# السياسة العامة للأمن السيبراني

مقيّد - داخلي

| | |
|---|---|
| التاريخ: | 10/01/2022 |
| الإصدار: | 1.2 |
| المرجع: | الهيئة الوطنية للأمن السيبراني |

متاح

# قائمة المحتويات

# السياسة العامة

## الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بتوثيق متطلبات الأمن السيبراني والتزام جامعة نجران بها، لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية، ويتم ذلك من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تهدف هذه السياسة إلى الالتزام بمتطلبات الأعمال التنظيمية الخاصة بـجامعة نجران، والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٣-١ والضابط رقم ١-٤-١ والضابط ١-٩-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

## نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية لـجامعة نجران وتنطبق على جميع العاملين في جامعة نجران.

وتعتبر هذه السياسة هي المحرك الرئيسي لجميع سياسات الأمن السيبراني وإجراءاته ومعاييره ذات المواضيع المختلفة، وكذلك أحد المدخلات لعمليات جامعة نجران الداخلية، مثل عمليات الموارد البشرية وعمليات إدارة الموردين وعمليات إدارة المشاريع وإدارة التغيير وغيرها.

## عناصر السياسة

١- يجب على إدارة الأمن السيبراني تحديد معايير الأمن السيبراني وتوثيق سياساته وبرامجه، بناءً على نتائج تقييم المخاطر، وبشكل يضمن نشر متطلبات الأمن السيبراني، والتزام جامعة نجران بها، وذلك وفقاً لمتطلبات الأعمال التنظيمية لـجامعة نجران، والمتطلبات التشريعية والتنظيمية ذات العلاقة. واعتمادها من قبل رئيس الجامعة أو من ينيبه. كما يجب إطلاع العاملين المعنيين في جامعة نجران والأطراف ذات العلاقة عليها.

٢- يجب على إدارة الأمن السيبراني تطوير سياسات الأمن السيبراني وبرامجه ومعاييره وتطبيقها، والمتمثلة في:

٢-١ **برنامج استراتيجية الأمن السيبراني (Cybersecurity Strategy)** لضمان خطط العمل للأمن السيبراني والأهـداف والمبادرات والمشاريع وفعاليتها داخل جامعة نجران في تحقيق المتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٢ **أدوار ومسؤوليات الأمن السيبراني (Cybersecurity Roles and Responsibilities)** لضمان تحديد مهمات ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني في جامعة نجران.

٢-٣ **برنامج إدارة مخاطر الأمن السيبراني (Cybersecurity Risk Management)** لضمان إدارة المخاطر السيبرانية على نحو ممنهج يهدف إلى حماية الأصول المعلوماتية والتقنية لـجامعة نجران،

وذلك وفقاً للسياسات والإجراءات التنظيمية لـجامعة نجران والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٤ **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 نجران وإجراءاتها لحماية السرية، وسلامة الأصول المعلوماتية والتقنية لـجامعة نجران وضمان دقتها وتوافرها، وكذلك التأكد من تطبيق معايير الأمن السيبراني في أنشطة تطوير التطبيقات والبرامج، وفقاً للسياسات والإجراءات التنظيمية لـجامعة نجران والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٥ **سياسة الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني (Cybersecurity Regulatory Compliance)** للتأكد من أن برنامج الأمن السيبراني لدى جامعة نجران متوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٦ **سياسة المراجعة والتدقيق الدوري للأمن السيبراني (Cybersecurity Periodical Assessment and Audit)** للتأكد من أن ضوابط الأمن السيبراني لدى جامعة نجران مطبقة، وتعمل وفقاً للسياسات والإجراءات التنظيمية لـجامعة نجران، والمتطلبات التشريعية التنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المُقرة تنظيمياً على جامعة نجران.

٢-٧ **سياسة الأمن السيبراني المتعلق بالموارد البشرية (Cybersecurity in Human Resources)** للتأكد من أن مخاطر الأمن السيبراني ومتطلباته المتعلقة بالعاملين (الموظفين والمتعاقدين) في جامعة نجران تعالج بفعالية قبل إنهاء عملهم، وأثنائه وعند انتهائه، وذلك وفقاً للسياسات والإجراءات التنظيمية لـجامعة نجران، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٨ **برنامج التوعية والتدريب بالأمن السيبراني (Cybersecurity Awareness and Training Program)** للتأكد من أن العاملين بـجامعة نجران لديهم الوعي الأمني اللازم، وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني، مع التأكد من تزويد العاملين بـجامعة نجران بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني؛ لحماية الأصول المعلوماتية والتقنية لـجامعة نجران والقيام بمسؤولياتهم تجاه الأمن السيبراني.

