جامعة بيشة
University of Bisha
إدارة الأمن السيبراني

إدارة الأمن السيبراني

السياسة العامة للأمن السيبراني

التاريخ:	02/03/2021
الإصدار:	1.2
المرجع:	الضوابط الأساسية للأمن السيبراني (ECC-2: 2024) الضابط الأساسي رقم ١-٨

١- يجب على إدارة الأمن السيبراني تحديد وتطوير سياسات الأمن السيبراني، المعايير التقنية، الأطر التنظيمية، الإجراءات والمنهجيات، بناءً على نتائج تقييم المخاطر، وبشكل يضمن نشر متطلبات الأمن السيبراني، والتزام جامعة بيشة بها، وذلك وفقًا لمتطلبات الأعمال التنظيمية لجامعة بيشة، والمتطلبات التشريعية والتنظيمية ذات العلاقة. كما يجب اعتماد السياسة من قبل رئيس الجامعة ونشرها للعاملين المعنيين في جامعة بيشة والأطراف ذات العلاقة عليها، والمتمثلة في:

١-١ استراتيجية الأمن السيبراني (**Cybersecurity Strategy**) لضمان خطط العمل للأمن السيبراني والأهداف والمبادرات والبرامج والمشاريع وفعاليتها داخل جامعة بيشة لتحقيق الأهداف الاستراتيجية والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-١ سياسات وإجراءات الأمن السيبراني (**Cybersecurity Policies and Procedures**) لضمان توثيق ونشر متطلبات الأمن السيبراني والتزام جامعة بيشة بها، وذلك وفقًا لمتطلبات الأعمال التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٣-١ أدوار ومسؤوليات الأمن السيبراني (**Cybersecurity Roles and Responsibilities**) لضمان تحديد أدوار ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني في جامعة بيشة.

٤-١ منهجية إدارة مخاطر الأمن السيبراني (**Cybersecurity Risk Management**) لضمان إدارة المخاطر السيبرانية على نحو ممنهج يهدف إلى حماية الأصول المعلوماتية والتقنية لجامعة بيشة، وذلك وفقًا للسياسات والإجراءات التنظيمية لجامعة بيشة والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٥-١ برنامج التوعية والتدريب بالأمن السيبراني (**Cybersecurity Awareness and Training Program**) للتأكد من أن العاملين بجامعة بيشة لديهم الوعي الأمني اللازم، وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني، مع التأكد من تزويد العاملين بجامعة بيشة بالمهارات والمؤهلات والدورات التدريبية المتخصصة في مجال العاملين والمطلوبة في مجال الأمن السيبراني؛ لحماية الأصول المعلوماتية والتقنية لجامعة بيشة والقيام بمسؤولياتهم تجاه الأمن السيبراني.

٦-١ سياسة الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية (**Cybersecurity in Information Technology Projects**) للتأكد من أن متطلبات الأمن السيبراني مضمنة في منهجية إدارة مشاريع جامعة بيشة وإجراءاتها لحماية السرية، وسلامة الأصول المعلوماتية والتقنية لجامعة بيشة وضمان دقتها وتوافرها، وكذلك التأكد من تطبيق معايير الأمن السيبراني في أنشطة تطوير التطبيقات والبرامج، وفقًا للسياسات والإجراءات التنظيمية لجامعة بيشة والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٧-١ سياسة الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني (**Regulatory Cybersecurity Compliance**) للتأكد من أن برنامج الأمن السيبراني لدى جامعة بيشة متوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٨ سياسة المراجعة والتدقيق الدوري للأمن السيبراني (**Cybersecurity Periodical Assessment and Audit**) للتأكد من أن ضوابط الأمن السيبراني لدى جامعة بيشة مطبقة، وتعمل وفقًا للسياسات والإجراءات التنظيمية لجامعة بيشة، والمتطلبات التشريعية التنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المُقرة تنظيميًا على جامعة بيشة.

١-٩ سياسة الأمن السيبراني المتعلق بالموارد البشرية (**Cybersecurity in Human Resources**) للتأكد من أن مخاطر الأمن السيبراني ومتطلباته المتعلقة بالعاملين في جامعة بيشة تعالج بفعالية قبل بدء عملهم، وأثنائه وعند انتهائه، وذلك وفقًا للسياسات والإجراءات التنظيمية لجامعة بيشة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-١٠ سياسة إدارة الأصول وسياسة الاستخدام المقبول للأصول (**Asset Management and Asset Acceptable Use Policies**) للتأكد من أن جامعة بيشة لديها قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العلاقة لجميع الأصول المعلوماتية والتقنية المتاحة لجامعة بيشة، من أجل دعم العمليات التشغيلية لجامعة بيشة ومتطلبات الأمن السيبراني، لتحقيق سرية الأصول المعلوماتية والتقنية وسلامتها لجامعة بيشة ودقتها وتوافرها.

