سياسات الأمن السيبراني بجامعة الباحة

الإصدار 3.0

المملكة العربية السعودية , الباحة . ص . ب (1988)
هاتف:966-17-7257700 فاكس:966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

معلومات الوثيقة

اعتماد الوثيقة

الدور	الاسم	التاريخ	التوقيع
المالك	وحدة الامن السيبراني	04/05/2021	وحدة الامن السيبراني
المُراجع	فريق أمن المعلومات ب وحدة الامن السيبراني	04/05/2021	وحدة الامن السيبراني
المصرّح	فريق أمن المعلومات ب وحدة الامن السيبراني	04/05/2021	وحدة الامن السيبراني
المعمِّد	وحدة الامن السيبراني	04/05/2021	وحدة الامن السيبراني

نسخ الوثيقة

النسخة	التاريخ	عُدلَ بواسطة	أسباب التعديل
1.0	12/01/2020	الهيئة الوطنية للأمن السيبراني	اصدار جديد
2.0	04/05/2021	فريق أمن المعلومات ب وحدة الامن السيبراني	اصدار جديد لموائمته مع متطلبات جامعة الباحة
3.0	01/05/2025	فريق وحدة الأمن السيبراني	نسخه محدثة
4.0	01/01/6202	فريق وحدة الأمن السيبراني	نسخة محدثة

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

قائمة المحتويات

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

السياسة العامة للأمن السيبراني

الأهداف

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

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأعمال التنظيمية الخاصة بجامعة الباحة، والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٣-١ من الضوابط الأساسية للأمن السيبراني ((ECC-2:2024 الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية لجامعة الباحة وتنطبق على جميع العاملين في جامعة الباحة.

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

عناصر السياسة

1- يجب على وحدة الامن السيبراني تحديد معايير الأمن السيبراني وتوثيق سياساته وبرامجه، بناءً على نتائج تقييم المخاطر، وبشكل يضمن نشر متطلبات الأمن السيبراني، والتزام جامعة الباحة بها، وذلك وفقاً لمتطلبات الأعمال التنظيمية لجامعة الباحة، والمتطلبات التشريعية والتنظيمية ذات العلاقة. واعتمادها من قبل وحدة الامن السيبراني . كما يجب إطلاع العاملين المعنيين في جامعة الباحة والأطراف ذات العلاقة عليها.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2- يجب على وحدة الامن السيبراني تطوير سياسات الأمن السيبراني وبرامجه ومعاييره وتطبيقها، والمتمثلة في:

2-1 **برنامج استراتيجية الأمن السيبراني (Cybersecurity Strategy)** لضمان خطط العمل للأمن السيبراني والأهداف والمبادرات والمشاريع وفعاليتها داخل جامعة الباحة في تحقيق المتطلبات التشريعية والتنظيمية ذات العلاقة.

2-2 **أدواروومسؤوليات الأمن السيبراني (Responsibilities Cybersecurity Roles and)** لضمان تحديد مهمات ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني في جامعة الباحة.

2-3 **برنامج إدارة مخاطر الأمن السيبراني (Cybersecurity Risk Management)** لضمان إدارة المخاطر السيبرانية على نحو ممنهج يهدف إلى حماية الأصول المعلوماتية والتقنية لجامعة الباحة، وذلك وفقاً للسياسات والإجراءات التنظيمية لجامعة الباحة والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-4 **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 الباحة وإجراءاتها لحماية السرية، وسلامة الأصول المعلوماتية والتقنية لجامعة الباحة وضمان دقتها وتوافرها، وكذلك التأكد من تطبيق معايير الأمن السيبراني في أنشطة تطوير التطبيقات والبرامج، وفقاً للسياسات والإجراءات التنظيمية لجامعة الباحة والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-5 **سياسة الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني (Regulatory Cybersecurity Compliance)** للتأكد من أن برنامج الأمن السيبراني لدى جامعة الباحة متوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

2-6 **سياسة المراجعة والتدقيق الدوري للأمن السيبراني (Assessment and Cybersecurity Periodical Audit)** للتأكد من أن ضوابط الأمن السيبراني لدى جامعة الباحة مطبقة، وتعمل وفقاً للسياسات والإجراءات التنظيمية لجامعة الباحة، والمتطلبات التشريعية التنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المُقرة تنظيمياً على جامعة الباحة.

2-7 **سياسة الأمن السيبراني المتعلق بالموارد البشرية (Resources Cybersecurity in Human)** للتأكد من أن مخاطر الأمن السيبراني ومتطلباته المتعلقة بالعاملين (الموظفين والمتعاقدين) في جامعة الباحة تعالج بفعالية

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

قبل إنهاء عملهم، وأثنائه وعند انتهائه، وذلك وفقاً للسياسات والإجراءات التنظيمية لجامعة الباحة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-8 **برنامج التوعية والتدريب بالأمن السيبراني (Training Program Cybersecurity Awareness and)** للتأكد من أن العاملين بجامعة الباحة لديهم الوعي الأمني اللازم، وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني، مع التأكد من تزويد العاملين بجامعة الباحة بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني؛ لحماية الأصول المعلوماتية والتقنية لجامعة الباحة والقيام بمسؤولياتهم تجاه الأمن السيبراني.

2-9 **سياسة إدارة الأصول (Asset Management)** للتأكد من أن جامعة الباحة لديها قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العلاقة لجميع الأصول المعلوماتية والتقنية المتاحة لجامعة الباحة، من أجل دعم العمليات التشغيلية لجامعة الباحة ومتطلبات الأمن السيبراني، لتحقيق سرية الأصول المعلوماتية والتقنية وسلامتها لجامعة الباحةودقتها وتوافرها.

2-10 **سياسة إدارة هويات الدخول والصلاحيات (Management Identity and Access)** لضمان حماية الأمن السيبراني للوصول المنطقي (Access Logical) إلى الأصول المعلوماتية والتقنية لجامعة الباحة من أجل منع الوصول غير المصرح به، وتقييد الوصول إلى ماهو مطلوب لإنجاز الأعمال المتعلقة بجامعة الباحة.

2-11 **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 الباحة من المخاطر السيبرانية.

2-12 **سياسة حماية البريد الإلكتروني (Email Protection)** لضمان حماية البريد الإلكتروني لجامعة الباحة من المخاطر السيبرانية.

2-13 **سياسة إدارة أمن الشبكات (Networks Security Management)** لضمان حماية شبكات جامعة الباحة من المخاطر السيبرانية.

2-14 **سياسة أمن الأجهزة المحمولة (Mobile Devices Security)** لضمان حماية أجهزة جامعة الباحة 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 الباحة وحمايتها، أثناء النقل والتخزين، وعند استخدام الأجهزة الشخصية للعاملين في جامعة الباحة (مبدأ "BYOD").

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2-15 **سياسة حماية البيانات والمعلومات (Data and Information Protection)** لضمان حماية السرية، وسلامة بيانات ومعلومات جامعة الباحة ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية لجامعة الباحة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-16 **سياسة التشفير ومعياره (Cryptography)** لضمان تطبيقات السليم والفعال للتشفير؛ لحماية الأصول المعلوماتية الإلكترونية لجامعة الباحة، وذلك وفقاً للسياسات، والإجراءات التنظيمية لجامعة الباحة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-17 **سياسة إدارة النسخ الاحتياطية (Backup and Recovery Management)** لضمان حماية بيانات جامعة الباحة ومعلوماتها، وكذلك حماية الإعدادات التقنية للأنظمة والتطبيقات الخاصة بجامعة الباحة من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقاً للسياسات والإجراءات التنظيمية لجامعة الباحة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-18 **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 الباحة.

2-19 **سياسة اختبار الاختراق ومعياره (Penetration Testing)** لتقييم مدى فعالية قدرات تعزيز الأمن السيبراني واختباره في جامعة الباحة، وذلك من خلال محاكاة تقنيات الهجوم السيبراني الفعلية وأساليبه، ولاكتشاف نقاط الضعف الأمنية غير المعروفة، والتي قد تؤدي إلى الاختراق السيبراني لجامعة الباحة؛ وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-20 **سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني (Logs and Monitoring Cybersecurity Event 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 الباحة أو تقليلها.

2-21 **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

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

تهديدات الأمن السيبراني استباقياً، من أجل منع الآثار السلبية المحتملة أو تقليلها على أعمال جامعة الباحة، مع مراعاة ما ورد في الأمر السامي الكريم ذو الرقم 37140 والتاريخ 14\8\1438هـ.

2-22 **سياسة الأمن المادي (Physical Security)** لضمان حماية الأصول المعلوماتية والتقنية لجامعة الباحة من الوصول المادي غير المصرح به، والفقدان والسرقة والتخريب.

2-23 **سياسة حماية تطبيقات الويب ومعياره (Web Application Security)** لضمان حماية تطبيقات الويب الداخلية والخارجية لجامعة الباحة من المخاطر السيبرانية.

