٣-٤ يُمنع تداول رسائل تتضمن محتوى غير لائق أو غير مقبول، بما في ذلك الرسائل المتداولة مع الأطراف الداخلية والخارجية.

٤-٤ يجب استخدام تقنيات التشفير عند إرسال معلومات حساسة عن طريق البريد الإلكتروني أو أنظمة الاتصالات.

٥-٤ يجب عدم تسجيل عنوان البريد الإلكتروني الخاص بجامعة بيشة في أي موقع ليس له علاقة بالعمل.

٦-٤ يجب تبليغ إدارة الأمن السيبراني عند الاشتباه بوجود رسائل بريد إلكتروني تتضمن محتوى قد يتسبب بأضرار لأنظمة جامعة بيشة أو أصولها.

٧-٤ تحتفظ جامعة بيشة بحقها في كشف محتويات رسائل البريد الإلكتروني بعد الحصول على التصاريح اللازمة من صاحب الصلاحية وإدارة الأمن السيبراني وفقاً للإجراءات والتنظيمات ذات العلاقة.

٨-٤ يُمنع فتح رسائل البريد الإلكتروني والمرفقات المشبوهة أو غير المتوقعة حتى وإن كانت تبدو من مصادر موثوقة.

٩-٤ لا يجوز للمستخدمين استخدام خدمات البريد الإلكتروني للأنشطة غير القانونية، بما في ذلك أرسال أو تلقي مواد محمية بحقوق الطبع والنشر لما فيه من انتهاك لقوانين حقوق النشر أو اتفاقيات الترخيص

٥- الاجتماعات المرئية والاتصالات القائمة على شبكة الإنترنت

١-٥ يُمنع استخدام أدوات أو برمجيات غير مصرح بها لإجراء اتصالات أو عقد اجتماعات مرئية.

٢-٥ يُمنع إجراء اتصالات أو عقد اجتماعات مرئية لا تتعلق بالعمل دون الحصول على تصريح مسبق.

٦- استخدام كلمات المرور

١-٦ يجب اختيار كلمات مرور آمنة، والمحافظة على كلمات المرور الخاصة بأنظمة جامعة بيشة وأصولها. كما يجب اختيار كلمات مرور مختلفة عن كلمات مرور الحسابات الشخصية، مثل حسابات البريد الشخصي ومواقع التواصل الاجتماعي.

٦-١ يُمنع مشاركة كلمة المرور عبر أي وسيلة كانت، بما في ذلك المراسلات الإلكترونية، والاتصالات الصوتية، والكتابة الورقية. كما يجب على جميع المستخدمين عدم الكشف عن كلمة المرور لأي طرف آخر بما في ذلك زملاء العمل وموظفو الإدارة العامة للاتصالات وتقنية المعلومات.

٦-٢ يجب تغيير كلمة المرور، عند تزويدك بكلمة مرور جديدة من قبل مسؤول النظام.

انتهى،،