١-١١ سياسة إدارة هويات الدخول والصلاحيات ومعياره (**Identity and Access Management**) لضمان حماية الأمن السيبراني للوصول المنطقي (**Logical Access**) إلى الأصول المعلوماتية والتقنية لجامعة بيشة من أجل منع الوصول غير المصرح به، وتقييد الوصول إلى ما هو مطلوب لإنجاز الأعمال المتعلقة بجامعة بيشة.

١-١٢ سياسة حماية الأنظمة وأجهزة معالجة المعلومات (**Information System and Processing Facilities Protection**) لضمان حماية الأنظمة، وأجهزة معالجة المعلومات؛ بما في ذلك أجهزة المستخدمين، والبنى التحتية لجامعة بيشة من المخاطر السيبرانية.

١-١٣ سياسة حماية البريد الإلكتروني ومعياره (**Email Protection**) لضمان حماية البريد الإلكتروني لجامعة بيشة من المخاطر السيبرانية.

١-١٤ سياسة إدارة أمن الشبكات ومعياره (**Networks Security Management**) لضمان حماية شبكات جامعة بيشة من المخاطر السيبرانية.

١-١٥ سياسة أمن الخوادم (**Servers Security**) لضمان حماية خوادم جامعة بيشة من المخاطر السيبرانية.

١-١٦ سياسة إدارة حزم التحديثات والإصلاحات (**Patch Management**) لضمان ادارة حزم التحديثات والإصلاحات للأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة وأجهزة معالجة المعلومات الخاصة بجامعة بيشة وتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية.

١-١٧ سياسة أمن الأجهزة المحمولة ومعياره (**Mobile Devices Security**) لضمان حماية أجهزة جامعة بيشة المحمولة (بما في ذلك أجهزة الحاسب المحمول، والهواتف الذكية، والأجهزة الذكية اللوحية) من المخاطر السيبرانية. ولضمان التعامل بشكل آمن مع المعلومات المصنفة،

والمعلومات الخاصة بأعمال جامعة بيشة وحمايتها، أثناء النقل، التخزين، إزالة، وعند استخدام الأجهزة الشخصية للعاملين في جامعة بيشة (مبدأ "**BYOD**").

١-١٨ سياسة حماية البيانات والمعلومات ومعياره (**Data and Information Protection**) لضمان حماية سرية وسلامة بيانات ومعلومات جامعة بيشة ودقتها وتوافرها، وذلك وفقًا للسياسات والإجراءات التنظيمية لجامعة بيشة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-١٩ سياسة التشفير ومعياره (**Cryptography**) لضمان الاستخدام السليم والفعال للتشفير؛ لحماية الأصول المعلوماتية الإلكترونية لجامعة بيشة، وذلك وفقًا للسياسات، والإجراءات التنظيمية لجامعة بيشة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٢٠ سياسة أمن قواعد البيانات (**Database Security**) لضمان حماية قواعد البيانات لجامعة بيشة من المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية.

١-٢١ سياسة إدارة النسخ الاحتياطية ومعياره (**Backup and Recovery Management**) لضمان حماية بيانات جامعة بيشة ومعلوماتها، وكذلك حماية الإعدادات التقنية للأنظمة والتطبيقات الخاصة بجامعة بيشة من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقًا للسياسات والإجراءات التنظيمية لجامعة بيشة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٢٢ سياسة إدارة الثغرات ومعياره (**Vulnerabilities Management**) لضمان اكتشاف الثغرات التقنية في الوقت المناسب، ومعالجتها بشكل فعال، وذلك لمنع احتمالية استغلال هذه الثغرات في الهجمات السيبرانية في جامعة بيشة وتقليل ذلك، وكذلك تقليل الآثار المترتبة على أعمال جامعة بيشة.