2-24 **جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال (Resilience Cybersecurity)** لضمان توافر متطلبات صمود الأمن السيبراني في إدارة استمرارية أعمال جامعة الباحة، ولضمان معالجة الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحرجة وتقليلها لجامعة الباحة وأنظمة معالجة معلوماتها وأجهزتها جراء الكوارث الناتجة عن المخاطر السيبرانية.

2-25 **سياسة الأمن السيبراني المتعلقة بالأطراف الخارجية (Third-Party and Cloud Computing Cybersecurity)** لضمان حماية أصول جامعة الباحة من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية (بما في ذلك خدمات الإسناد لتقنية المعلومات "Outsourcing" والخدمات المدارة "Managed Services") وفقاً للسياسات والإجراءات التنظيمية لجامعة الباحة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-26 **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 لجامعة الباحة، والمتطلبات التشريعية والتنظيمية، والأوامر والقرارات ذات العلاقة. وضمان حماية الأصول المعلوماتية والتقنية لجامعة الباحة على خدمات الحوسبة السحابية، التي تتم استضافتها أو معالجتها، أو إدارتها بواسطة أطراف خارجية.

3- يحق لـ وحدة الامن السيبراني الاطلاع على المعلومات، وجمع الأدلة اللازمة؛ للتأكد من الالتزام بالمتطلبات التشريعية والتنظيمية ذات العلاقة المتعلقة بالأمن السيبراني.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

الأدوار والمسؤوليات

1- تُمثل القائمة الآتية مجموعة الأدوار والمسؤوليات اللازمة لإقرار سياسات الأمن السيبراني وإجراءاته، ومعاييره وبرامجه، وتنفيذها واتباعها:

1-1 مسؤوليات صاحب الصلاحية وحدة الامن السيبراني ، على سبيل المثال:

1-1-1 إنشاء لجنة إشرافية للأمن السيبراني ويكون عمادة التعلم الإلكتروني وتقنية المعلومات أحد أعضائها.

2-1 مسؤوليات إدارة الشؤون القانونية، على سبيل المثال:

1-2-1 التأكد من أن شروط ومتطلبات الامن السيبراني والمحافظة على سرية المعلومات (Non-disclosure Clauses) مُلزمة قانونياً في عقود العاملين في جامعة الباحة، والأطراف الخارجية.

3-1 مسؤوليات أدارة المراجعة الداخلية، على سبيل المثال:

1-3-1 مراجعة ضوابط الأمن السيبراني وتدقيق تطبيقها وفقاً للمعايير العامة المقبولة للمراجعة والتدقيق، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

4-1 مسؤوليات الإدارة العامة للموارد البشرية، على سبيل المثال:

1-4-1 تطبيق متطلبات الأمن السيبراني المتعلقة بالعاملين في جامعة الباحة.

5-1 مسؤوليات وحدة الامن السيبراني ، على سبيل المثال:

1-5-1 الحصول على موافقة وحدة الامن السيبراني على سياسات الأمن السيبراني، والتأكد من إطلاع الأطراف المعنية عليها وتطبيقها، ومراجعتها وتحديثها بشكل دوري.

6-1 مسؤوليات رؤساء الإدارات الأخرى، على سبيل المثال:

1-6-1 دعم سياسات الأمن السيبراني وإجراءاته ومعاييره وبرامجه، وتوفير جميع الموارد المطلوبة، لتحقيق الأهداف المنشودة، بما يخدم المصلحة العامة لجامعة الباحة.

7-1 مسؤوليات العاملين، على سبيل المثال:

1-7-1 المعرفة بمتطلبات الأمن السيبراني المتعلقة بالعاملين في جامعة الباحة، والالتزام بها.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

الالتزام بالسياسة

1- يجب على صاحب الصلاحية وحدة الامن السيبراني ضمان الالتزام بسياسة الأمن السيبراني ومعاييره.

2- يجب على وحدة الامن السيبراني التأكد من التزام جامعة الباحة بسياسات الأمن السيبراني ومعاييره بشكل دوري.

3- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في الإلتزام بهذه السياسة.

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

الاستثناءات

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

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة أدوار ومسؤليات الامن السيبراني

مقدمة

تم تطوير هذه الوثيقة لتحديد المسؤوليات الخاصة بتطبيق برامج ومتطلبات الأمن السيبراني ودعمه وتعزيزه في جامعة الباحة، ويجب على جميع الأطراف المشاركة في تطبيق برامج ومتطلبات الأمن السيبراني فهم أدوارهم والقيام بمسؤولياتهم المتعلقة بالأمن السيبراني في جامعة الباحة.

الأهداف

تهدف هذه الوثيقة إلى التأكد من أن جميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني في جامعة الباحة على دراية بمسؤولياتهم في تطبيق برامج ومتطلبات الأمن السيبراني في جامعة الباحة والجهات التابعة لها.

وتهدف هذه الوثيقة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٤-١ والضابط رقم ١-٩-١ من الضوابط الأساسية للأمن السيبراني (ECC-2:2024) الصادرة من الهيئة الوطنية للأمن السيبراني.

الأدوار والمسؤوليات المتعلقة بالأمن السيبراني

صاحب الصلاحية

#	المسؤوليات
1	تأسيس وحدة الامن السيبراني وضمان استقلاليتها لعدم تضارب المصالح، وتعيين وكيلا للإدارة المعينة بالأمن السيبراني ويجب أن يكون سعودي الجنسية.
2	تأسيس اللجنة الإشرافية للأمن السيبراني.
3	الموافقة على وثيقة اللجنة الإشرافية للأمن السيبراني.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

4	تخصيص الميزانية الكافية لمتطلبات الأمن السيبراني بما في ذلك ميزانية الموارد البشرية.
5	اعتماد استراتيجية الأمن السيبراني بعد رفعها للّجنة الإشرافية للأمن السيبراني.
6	اعتماد سياسات الأمن السيبراني بعد رفعها للّجنة الإشرافية للأمن السيبراني.
7	اعتماد حوكمة الأمن السيبراني ومنهجية إدارة المخاطر السيبرانية بعد رفعهما للّجنة الإشرافية للأمن السيبراني.
8	اعتماد منهجية إدارة المخاطر السيبرانية بعد رفعها للّجنة الإشرافية للأمن السيبراني.
9	الاطلاع على تقارير حالة الأمن السيبراني دورياً، وتوفيرالدعم المطلوب.

أعضاء اللجنة الإشرافية للأمن السيبراني

#	المسؤوليات
1	متابعة المبادئ (Principles) والمتطلبات التشغيلية وفقاً للوثيقة المنظمة للّجنة الإشرافية للأمن السيبراني.
2	ترسيخ مبادئ المساءلة والمسؤولية والصلاحية من خلال تحديد الأدوار والمسؤوليات بهدف حماية الأصول المعلوماتية والتقنية الخاصة بجامعة الباحة.
3	التأكد من وجود منهجية معتمدة لإدارة وتقييم المخاطر السيبرانية ومستوى المخاطر المقبول (Appetite Risk) لدى جامعة الباحة، ومراجعتها بشكل مستمر أو عند حدوث أي تغيير جوهري في مستوى المخاطر المقبول.
4	الموافقة على إجراءات مخاطر الأمن السيبراني ودعمها ومراقبتها.
5	الموافقة على حوكمة الأمن السيبراني ودعمها ومراقبتها.
6	مراجعة استراتيجية الأمن السيبراني لضمان توافقها مع الأهداف الاستراتيجية لجامعة الباحة قبل اعتمادها.
7	اعتماد تنفيذ استراتيجية الأمن السيبراني ودعمه ومراقبته.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

#	المسؤوليات
8	الموافقة على تطبيق سياسات الأمن السيبراني ودعمه ومراقبته.
9	اعتماد مبادرات ومشاريع الأمن السيبراني (مثل: برنامج التوعية بالأمن السيبراني، وحماية البيانات والمعلومات، وغيرها) ودعمها ومراقبتها.
10	الموافقة على مؤشرات الأداء (Key Performance Indicators "KPIs") ومتابعتها، والتأكد من فعاليتها لأعمال وحدة الامن السيبراني والعمل على رفع مستوى الأداء.
11	متابعة تقارير إدارة حزم البيانات والإعدادات ومراقبتها دورياً.
12	متابعة إدارة حوادث الأمن السيبراني ودعمها.
13	مراجعة التقارير الدورية الصادرة من وحدة الامن السيبراني والتي تشتمل على مشاريع الأمن السيبراني، والحالة العامة لوضع الأمن السيبراني، والمخاطر السيبرانية الداخلية التي قد تؤثر على عمل جامعة الباحة، وكذلك المخاطر السيبرانية الخارجية والتي قد تؤثر بشكل مباشر أو غير مباشر على أعمال جامعة الباحة، وتقديم الدعم اللازم لمواجهة تلك المخاطر.
14	مراجعة التقارير الخاصة بمخاطر الأمن السيبراني ومتابعة معالجتها وتقديم الدعم اللازم لمعالجتها أو العمل على تقليلها.
15	مراجعة التقارير الأمنية الخاصة بحوادث الأمن السيبراني وتقديم التوصيات بشأنها.
16	مراجعة طلبات الاستثناءات الخاصة بالأمن السيبراني وتقديم التوصيات بشأنها.
17	متابعة تقارير حالة حزم التحديثات والإصلاحات الأمنية، وتقييم الثغرات الأمنية على جميع الأصول التقنية والمعلوماتية والتأكد من معالجتها.
18	مراجعة نتائج تدقيق الأمن السيبراني الداخلي والخارجي، والتأكد من وجود خطة مناسبة لمعالجة الملاحظات المكتشفة ومتابعتها وتقديم الدعم اللازم لمعالجتها.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

#	المسؤوليات
19	رفع التقارير الدورية عن حالة الأمن السيبراني والدعم المطلوب لصاحب الصلاحية.
20	مراجعة حالة الالتزام بالمتطلبات الداخلية للجهة والمتطلبات التشريعية الصادرة من الهيئة الوطنية للأمن السيبراني.