٢-٩ **سياسة إدارة الأصول (Asset Management)** للتأكد من أن جامعة نجران لديها قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العلاقة لجميع الأصول المعلوماتية والتقنية المتاحة لـجامعة نجران، من أجل دعم العمليات التشغيلية لـجامعة نجران ومتطلبات الأمن السيبراني، لتحقيق سرية الأصول المعلوماتية والتقنية وسلامتها لـجامعة نجران ودقتها وتوافرها.

٢-١٠ **سياسة إدارة هويات الدخول والصلاحيات (Identity and Access Management)** لضمان حماية الأمن السيبراني للوصول المنطقي (Access Logical) إلى الأصول المعلوماتية والتقنية لـجامعة نجران من أجل منع الوصول غير المصرح به، وتقييد الوصول إلى ما هو مطلوب لإنجاز الأعمال المتعلقة بـجامعة نجران.

٢-١١ **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 لـجامعة نجران من المخاطر السيبرانية.

٢-١٢ **سياسة حماية البريد الإلكتروني (Email Protection)** لضمان حماية البريد الإلكتروني لـجامعة نجران من المخاطر السيبرانية.

٢-١٣ **سياسة إدارة أمن الشبكات (Networks Security Management)** لضمان حماية شبكات جامعة نجران من المخاطر السيبرانية.

٢-١٤ **سياسة أمن الأجهزة المحمولة (Mobile Devices Security)** لضمان حماية أجهزة جامعة نجران المحمولة (بما في ذلك أجهزة الحاسب المحمول، والهواتف الذكية، والأجهزة الذكية اللوحية) من المخاطر السيبرانية. ولضمان التعامل بشكل آمن مع المعلومات الحساسة، والمعلومات الخاصة بأعمال جامعة نجران وحمايتها، أثناء النقل والتخزين، وعند استخدام الأجهزة الشخصية للعاملين في جامعة نجران (مبدأ "BYOD").

٢-١٥ **سياسة حماية البيانات والمعلومات (Data and Information Protection)** لضمان حماية السرية، وسلامة بيانات ومعلومات جامعة نجران ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية لـجامعة نجران، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-١٦ **سياسة التشفير ومعياره (Cryptography)** لضمان الاستخدام السليم والفعال للتشفير؛ لحماية الأصول المعلوماتية الإلكترونية لـجامعة نجران، وذلك وفقاً للسياسات، والإجراءات التنظيمية لـجامعة نجران، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-١٧ **سياسة إدارة النسخ الاحتياطية (Backup and Recovery Management)** لضمان حماية بيانات جامعة نجران ومعلوماتها، وكذلك حماية الإعدادات التقنية للأنظمة والتطبيقات الخاصة بـجامعة نجران من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقاً للسياسات والإجراءات التنظيمية لـجامعة نجران، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-١٨ **سياسة إدارة الثغرات ومعياره (Vulnerabilities Management)** لضمان اكتشاف الثغرات التقنية في الوقت المناسب، ومعالجتها بشكل فعال، وذلك لمنع احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية وتقليل ذلك، وكذلك تقليل الآثار المترتبة على أعمال جامعة نجران.

٢-١٩ **سياسة اختبار الاختراق ومعياره (Penetration Testing)** لتقييم مدى فعالية قدرات تعزيز الأمن السيبراني واختباره في جامعة نجران، وذلك من خلال محاكاة تقنيات الهجوم السيبراني الفعلية وأساليبه، ولاكتشاف نقاط الضعف الأمنية غير المعروفة، والتي قد تؤدي إلى الاختراق السيبراني لـجامعة نجران؛ وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٢٠ **سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني (Cybersecurity Event Logs and Monitoring Management)** لضمان جمع سجلات أحداث الأمن السيبراني، وتحليلها، ومراقبتها في الوقت المناسب؛ من أجل الاكتشاف الاستباقي للهجمات السيبرانية، وإدارة مخاطرها بفعالية؛ لمنع الآثار السلبية المحتملة على أعمال جامعة نجران أو تقليلها.