١-٢٣ سياسة اختبار الاختراق ومعياره (**Penetration Testing**) لتقييم مدى فعالية أنظمة وفريق المراقبة في رصد التهديدات المحتملة واختباره في جامعة بيشة، وذلك من خلال محاكاة تقنيات الهجوم السيبراني الفعلية وأساليبه، ولاكتشاف نقاط الضعف الأمنية غير المعروفة ومدى فاعلية أنظمة وفريق المراقبة في رصد التهديدات المحتملة، والتي قد تؤدي إلى الاختراق السيبراني لجامعة بيشة؛ وذلك وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٢٤ سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني ومعياره (**Cybersecurity Event Logs and Monitoring Management**) لضمان جمع سجلات أحداث الأمن السيبراني بشكل آلي، وتحليلها، وتخزينها ومراقبتها في الوقت المناسب؛ من أجل الاكتشاف الاستباقي للهجمات السيبرانية، وإدارة مخاطرها بفعالية؛ لمنع الآثار السلبية المحتملة على أعمال جامعة بيشة أو تقليلها.

١-٢٥ سياسة إدارة حوادث وتهديدات الأمن السيبراني (**Cybersecurity Incident and Threat Management**) لضمان اكتشاف حوادث الأمن السيبراني وتحديدها في الوقت المناسب، وإدارتها بشكل فعّال، والتعامل مع تهديدات الأمن السيبراني استباقيًا، من أجل منع الآثار السلبية المحتملة أو تقليلها على أعمال جامعة بيشة.

١-٢٦ سياسة الحماية من البرمجيات الضارة (**Anti-Malware security**) لضمان حماية أجهزة المستخدمين والأجهزة المحمولة والخوادم الخاصة بجامعة بيشة من تهديدات البرمجيات الضارة.

١-٢٧ سياسة الأمن المادي ومعياره (**Physical Security**) لضمان حماية الأصول المعلوماتية والتقنية لجامعة بيشة من الوصول المادي غير المصرح به، والفقدان والسرقة والتخريب.

١-٢٨ سياسة حماية تطبيقات الويب ومعياره (**Web Application Security**) لضمان حماية تطبيقات الويب الداخلية والخارجية لجامعة بيشة من المخاطر السيبرانية.

١-٢٩ سياسة صمود الأمن السيبراني في إدارة استمرارية الأعمال (**Resilience Cybersecurity Aspects of Business Continuity Management**) لضمان توافر متطلبات صمود لأمن السيبراني في إدارة استمرارية أعمال جامعة بيشة، ولضمان معالجة الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحرجة وتقليلها لجامعة بيشة وأنظمة معالجة معلوماتها وأجهزتها جراء الكوارث الناتجة عن المخاطر السيبرانية.

١-٣٠ سياسة الأمن السيبراني المتعلقة بالأطراف الخارجية (**Third-Party Cybersecurity**) لضمان حماية أصول جامعة بيشة من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية (بما في ذلك خدمات الإسناد لتقنية المعلومات "**Outsourcing**" والخدمات المدارة "**Managed Services**") وفقًا للسياسات والإجراءات التنظيمية لجامعة بيشة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٣١ سياسة الأمن السيبراني المتعلقة بالحوسبة السحابية والاستضافة (**Cloud Computing and Hosting Cybersecurity**) لضمان معالجة المخاطر السيبرانية، وتنفيذ متطلبات الأمن السيبراني للحوسبة السحابية، والاستضافة بشكل ملائم وفعّال، وذلك وفقًا للسياسات والإجراءات التنظيمية لجامعة بيشة، والمتطلبات التشريعية والتنظيمية، والأوامر والقرارات ذات العلاقة. وضمان حماية الأصول المعلوماتية والتقنية لجامعة بيشة على خدمات الحوسبة السحابية، التي تتم استضافتها أو معالجتها، أو إدارتها بواسطة أطراف خارجية.

١-٣٢ سياسة الأمن السيبراني للبيانات (Data Cybersecurity) لتحديد متطلبات الأمن السيبراني المتعلقة بالأمن السيبراني للبيانات الخاصة بـ جامعة بيشة لتقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية وذلك لتحقيق الأهداف الرئيسية للحماية وهي: سرية المعلومات، وسلامة أنظمة المعلومات، وتوافرها.

٢- يحق لإدارة الأمن السيبراني الاطلاع على المعلومات، وجمع الأدلة اللازمة؛ للتأكد من الالتزام بالمتطلبات التشريعية والتنظيمية ذات العلاقة.

٣- يجب استخدام مؤشر قياس الأداء (**KPI**) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات حماية الأصول المعلوماتية والتقنية.

انتهى،،