وحدة الامن السيبراني

#	المسؤوليات
1	الإشراف على تطوير استراتيجية الأمن السيبراني وتحديثها.
2	الإشراف على تطوير وتنفيذ منهجيات وإجراءات مراقبة حوادث الأمن السيبراني، وتوجيه أنشطة الأمن السيبراني ومتابعتها بشكل مستمر ورفع التقارير الخاصة بها.
3	الإشراف على تطوير وتحديث منهجية وإجراءات إدارة مخاطر الأمن السيبراني.
4	التأكد من تطوير معايير وإجراءات الأمن السيبراني والموافقة عليها وتطبيقها.
5	الإشراف على تطوير سياسات الأمن السيبراني وتحديثها بناءً على متطلبات الأمن السيبراني.
6	التأكّد من توافق إدارة مخاطر الأمن السيبراني مع إدارة المخاطر في جامعة الباحة.
7	تقديم حلول وتوصيات حول الأمن السيبراني لتقليل المخاطر السيبرانية على الأصول المعلوماتية والتقنية.
8	تقديم التوجيهات والدعم اللازم ومعالجة المسائل المتعلقة بتخطيط وإدارة الموارد البشرية الخاصة بالأمن السيبراني (مثل: التوظيف والاحتفاظ بالموظفين والتدريب).
9	الإشراف على تحديد متطلبات الأمن السيبراني وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة والتأكد من الالتزام بها.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

#	المسؤوليات
10	الإشراف على حوادث الاستجابة للأمن السيبراني ورفع التقارير الخاصة بها.
11	الإشراف على التقييم المستمر للثغرات ومتابعة تطبيق حزم التحديثات الأمنية والإعدادات.
12	الإشراف على جمع وتحليل المعلومات الاستباقية المتعلقة بالأمن السيبراني من المصادر الوطنية أو المصادر الدولية.
13	الإشراف على إجراء اختبارات اختراق دورية على جميع الخدمات المقدمة خارجياً ومكوناتها التقنية لتقييم مستوى الأمن السيبراني.
14	الإشراف على إعداد مبادئ تصميم الأمن السيبراني، وتصاميم الأمن السيبراني للأنظمة والشبكات، ومعمارية الأمن السيبراني، مع ضمان المواءمة مع المعمارية المؤسسيةArchitecture (Enterprise).
15	الإشراف على إدارة الوصول المنطقي (Logical Access) إلى الأصول المعلوماتية والتقنية لجامعة الباحة من خلال تحديد متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في جامعة الباحة وتوثيقها وتطبيقها.
16	الإشراف على إعداد الميزانية الخاصة بتنفيذ مبادرات ومشاريع الأمن السيبراني.
17	التأكد من مراجعة متطلبات الأمن السيبراني دورياً.
18	توفير الدعم والإشراف على إعداد آلية مناسبة لقياس مؤشرات الأداء (KPIs) لأعمال الأمن السيبراني ومشاركتها مع اللجنة الإشرافية للأمن السيبراني.
19	التواصل مع الهيئة الوطنية للأمن السيبراني وإدارة العلاقة معها.
20	الإشراف على برامج الأمن السيبراني ومنها برنامج التوعية بالأمن السيبراني.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

موظفو وحدة الامن السيبراني

#	المسؤوليات
1	تطوير سياسات وإجراءات ومعايير الأمن السيبراني ومراجعتها سنوياً.
2	تحديد منهجية وإجراءات إدارة مخاطر الأمن السيبراني وتطبيقها ومراجعتها دورياً.
3	التأكد من تطبيق سياسات وإجراءات ومعايير الأمن السيبراني.
4	تطبيق عملية إدارة مخاطر الأمن السيبراني وتنفيذها.
5	إجراء تقييمات المخاطر، ومتابعة وضع المخاطر والإجراءات التي تم اتخاذها بالتنسيق مع أصحاب المصلحة.
6	تحديد المسؤوليات المتعلقة بالمخاطر بالتنسيق مع أصحاب المصلحة.
7	إعداد تقارير تقييم المخاطر واعتمادها من قبل وحدة الامن السيبراني .
8	تنفيذ برنامج الالتزام بالأمن السيبراني ومراجعته سنوياً.
9	تطوير برنامج التوعية والتدريب بالأمن السيبراني.
10	تطبيق برنامج التوعية والتدريب بالأمن السيبراني بالتنسيق مع الإدارة العامة للموارد البشرية وقياس مدى التزام العاملين بالتوعية بالأمن السيبراني.
11	إعداد تقارير الالتزام بمتطلبات الأمن السيبراني واعتمادها من قبل وحدة الامن السيبراني .
12	القيام بأنشطة المراقبة وإعداد التقارير المتعلقة بالالتزام بالأمن السيبراني.
13	توفير نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني (SIEM) ومراقبته.
14	متابعة أنظمة مراقبة الأمن السيبراني للتأكد من استقرارها وتوافرها، وتقديم تقارير لوصف حالتها.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

#	المسؤوليات
15	جمع أحداث الأمن السيبراني في الأصول المعلوماتية والتقنية في نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني (SIEM)، وتحليل السجلات، وتحديد مخاطر الأمن السيبراني.
16	التعامل مع حوادث الأمن السيبراني ومتابعة إغلاقها، وتصعيد الأحداث القائمة التي تتجاوز اتفاقية مستوى الخدمة المحددة.
17	التقييم المستمر للثغرات ومتابعة تطبيق حزم التحديثات الأمنية والإعدادات.
18	إجراء اختبارات اختراق دورية على جميع الخدمات المقدمة خارجياً ومكوناتها التقنية لتقييم مستوى الأمن السيبراني.
19	إعداد مبادئ تصميم الأمن السيبراني وتصاميم الأمن السيبراني للأنظمة والشبكات ومعمارية الأمن السيبراني، مع ضمان المواءمة مع المعمارية المؤسسية (Enterprise Architecture).
20	إدارة الوصول المنطقي (Logical Access) إلى الأصول المعلوماتية والتقنية لجامعة الباحة من خلال تحديد متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في جامعة الباحة وتوثيقها وتطبيقها.

عميد التعلم الإلكتروني وتقنية المعلومات

#	المسؤوليات
1	التأكد من التزام وحدة الامن السيبراني بجميع متطلبات الأمن السيبراني.
2	قيادة وتوجيه موظفي وحدة الامن السيبراني من خلال الإشراف على التدريب والتوعية والتثقيف بالأمن السيبراني تماشياً مع مسؤولياتهم.
3	المشاركة والمساهمة في تطوير إطار وإجراءات وعمليات إدارة المخاطر وتطبيقها.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

#	المسؤوليات
4	اعتماد وسائل يدوية (غير آلية) للتحديثات والإصلاحات في حال لم تكن الأدوات الآلية المستخدمة في جامعة الباحة مدعومة.
5	الإشراف والمتابعة الدورية لتنفيذ الحلول الآلية لإدارة حزم التحديثات والإصلاحات.
6	مراجعة فاعلية وكفاءة إدارة التحديثات والإصلاحات في الأنظمة الحساسة المتعلقة بتقنية المعلومات.
7	التأكد من إشراك وحدة الامن السيبراني في جميع المسائل المتعلقة بالأصول المعلوماتية والتقنية، وإدارة المشاريع، والمشتريات.
8	التأكد من إشراك وحدة الامن السيبراني لضمان حماية الأصول المعلوماتية والتقنية لجامعة الباحة على النحو المطلوب.
9	التأكّد من مراجعة عقود الصيانة الحالية مع موردي أنظمة تقنية المعلومات و/أو الأنظمة الحسّاسة لتزويد جامعة الباحة بأحدث الإصدارات من حزم التحديثات والإصلاحات.
10	الإشراف على سرعة تطبيق التوصيات للتقليل من مخاطر الأمن السيبراني.
11	الإشراف على إدارة عمليات التشغيل للأصول التقنية المتعلقة بالأمن السيبراني.