٢-٢١ **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 استباقياً، من أجل منع الآثار السلبية المحتملة أو تقليلها على أعمال جامعة نجران، مع مراعاة ما ورد في الأمر السامي الكريم ذو الرقم ٣٧١٤٠ والتاريخ ١٤٣٨/٨/١٤هـ.

٢-٢٢ **سياسة الأمن المادي (Physical Security)** لضمان حماية الأصول المعلوماتية والتقنية لـجامعة نجران من الوصول المادي غير المصرح به، والفقدان والسرقة والتخريب.

٢-٢٣ **سياسة حماية تطبيقات الويب ومعياره (Web Application Security)** لضمان حماية تطبيقات الويب الداخلية والخارجية لـجامعة نجران من المخاطر السيبرانية.

٢-٢٤ **جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال (Cybersecurity Resilience)** لضمان توافر متطلبات صمود الأمن السيبراني في إدارة استمرارية أعمال جامعة نجران، ولضمان معالجة الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحرجة وتقليلها لـجامعة نجران وأنظمة معالجة معلوماتها وأجهزتها جراء الكوارث الناتجة عن المخاطر السيبرانية.

٢-٢٥ **سياسة الأمن السيبراني المتعلقة بالأطراف الخارجية (Third-Party and Cloud Computing Cybersecurity)** لضمان حماية أصول جامعة نجران من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية (بما في ذلك خدمات الإسناد لتقنية المعلومات "Outsourcing" والخدمات المدارة "Managed Services") وفقاً للسياسات والإجراءات التنظيمية لـجامعة نجران، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٢٦ **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 وفقاً للسياسات والإجراءات التنظيمية لـجامعة نجران، والمتطلبات التشريعية والتنظيمية، والأوامر والقرارات ذات العلاقة. وضمان حماية الأصول المعلوماتية والتقنية لـجامعة نجران على خدمات الحوسبة السحابية، التي تتم استضافتها أو معالجتها، أو إدارتها بواسطة أطراف خارجية.

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

## الاستثناءات

يُمنع تجاوز سياسات الأمن السيبراني ومعاييره، دون الحصول على تصريح رسمي مسبق من إدارة الأمن السيبراني أو اللجنة الإشرافية للأمن السيبراني، ما لم يتعارض مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

# الأدوار والمسؤوليات

## الأدوار والمسؤوليات المتعلقة بالأمن السيبراني

### منسوبي الجامعة

| # | المسؤوليات |
|---|---|
| ١ | التعامل مع البيانات والمعلومات حسب مستوى تصنيفها. |
| ٢ | تلافي انتهاك حقوق أي شخص أو شركة محمية بحقوق النشر أو براءة الاختراع أو أي ملكية فكرية أخرى أو قوانين أو لوائح مماثلة. |
| ٣ | الالتزام بسياسات وإجراءات الأمن السيبراني. |
| ٤ | الالتزام بمتطلبات الأمن السيبراني المتعلقة بحماية أجهزة المستخدمين. |
| ٥ | الالتزام بمتطلبات الأمن السيبراني المتعلقة باستخدام الإنترنت والبرمجيات. |
| ٦ | الالتزام بمتطلبات الأمن السيبراني المتعلقة بالبريد الإلكتروني. |
| ٧ | الالتزام بالمتطلبات المتعلقة بنظم وتقنيات حماية الأمن السيبراني. |
| ٨ | استخدام جميع الأصول المعلوماتية والتقنية الخاصة بجامعة نجران لأغراض العمل فقط وحسب سياسة الاستخدام المقبول للأصول المعتمدة في جامعة نجران. |
| ٩ | الحصول على التصريح المطلوب من الإدارات ذات العلاقة قبل استضافة الزوار في المواقع الحساسة المحددة في جامعة نجران. |
| ١٠ | الإبلاغ عن حوادث الأمن السيبراني. |
| ١١ | الالتزام بسياسة الاستخدام المقبول. |

## الالتزام بالسياسة

١- يجب على صاحب الصلاحية ضمان الالتزام بسياسة الأمن السيبراني ومعاييره.

٢- يجب على إدارة الأمن السيبراني متابعة الالتزام بسياسات الأمن السيبراني ومعاييره بشكل دوري.

٣- يجب على جميع العاملين في جامعة نجران الالتزام بهذه السياسة.

٤- قد يُعرّض أي انتهاك للسياسات المتعلقة بالأمن السيبراني صاحب المخالفة إلى إجراءٍ تأديبي حسب الإجراءات المتبعة في جامعة نجران.