موظفو وحدة الامن السيبراني

#	المسؤوليات
1	تطبيق متطلبات الأمن السيبراني المتعلقة بـ وحدة الامن السيبراني ، بما في ذلك سياسات الأمن السيبراني وإجراءاته وعملياته ومعاييره وإرشاداته.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2	معالجة الثغرات ومتابعة تطبيق حزم التحديثات الأمنية والإعدادات.
3	تطبيق متطلبات الأمن السيبراني فيما يتعلق بطبيعة عمل الموظف المعني.
4	تصعيد أي أنشطة مشبوهة أو مخاوف تتعلق بالأمن السيبراني إلى وحدة الامن السيبراني والإبلاغ عنها.
5	المساعدة في تقديم مدخلات لأنشطة عمليات إطار إدارة المخاطر والوثائق ذات العلاقة.
6	التنسيق مع وحدة الامن السيبراني حول جميع المسائل المتعلقة بالأصول المعلوماتية والتقنية وإدارة المشاريع.
7	التنسيق مع وحدة الامن السيبراني لضمان حماية الأصول المعلوماتية والتقنية لجامعة الباحة وتأمينها على النحو المطلوب.
8	مراجعة عقود الصيانة الحالية مع موردي أنظمة تقنية المعلومات والأنظمة الحسّاسة للتأكد من تزويد جامعة الباحة بأحدث الإصدارات من حزم التحديثات والإصلاحات.

وكيل تقنية المعلومات

#	المسؤوليات
1	الإشراف على تنفيذ متطلبات الأمن السيبراني المتعلقة بتطوير التطبيقات في جامعة الباحة.
2	التنسيق مع فريق الأمن السيبراني حول المسائل المتعلقة بالأمن السيبراني التي تؤثر على وكالة تقنية المعلومات .
3	التأكد من تطبيق معايير الأمن السيبراني المعتمدة لتطوير التطبيقات، مثل (Application Security Open Web Project "OWASP").
4	الإشراف على تطبيق معايير وأدوات الاختبار الأمني (Testing Standards) والمعايير الأمنية لشفرة البرامج والتطبيقات (Coding Standards)، بما في ذلك الفحص العشوائي (Fuzzing) لأدوات التحليل الثابت للشفرات (Static Code Analysis) وإجراء مراجعات لشفرة البرامج والتطبيقات (Code Reviews).

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

#	المسؤوليات
5	تحديد حزم التحديثات والإصلاحات وتوثيقها والتأكد من سلامتها قبل تنصيبها.
6	التأكد من توثيق الشفرة المصدرية لعمليات التطوير الداخلية والخارجية (أي من خلال طرف خارجي) للتطبيقات في جامعة الباحة لتمكين عمليات التتبع والمراجعة في إدارة الثغرات.
7	التأكد من البرمجة الآمنة من خلال التأكد من معالجة الأخطاء وتحديد الأخطاء المحتملة في التشفير للحد من الثغرات.
8	التأكد من معالجة جميع الثغرات في مرحلة بيئة الاختبار (Software Acceptance Phase)، بما في ذلك معايير الإتمام (Completion Criteria)، وقبول المخاطر وتوثيقها، والمعايير المشتركة (Common Criteria)، وأساليب الاختبار المستقل (Independent Testing)، وإطلاع وحدة الامن السيبراني على جميع مشاريع تطوير التطبيقات.
9	التأكد من تحديد الخدمات والوظائف المتعلقة بالأمن السيبراني (مثل: التشفير، والتحكم بالوصول، وإدارة الهوية) واستخدامها للحد من فرص الاستغلال.

المعنيون بتطوير التطبيقات

#	المسؤوليات
بالإضافة إلى جميع المسؤوليات المذكورة لموظفي وحدة الامن السيبراني ، يتولّى المعنيون بتطوير التطبيقات المسؤوليات التالية:	
1	تنفيذ متطلبات الأمن السيبراني المتعلقة بتطوير التطبيقات في جامعة الباحة، واتباع المعايير والإجراءات المعتمدة في تطوير التطبيقات (مثل: معايير التطوير الآمن للتطبيقات).
2	متابعة عمليات إدارة المشاريع والتغييرات في جامعة الباحة، وذلك بالنسبة لجميع التغييرات التي تنطبق على التطبيقات الخاصة بجامعة الباحة.
3	تحديد التحديثات والإصلاحات اللازمة للبرامج وتوثيقها.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

#	المسؤوليات
4	إجراء البرمجة الآمنة، ومعالجة الأخطاء، وتحديد الأخطاء المحتملة في التشفير للحد من الثغرات.
5	تطبيق معايير وأدوات الاختبار الأمني والمعايير الأمنية لشفرة البرامج والتطبيقات، بما في ذلك الفحص العشوائي لأدوات التحليل الثابت للشفرات، وإجراء مراجعات لشفرة البرامج والتطبيقات.
6	تحديد وتوثيق التحديثات والإصلاحات اللازمة للبرامج، والإصدارات التي تكون خلالها البرامج عرضة للثغرات.

وكيل تقنية المعلومات

#	المسؤوليات
1	تنسيق فترات الصيانة حسب الأولوية وتخطيطها وتحديد موعدها من أجل تثبيت التحديثات والإصلاحات وفقاً لسياسة إدارة المشاريع والتغييرات المعتمدة في جامعة الباحة بما لا يؤثر على الأمن السيبراني للأصول.
2	الإشراف على الحلول الآلية لإدارة حزم التحديثات والإصلاحات، والتأكد من إجراء التحديثات اليدوية في حال كانت التحديثات والإصلاحات الآلية غير مدعومة.
3	الإشراف على النسخ الاحتياطية المنتظمة واختبارات النسخ الاحتياطية.
4	الإشراف على تنفيذ متطلبات الأمن السيبراني المتعلقة بعمليات تقنية المعلومات في جامعة الباحة.
5	التأكد من اختبار تحديثات وإصلاحات الأصول المعلوماتية والتقنية قبل النشر.
6	التأكد من نجاح تثبيت التحديثات والإصلاحات على الأنظمة.
7	التأكد من تنفيذ سياسات الأمن السيبراني المتعلقة بالأصول المعلوماتية والتقنية الخاصة بجامعة الباحة (مثل نموذج سياسة أمن أجهزة المستخدمين، ونموذج سياسة أمن الخوادم، وغيره).

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

#	المسؤوليات
8	تحديد وترتيب الأولويات والقدرات لاستعادة الأنظمة ووحدات الأعمال الأساسية اللازمة كلياً أو جزئياً بعد وقوع حدث كارثي يؤثر على الأنظمة واستمرارية الأعمال.
9	تحديد المستويات الملائمة لتوافر المعلومات في الأنظمة، وذلك استناداً إلى الوظائف الأساسية للنظام المعني، مع ضمان أن متطلبات النظام تحدد متطلبات التعافي من الكوارث واستمرارية الأعمال، بما في ذلك أي متطلبات موقع بديل (Fail-over Site)، ومتطلبات النسخ الاحتياطية، ومتطلبات القدرة على الدعم لاستعادة واسترداد النظام.
10	الإشراف على اختبار كفاءة خطة التعافي من الكوارث والمشاركة في اختبار كفاءة خطة استمرارية الأعمال.

المعنيون بعمليات تقنية المعلومات

#	المسؤوليات
بالإضافة إلى جميع المسؤوليات المذكورة لموظفي وحدة الامن السيبراني ، يتولّى المعنيون بعمليات تقنية المعلومات المسؤوليات التالية:	
1	المساعدة في التنسيق مع وحدة الامن السيبراني حول المسائل المتعلقة بالأمن السيبراني التي تؤثر على الإدارة المعنية بعمليات تقنية المعلومات.
2	تنفيذ متطلبات الأمن السيبراني المتعلقة بعمليات تقنية المعلومات في جامعة الباحة.
3	تنفيذ الحلول الآلية لإدارة حزم التحديثات والإصلاحات.
4	توفير النسخ الاحتياطية واختبارها دورياً.
5	تنفيذ الحلول الآلية لإدارة حزم التحديثات والإصلاحات، والتأكد من إجراء التحديثات اليدوية متى ما كانت التحديثات والإصلاحات الآلية غير مدعومة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

#	المسؤوليات
6	تفعيل وحماية السجلات المناسبة ودمجها مع نظام إدارة السجلات المركزي.
7	تهيئة جميع برامج الإدارة وبرامج الحماية ونظام التشغيل على الأصول المعلوماتية والتقنية.
8	الإشراف على صلاحيات الوصول وحسابات المستخدمين للأصول المعلوماتية والتقنية حسب السياسة الخاصة بها.
9	مراعاة عزل الأصول المعلوماتية والتقنية والتقسيم المنطقي لأجزاء الشبكات بشكل آمن.
10	المشاركة في إدارة التهديدات والحوادث في أنظمة تقنية المعلومات في المراحل المعنية بها (مثل: مراحل الاحتواء (Containment)، والاستئصال (Eradication)، والتعافي أو الاستعادة (Recovery)).
11	المساعدة في تحديد وترتيب أولويات قدرات الأنظمة ووحدات الأعمال الأساسية اللازمة لاستعادة النظام المعني كلياً أو جزئياً بعد وقوع حدث كارثي يتسبب في فشل متعلق بالأمن السيبراني.
12	المساعدة في تحديد المستويات الملائمة لتوافر المعلومات في الأنظمة، وذلك استناداً إلى الوظائف الأساسية للنظام المعني، مع ضمان أن متطلبات النظام تحدد متطلبات التعافي من الكوارث واستمرارية الأعمال، بما في ذلك أي متطلبات موقع بديل (Fail-over Site)، ومتطلبات النسخ الاحتياطية، ومتطلبات القدرة على الدعم لاستعادة النظام واسترداده.

مدير عام الإدارة العامة للموارد البشرية

#	المسؤوليات
1	الإشراف على تنفيذ متطلبات الأمن السيبراني المتعلقة بالموارد البشرية في جامعة الباحة.
2	التأكد من إجراء المسح الأمني للعاملين في وظائف الأمن السيبراني والوظائف التقنية ذات الصلاحيات الهامة والحساسة بالتنسيق مع الجهات المعنية.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

3	تولي المسؤولية المتعلقة بدعم تطبيق سياسة الاستخدام المقبول للأصول وتطبيق العقوبات على المخالفين حسب الإجراءات المعتمدة لدى جامعة الباحة.
4	تولي المسؤولية المتعلقة بسياسة الأمن السيبراني للموارد البشرية مما يترتب على تحديث السياسة ومراجعتها.
5	حضور اجتماعات اللجنة الإشرافية للأمن السيبراني والمشاركة بها حسب الضرورة.
6	المطالبة بالتمويل الكافي للموارد التدريبية المتعلقة بالأمن السيبراني، بما في ذلك الدورات الداخلية والدورات المتعلقة بالقطاع، والمدربين والمواد ذات الصلة.
7	إجراء تقييمات الاحتياجات التعليمية وتحديد المتطلبات المتعلقة بالأمن السيبراني.
8	التأكد من إعداد وتنفيذ أدوار ومسؤوليات وظيفية قياسية وفقاً للأدوار الوظيفية المحددة المتعلقة بالأمن السيبراني.
9	تحديد المسارات المهنية للأمن السيبراني لإتاحة الفرصة للنمو المهني والترقيات في المجالات المهنية المتعلقة بالأمن السيبراني.
10	التنسيق مع وحدة الامن السيبراني حول المسائل المتعلقة بالأمن السيبراني التي تؤثر على الإدارة العامة للموارد البشرية.
11	المشاركة في مراجعة استراتيجية وسياسات الأمن السيبراني وتقديم المدخلات لها.
12	التعامل مع مخالفات عدم الالتزام بسياسات الأمن السيبراني وذلك بالتنسيق مع إدارة الشؤون القانونية.

موظفو الإدارة العامة للموارد البشرية

#	المسؤوليات
1	تنفيذ متطلبات الأمن السيبراني المتعلقة بالموارد البشرية في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2	إجراء المسح الأمني للعاملين في وظائف الأمن السيبراني والوظائف التقنية ذات الصلاحيات الهامة والحساسة بالتنسيق مع الجهات المعنية.
3	إجراء تقييم للوعي الأمني لجميع العاملين وتحديد نقاط الضعف المتعلقة بالأمن السيبراني والعمل على معالجتها.
4	تنفيذ برنامج التوعية والتدريب بالأمن السيبراني بالتنسيق مع الإدارة المعنية بالتوعية والتدريب بالأمن السيبراني.
5	إعداد وتنفيذ أوصاف وظيفية قياسية وفقاً للأدوار الوظيفية المحددة المتعلقة بالأمن السيبراني.
6	المساعدة في تحديد المسارات المهنية للأمن السيبراني لإتاحة الفرصة للنمو المهني والترقيات في المجالات المهنية المتعلقة بالأمن السيبراني.
7	تقديم الدعم في المطالبة بالتمويل الكافي للموارد التدريبية المتعلقة بالأمن السيبراني، بما في ذلك الدورات الداخلية والدورات المتعلقة بالقطاع، والمدربين والمواد ذات الصلة.

مدير أدارة التدقيق الداخلية

#	المسؤوليات
1	الإشراف على المراجعة والتدقيق الدوري لبرامج ومتطلبات الأمن السيبراني وفقاً لمعايير التدقيق المتعارف عليها والمقبولة عموماً، والقوانين والتنظيمات ذات العلاقة.
2	الإشراف على تدقيق الأمن السيبراني وفقاً لشروط سياسة تدقيق ومراجعة الأمن السيبراني.
3	التأكد من المراجعة والتحديث الدوري لجميع الوثائق المتعلقة بالأمن السيبراني.
4	حضور اجتماعات اللجنة الإشرافية للأمن السيبراني والمشاركة بها حسب الضرورة.
5	التأكد من تحديث مخاطر الأمن السيبراني وإعادة تقييمها وفقاً لسياسة إدارة مخاطر الأمن السيبراني.
6	التأكد من مواءمة قبول المخاطر مع سياسة إدارة مخاطر الأمن السيبراني.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

#	المسؤوليات
7	اقتراح خطّة معالجة لنتائج وملاحظات التدقيق.
8	توثيق النتائج والملاحظات والإبلاغ عنها ومناقشتها مع الإدارة المعنية.
9	تقديم نتائج وملاحظات التدقيق إلى اللجنة الإشرافية المعنية بالأمن السيبراني.
10	مناقشة الإجراءات التصحيحية مع مسؤولي نتائج التدقيق وتوثيقها.
11	الإبلاغ عن أي ضوابط غير فعّالة متعلّقة بالأمن السيبراني.
12	الإبلاغ عن عدم الالتزام بمتطلبات الأمن السيبراني.
13	التنسيق مع فريق الأمن السيبراني حول المسائل المتعلقة بالأمن السيبراني التي تؤثر على الإدارة المعنية بالتدقيق الداخلي.
14	مراجعة استراتيجية وسياسات الأمن السيبراني وتقديم المدخلات لها.

موظفو أدارة التدقيق الداخلية

#	المسؤوليات
1	المساعدة في مراجعة وتدقيق تنفيذ ضوابط الأمن السيبراني وفقاً لمعايير التدقيق المتعارف عليها والمقبولة عموماً، والقوانين والتنظيمات ذات العلاقة.
2	تنفيذ متطلبات الأمن السيبراني المتعلقة بالتدقيق الداخلي في جامعة الباحة.
3	المراجعة والتحديث الدوري لجميع الوثائق المتعلقة بالأمن السيبراني.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

#	المسؤوليات
4	إجراء مراجعات للتأكّد من تحديث مخاطر الأمن السيبراني وإعادة تقييمها وفقاً لسياسة إدارة مخاطر الأمن السيبراني.
5	إجراء مراجعات للتأكد من مواءمة قبول المخاطرمع سياسة إدارة مخاطر الأمن السيبراني.
6	إجراء مراجعات وإبلاغ رئيس التدقيق الداخلي بعدم الالتزام بمتطلبات الأمن السيبراني.
7	تنفيذ عملية تدقيق الأمن السيبراني وفقاً لشروط سياسة تدقيق ومراجعة الأمن السيبراني.
8	تحليل الضوابط الفعالة للأمن السيبراني، وتقديم التوصيات لرئيس التدقيق الداخلي بشأنها.
9	اقتراح الإجراءات التصحيحية على رئيس التدقيق الداخلي وفقاً لنتائج وملاحظات التدقيق.
10	المساعدة في اقتراح خطّة معالجة لنتائج وملاحظات التدقيق.
11	المساعدة في التنسيق مع فريق الأمن السيبراني حول المسائل المتعلقة بالأمن السيبراني التي تؤثر على الإدارة المعنية بالتدقيق الداخلي.

إدارة الشؤون القانونية

#	المسؤوليات
1	حصر المتطلبات التنظيمية والتشريعية الوطنية ذات العلاقة بالأمن السيبراني، والاتفاقيات والالتزامات الدولية المعتمدة محلياً التي تتضمن متطلبات خاصة بالأمن السيبراني تنطبق على جامعة الباحة.
2	ترجمة ضوابط الأمن السيبراني وتنظيماته وسياساته ومعاييره وإجراءاته، وجعلها ملزمة قانونياً.
3	التأكد من أن الشروط والأحكام وبنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) ملزمة للموظفين وللأطراف الخارجية من أجل حماية الأصول المعلوماتية والتقنية لجامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

#	المسؤوليات
4	الإشراف على تنفيذ متطلبات الأمن السيبراني المتعلقة بالشؤون القانونية في جامعة الباحة.
5	حضور اجتماعات اللجنة الإشرافية للأمن السيبراني والمشاركة بها حسب الضرورة.
6	تقييم فعالية قوانين وتنظيمات الأمن السيبراني.
7	مراجعة سياسة أمن الأطراف الخارجية المعتمدة في جامعة الباحة وفقاً للمتطلّبات القانونية ذات العلاقة.
8	العمل مع وحدة الامن السيبراني حول المسائل المتعلقة بالأمن السيبراني التي تؤثر على الإدارة المعنية بالشؤون القانونية.
9	تقديم الدعم لحوادث الأمن السيبراني عند الحاجة.

موظفو إدارة الشؤون القانونية

#	المسؤوليات
1	المساعدة في تفسير قوانين الأمن السيبراني وتنظيماته وسياساته ومعاييره وإجراءاته وتطبيقها على مسائل محددة.
2	تنفيذ متطلبات الأمن السيبراني المتعلقة بالشؤون القانونية في جامعة الباحة.
3	المساعدة في تقييم فعالية قوانين وتنظيمات الأمن السيبراني.

جميع العاملين

#	المسؤوليات
1	التعامل مع البيانات والمعلومات حسب مستوى تصنيفها.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2	تلافي انتهاك حقوق أي شخص أو شركة محمية بحقوق النشر أو براءة الاختراع أو أي ملكية فكرية أخرى أو قوانين أو لوائح مماثلة.
3	الالتزام بسياسات وإجراءات الأمن السيبراني.
4	الالتزام بمتطلبات الأمن السيبراني المتعلقة بحماية أجهزة المستخدمين.
5	الالتزام بمتطلبات الأمن السيبراني المتعلقة باستخدام الإنترنت والبرمجيات.
6	الالتزام بمتطلبات الأمن السيبراني المتعلقة بالبريد الإلكتروني.
7	الالتزام بالمتطلبات المتعلقة بنظم وتقنيات حماية الأمن السيبراني.
8	استخدام جميع الأصول المعلوماتية والتقنية الخاصة بجامعة الباحة لأغراض العمل فقط وحسب سياسة الاستخدام المقبول للأصول المعتمدة في جامعة الباحة.
9	الحصول على التصريح المطلوب من وحدة الامن السيبراني أو صاحب الصلاحية في جامعة الباحة قبل استضافة الزوار في المواقع الحساسة المحددة في جامعة الباحة.
10	الإبلاغ عن حوادث الأمن السيبراني.
11	الالتزام بسياسة الاستخدام المقبول.

الأدوار والمسؤوليات

1- **راعي ومالك الوثيقة:** وحدة الامن السيبراني .

2- **مراجعة الوثيقة وتحديثها:** وحدة الامن السيبراني .

3- **تنفيذ الوثيقة وتطبيقها:** وحدة الامن السيبراني والإدارة العامة للموارد البشرية.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة الالتزام بتشريعات وتنظيمات الأمن السيبراني

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان التأكد من أن برنامج الأمن السيبراني لدى جامعة الباحة يتوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٧-١ من الضوابط الأساسية للأمن السيبراني ((ECC-2:2024الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأنظمة؛ والإجراءات الخاصة بجامعة الباحة، وتنطبق على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم من في جامعة الباحة.

بنود السياسة

1- يجب تحديد قائمة التشريعات والتنظيمات، المتعلقة بالأمن السيبراني، والمتطلبات ذات الصلة، وتوثيقها وتحديثها دورياً.

2- يجب توفير التقنيات اللازمة؛ للتحقق من الالتزام بمتطلبات الجهات التشريعية والتنظيمية، المتعلقة بالأمن السيبراني.

3- يجب مراجعة سياسات الأمن السيبراني وإجراءاته دورياً؛ لضمان التزامها بالمتطلبات التشريعية والتنظيمية، ذات العلاقة.

4- يجب التأكد من تطبيق سياسات الأمن السيبراني وإجراءاته دورياً.

5- يجب التأكد من الالتزام بالمتطلبات التشريعية والتنظيمية ذات العلاقة؛ بشكل دوري، عن طريق استخدام الأدوات المناسبة مثل:

5-1 أنشطة تقييم مخاطر الأمن السيبراني (Cybersecurity Risk Assessment).

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

5-2 أنشطة إدارة الثغرات (Vulnerabilities Management).

5-3 أنشطة اختبار الاختراقات (Penetration Test).

5-4 مراجعة معايير الأمن السيبراني.

5-5 المراجعة الأمنية للشفرة المصدرية (Security Source Code Review).

5-6 استبيانات المستخدمين.

5-7 المقابلات مع أصحاب المصلحة.

5-8 مراجعة الصلاحيات على النظام والشبكة.

5-9 مراجعة سجلات الأمن السيبراني وحوادثه.

6- يجب تحديد الإجراءات التصحيحية اللازمة والعمل على تطبيقها؛ لتصحيح الثغرات لجميع متطلبات الالتزام من قبل أصحاب العلاقة.

7- يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لبرنامج الالتزام.

8- يجب تنفيذ الإجراءات المناسبة؛ لضمان الالتزام بالمتطلبات التشريعية والتنظيمية، المتعلقة بحقوق الملكية الفكرية، واستخدام البرمجيات.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** وحدة الامن السيبراني .

2- **مراجعة السياسة وتحديثها:** وحدة الامن السيبراني .

3- **تنفيذ السياسة وتطبيقها:** وحدة الامن السيبراني .

الالتزام بالسياسة

1- يجب على وحدة الامن السيبراني ضمان التزام جامعة الباحة بهذه السياسة بشكل دوري.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في الإلتزام بهذه السياسة.

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة، إلى إجراء تأديبي؛ حسب الإجراءات المتبعة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة الأمن السيبراني ضمن استمرارية الأعمال

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير ضمن إدارة استمرارية الأعمال لضمان استمرارية أعمال وحدة الامن السيبراني بجامعة الباحه وحمايتها من المخاطر السيبرانية والتهديدات الداخلية والخارجية، ويتم ذلك من خلال التركيز على هدف التوافر وهو من الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم 3-1-1 من الضوابط الأساسية للأمن السيبراني (ECC-2:2024) والضابط رقم 3-1-1 من ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC-1:2019) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة إدارة استمرارية الأعمال الخاصة بالأمن السيبراني في وحدة الامن السيبراني بجامعة الباحه وتنطبق على جميع العاملين في جامعة الباحه.

بنود السياسة

1- يجب التأكد من استمرارية الأنظمة والإجراءات المتعلقة بالأمن السيبراني في وحدة الامن السيبراني بجامعة الباحه.

2- يجب إجراء تقييم للمخاطر التي قد تؤثر على استمرارية أعمال وحدة الامن السيبراني بجامعة الباحه.

3- يجب معالجة نقاط الضعف لتجنب الحوادث التي قد تؤثر على استمرارية أعمال وحدة الامن السيبراني بجامعة الباحه.

4- يجب تحديد المتطلبات التشريعية والتنظيمية الخاصة باستمرارية الأعمال لدى وحدة الامن السيبراني بجامعة الباحه.

5- يجب وضع خطط الاستجابة لحوادث الأمن السيبراني التي قد تؤثر على استمرارية أعمال وحدة الامن السيبراني بجامعة الباحه.

6- يجب وضع خطط التعافي من الكوارث (Disaster Recovery Plan).

7- يجب إدراج الأنظمة الحساسة لـ جامعة الباحه ضمن خطط التعافي من الكوارث.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

8- يجب إنشاء مركز للتعافي من الكوارث للأنظمة الحساسة.

9- يجب إجراء اختبارات دورية للتأكد من فعالية خطط التعافي من الكوارث للأنظمة الحساسة لـ جامعة الباحه مرة واحدة سنويًا على الأقل.

10- يجب إجراء اختبار دوري حي للتعافي من الكوارث (Live DR Test) للأنظمة الحساسة.

11- يجب تضمين حوادث الأمن السيبراني عالية الخطورة ضمن الأسباب الموجبة لتفعيل خطة استمرارية الأعمال في وحدة الامن السيبراني بجامعة الباحه.

12- يجب إجراء تحليل التأثير على الأعمال (Business Impact Analysis) لتحديد الأنظمة الحساسة في جامعة الباحه ونسخها إلى موقع التعافي من الكوارث.

13- يجب تحديد متطلبات النسخ الدورية الخاصة بالأنظمة الحساسة لـ جامعة الباحه إلى مركز التعافي.

14- يجب تضمين خطط استمرارية سلاسل التوريد والإمداد ضمن خطط استمرارية أعمال وحدة الامن السيبراني بجامعة الباحه.

15- يجب تضمين طرق التواصل الخاصة بفريق الأمن السيبراني في وحدة الامن السيبراني بجامعة الباحه سواءً الداخلية أو الخارجية وتوثيقها.

16- يجب تحديد الأدوار والمسؤوليات للأطراف ذات العلاقة باستمرارية الأعمال في وحدة الامن السيبراني بجامعة الباحه.

17- يجب وضع خطط تنفيذ ومتابعة المسؤوليات والأعمال الخاصة بالأمن السيبراني خلال الكوارث ولحين عودة الأوضاع لطبيعتها.

18- يجب إدارة هويات الدخول والصلاحيات على جميع الأنظمة والبيانات المستضافة في موقع التعافي من الكوارث الخاص بـ وحدة الامن السيبراني بجامعة الباحه لضمان عدم الوصول إليها من قبل الأشخاص غير المصرح لهم.

19- يجب تضمين متطلبات خطط التعافي من الكوارث في عقود واتفاقيات وحدة الامن السيبراني بجامعة الباحه مع الأطراف الخارجية ومقدمي الخدمات السحابية.

20- يجب ضمان تطبيق الضوابط الأساسية للأمن السيبراني (ECC-2:2024) في بيئة مركز التعافي من الكوارث التابع لـ جامعة الباحه مثل: الأمن المادي، أمن الشبكة والبنية التحتية، أمن البيانات والمعلومات، التشفير، إلخ.

21- يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لمتطلبات الأمن السيبراني الخاصة باستمرارية أعمال الأمن السيبراني.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

الأدوار والمسؤوليات

1- **راعي ومالك الوثيقة:** وحدة الامن السيبراني بجامعة الباحه .

2- **مراجعة الوثيقة وتحديثها:** وحدة الامن السيبراني بجامعة الباحه.

3- **تنفيذ الوثيقة وتطبيقها:** وحدة الامن السيبراني بجامعة الباحه بالتعاون مع وحدة الامن السيبراني , ووكالة العمادة لتقنية المعلومات, وكالة العمادة للتعلم الإلكتروني, وكالة العمادة لشطر الطالبات واي جهة داخلية بجامعة الباحه.

الالتزام بالسياسة

1- يجب على وحدة الامن السيبراني ضمان إلتزام جامعة الباحة بهذه السياسة بشكل دوري.

2- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في جامعة الباحه الإلتزام بهذه السياسة.

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة الإعدادات والتحصين

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية وتحصين وضبط إعدادات الأصول المعلوماتية والتقنية والتطبيقات الخاصة بجامعة الباحة لمقاومة الهجمات السيبرانية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٦-٢-٢ والضابط رقم ١-٦-٣-٥ من الضوابط الأساسية للأمن السيبراني ((ECC-2:2024 الصادرة عن الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية والتطبيقات الخاصة بجامعة الباحة، وتنطبق على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم من في جامعة الباحة.

بنود السياسة

1- يجب تحديد جميع الأصول المعلوماتية والتقنية المستخدمة داخل جامعة الباحة وكذلك التطبيقات والبرمجيات المعتمدة والتأكد من توفير معايير تقنية أمنية (Technical Security Standards) لها.

2- يجب تطوير وتوثيق واعتماد المعايير التقنية الأمنية الخاصة بجميع الأصول المعلوماتية والتقنية والتطبيقات والبرمجيات المصرح بها داخل جامعة الباحة.

3- يجب تحصين وضبط إعدادات أجهزة الحاسب الآلي، والأنظمة، والتطبيقات، وأجهزة الشبكات، والأجهزة الأمنية الخاصة بجامعة الباحة بما يتوافق مع المعايير التقنية الأمنية المعتمدة لمقاومة الهجمات السيبرانية.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

4- يجب استخدام إحدى الطرق التالية لتطوير المعايير الأمنية التقنية:

1-4 دليل الإعدادات والتحصين (Security Configuration Guidance) الخاص بالمُورد وذلك وفقاً للسياسات والإجراءات التنظيمية الخاصة بجامعة الباحة، والمتطلبات التشريعية والتنظيمية ذات العلاقة وأفضل الممارسات الدولية.

2-4 دليل الإعدادات والتحصين من مصادر موثوقة ومتوافقة مع المعايير المصنعية، مثل: مركز أمن الإنترنت (CIS)، ومعهد الأمن والشبكات وإدارة النظم (SANS)، والمعهد الوطني للمعايير والتقنية (NIST)، ووكالة أنظمة معلومات الدفاع (DISA)، ودليل التطبيق الفني الأمني (STIG)، وغيرها.

3-4 تطوير معايير أمنية تقنية خاصة بجامعة الباحة بما يتناسب مع طبيعة الأعمال وبما يتوافق مع دليل الإعدادات والتحصين الخاص بالمورد والمعايير المصنعية.

5- يجب أن تغطي الضوابط الخاصة بالمعايير التقنية الأمنية بحد أدنى ما يلي:

1-5 إيقاف أو تغيير الحسابات المصنعية والافتراضية.

2-5 منع تثبيت البرمجيات غير المرغوب بها.

3-5 تعطيل منافذ الشبكة غير المستخدمة.

4-5 تعطيل الخدمات غير المستخدمة.

5-5 تقييد استخدام وسائط الحفظ والتخزين الخارجي.

6-5 تغيير الإعدادات الافتراضية التي قد تُستغل في الهجمات السيبرانية.

6- يجب مراجعة الإعدادات والتحصين والتأكد من تطبيقها في الحالات التالية:

1-6 مراجعة الإعدادات والتحصين للأصول المعلوماتية والتقنية والتطبيقات دورياً والتأكد من تطبيقها وفقاً للمعايير التقنية الأمنية المعتمدة.

2-6 مراجعة الإعدادات والتحصين قبل إطلاق وتدشين المشاريع والتغييرات المتعلقة بالأصول المعلوماتية والتقنية.

3-6 مراجعة الإعدادات والتحصين قبل إطلاق وتدشين التطبيقات.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

4-6 مراجعة الإعدادات والتحصين لأنظمة التحكم الصناعي دورياً والتأكد من تطبيقها وفقاً للمعايير التقنية الأمنية المعتمدة.

7- يجب اعتماد صورة (Image) لإعدادات وتحصين الأصول المعلوماتية والتقنية الخاصة بجامعة الباحة وفقاً للمعايير التقنية الأمنية، وحفظها في مكان آمن.

8- يجب استخدام صورة (Image) معتمدة في تثبيت أو تحديث الأصول المعلوماتية والتقنية.

9- يجب توفير التقنيات اللازمة لإدارة الإعدادات والتحصين مركزياً، والتأكد من إمكانية تطبيق أو تحديث الإعدادات والتحصين تلقائياً لكافة الأصول المعلوماتية والتقنية في مواعيد زمنية محددة ومخطط لها.

10- يجب توفير نظام مراقبة الإعدادات المتوافقة مع «بروتوكول أتمتة المحتوى الأمني» (Security Content Automation Protocol "SCAP") للتأكد من أن الإعدادات متوافقة مع المعايير التقنية الأمنية المعتمدة ومطبقة بشكل كامل، كما يجب الإبلاغ عن أي تغييرات غير مصرّح بها.

11- يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لإدارة الإعدادات والتحصين.

12- يجب مراجعة متطلبات الأمن السيبراني المتعلقة بالإعدادات والتحصين للأصول المعلوماتية والتقنية والتطبيقات الخاصة بجامعة الباحة سنوياً، أو في حالة حدوث تغييرات في المتطلبات التشريعية أو التنظيمية أو المعايير ذات العلاقة.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** وحدة الامن السيبراني .

2- **مراجعة السياسة وتحديثها:** وحدة الامن السيبراني .

3- **تنفيذ السياسة وتطبيقها:** وحدة الامن السيبراني .

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

الالتزام بالسياسة

1- يجب على وحدة الامن السيبراني ضمان التزام جامعة الباحة بهذه السياسة دورياً.

2- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في الإلتزام بهذه السياسة.

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة الحماية من البرمجيات الضارة

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية أجهزة المستخدمين والأجهزة المحمولة والخوادم الخاصة بجامعة الباحة من تهديدات البرمجيات الضارة وتقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-٣-١ من الضوابط الأساسية للأمن السيبراني ((ECC-2:2024الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أجهزة المستخدمين والخوادم الخاصة بجامعة الباحة، وتنطبق على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم من في جامعة الباحة.

بنود السياسة

1- البنود العامة

1-1 يجب على جامعة الباحة تحديد تقنيات وآليات الحماية الحديثة والمتقدمة وتوفيرها والتأكد من موثوقيتها.

2-1 يجب تطبيق تقنيات وآليات الحماية لحماية أجهزة المستخدمين والأجهزة المحمولة والخوادم من البرمجيات الضارة (Malware) وإدارتها بشكل آمن.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

3-1 يجب التأكد من أن تقنيات وآليات الحماية قادرة على اكتشاف جميع أنواع البرمجيات الضارة المعروفة وإزالتها، مثل الفيروسات (Virus)، وأحصنة طروادة (Trojan Horse)، والديدان (Worms)، وبرمجيات التجسس (Spyware)، وبرمجيات الإعلانات المتسللة (Adware)، ومجموعة الجذر (Root Kits).

4-1 قبل اختيار تقنيات وآليات الحماية، يجب التأكد من ملاءمتها لأنظمة التشغيل الخاصة بجامعة الباحة مثل أنظمة ويندوز (Windows)، وأنظمة يونكس (UNIX)، وأنظمة لينكس (Linux)، ونظام ماك (Mac)، وغيرها.

5-1 في حال تسبب تحديث تقنيات الحماية بضرر للأنظمة أو متطلبات الأعمال، يجب التأكد من أن تقنيات الحماية قابلة للاسترجاع إلى النسخة السابقة.

6-1 يجب تقييد صلاحيات تعطيل التثبيت أو إلغائه أو تغيير إعدادات تقنيات الحماية من البرمجيات الضارة ومنحها لمشرفي نظام الحماية فقط.

2- إعدادات تقنيات وآليات الحماية من البرمجيات الضارة

1-2 يجب ضبط إعدادات تقنيات الحماية وآلياتها وفقاً للمعايير التقنية الأمنية المعتمدة لدى جامعة الباحة، مع الأخذ بالاعتبار إرشادات المورد وتوصياته.

2-2 يجب ضبط إعدادات برنامج مكافحة الفيروسات على خوادم البريد الإلكتروني لفحص جميع رسائل البريد الإلكتروني الواردة والصادرة.

3-2 لا يُسمح للأشخاص التابعين لأطراف خارجية بالاتصال بالشبكة أو الشبكة اللاسلكية لجامعة الباحة دون تحديث برنامج مكافحة الفيروسات وضبط الإعدادات المناسبة.

4-2 يجب ضمان توافر خوادم برامج الحماية من البرمجيات الضارة، كما يجب أن تكون البيئة الاحتياطية مناسبة لخوادم برامج الحماية من البرمجيات الضارة المخصصة للمهام والأعمال غير الحساسة.

5-2 يجب منع الوصول إلى المواقع الإلكترونية والمصادر الأخرى على الإنترنت المعروفة باستضافتها لبرمجيات ضارة وذلك باستخدام آلية تصفية محتوى الويب (Filtering Web Content).

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2-6 يجب مزامنة التوقيت (Clock Synchronization) مركزياً ومن مصدر دقيق وموثوق لجميع تقنيات وآليات الحماية من البرمجيات الضارة.

2-7 يجب ضبط إعدادات تقنيات الحماية من البرمجيات الضارة للقيام بعمليات التحقق من المحتوى المشبوه في مصادر معزولة مثل صندوق الفحص (Sandbox).

2-8 يجب القيام بعمليات مسح دورية لأجهزة المستخدمين والخوادم والتأكد من سلامتها من البرمجيات الضارة.

2-9 يجب تحديث تقنيات الحماية من البرمجيات الضارة تلقائياً عند توفر إصدارات جديدة من المورد، مع الأخذ بالاعتبار سياسة إدارة التحديثات والإصلاحات.

2-10 يجب توفير تقنيات حماية البريد الإلكتروني وتصفح الإنترنت من التهديدات المتقدمة المستمرة (APT Protection)، والتي تستخدم عادةً الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Malware)، وتطبيقها وإداراتها بشكل آمن.

2-11 يجب ضبط إعدادات تقنيات الحماية بالسماح لقائمة محددة فقط من ملفات التشغيل (Whitelisting) للتطبيقات والبرامج للعمل على الخوادم الخاصة بالأنظمة الحساسة. (CSCC-2-3-1-1)

2-12 يجب حماية الخوادم الخاصة بالأنظمة الحساسة عن طريق تقنيات حماية الأجهزة الطرفية المعتمدة لدى جامعة الباحة (End-point Protection). (CSCC-2-3-1-2)

2-13 يجب إعداد تقارير دورية حول حالة الحماية من البرمجيات الضارة يوضح فيها عدد الأجهزة والخوادم المرتبطة بتقنيات الحماية وحالتها (مثل: محدثة، أو غير محدثة، أو غير متصلة، إلخ)، ورفعها إلى وحدة الامن السيبراني .

2-14 يجب إدارة تقنيات الحماية من البرمجيات الضارة مركزياً ومراقبتها باستمرار.

3- متطلبات أخرى

3-1 يجب على وحدة الامن السيبراني التأكد من توافر الوعي الأمني اللازم لدى جميع العاملين للتعامل مع البرمجيات الضارة والتقليل من مخاطرها.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2-3 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لحماية أجهزة المستخدمين والخوادم من البرمجيات الضارة.

3-3 يجب مراجعة متطلبات الأمن السيبراني لحماية أجهزة المستخدمين والخوادم الخاصة بجامعة الباحة دورياً.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** وحدة الامن السيبراني .

2- **مراجعة السياسة وتحديثها:** وحدة الامن السيبراني .

3- **تنفيذ السياسة وتطبيقها:** عمادة التعلم الالكتروني وتقنية المعلومات و وحدة الامن السيبراني .

الالتزام بالسياسة

1- يجب على وحدة الامن السيبراني ضمان التزام جامعة الباحة بهذه السياسة دورياً.

2- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في الإلتزام بهذه السياسة

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة أمن الخوادم

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بالخوادم (Servers) الخاصة بجامعة الباحة لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-٣-١ من الضوابط الأساسية للأمن السيبراني ((ECC-2:2024الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الخوادم الخاصة بجامعة الباحة، وتنطبق على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم من في جامعة الباحة.

بنود السياسة

1- البنود العامة

1-1 يجب تحديد جميع الخوادم الخاصة بجامعة الباحة وتوثيقها، والتأكد من أن برمجيات الخوادم محدثة ومعتمدة.

2-1 يجب تطوير وتطبيق معايير تقنية أمنية (Technical Security Standards) للخوادم المستخدمة داخل جامعة الباحة باستخدام أفضل المعايير الدولية.

3-1 يجب ضبط إعدادات الخوادم وفقاً للمعايير التقنية الأمنية المعتمدة قبل تشغيل الخوادم في بيئة الإنتاج.

4-1 يجب توفير الحماية اللازمة لجميع الخوادم للسيطرة على مخاطر الأمن السيبراني ذات العلاقة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

5-1 يجب عمل نسخ احتياطية منتظمة للخوادم وفقاً لسياسة إدارة النسخ الاحتياطية المعتمدة في جامعة الباحة لضمان إمكانية استعادتها في حال تعرّضها لتلف أو حادث غير مقصود. (توصي الهيئة بعمل نسخ احتياطية يومياً للأنظمة الحساسة).

6-1 يجب تحديث برمجيات الخوادم بما في ذلك أنظمة التشغيل وبرامج التطبيقات وتزويدها بأحدث حزم التحديثات والإصلاحات الأمنية وفقاً لسياسة إدارة التحديثات والإصلاحات المعتمدة في جامعة الباحة.

2- إعدادات الخوادم

1-2 يجب اعتماد صورة (Image) لإعدادات وتحصين أنظمة تشغيل الخوادم الخاصة بجامعة الباحة وحفظها في مكان آمن وفقاً للمعايير التقنية الأمنية المعتمدة.

2-2 يجب استخدام صورة (Image) معتمدة لتثبيت أنظمة تشغيل الخوادم أو تحديثها.

3-2 يجب اعتماد إعدادات وتحصين الخوادم، ومراجعتها وتحديثها دورياً، وكل ستة أشهر على الأقل بالنسبة لخوادم الأنظمة الحساسة (CSCC-6-1-3-2).

3- الوصول والإدارة

1-3 يجب تقييد الوصول إلى الخوادم الخاصة بجامعة الباحة بحيث يكون الوصول متاحاً للمستخدمين المصرح لهم وعند الحاجة فقط.

2-3 يجب تقييد الدخول إلى الخوادم وحصره على حسابات مشرف في الأنظمة ومراجعة الحسابات والصلاحيات الممنوحة للمشرفين بشكل دوري.

3-3 يجب تقييد الوصول إلى الخوادم الخاصة بالأنظمة الحساسة وحصره على الفريق التقني ذي الصلاحيات الهامة وذلك عن طريق أجهزة حاسب (Workstations)، كما يجب عزل هذه الأجهزة في شبكة خاصة لإدارة الأنظمة (Management Network)، ومنع ارتباطها بأي شبكة أو خدمة أخرى (مثل خدمة البريد الإلكتروني والإنترنت).

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

4-3 يجب استخدام التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) للدخول إلى الخوادم الخاصة بالأنظمة الحساسة، مع تحديد عناصر التحقق المناسبة وعددها بناءً على تقييم الأثر المحتمل لفشل عملية التحقق (CSCC-3-1-2-2).

5-3 يجب إيقاف الحسابات المصنعية والافتراضية أو تغييرها، وإيقاف الخدمات غير المستخدمة، ومنافذ الشبكة غير المستخدمة في نظام التشغيل (Operating System).

6-3 يجب حماية البيانات المخزنة على الخوادم وتشفيرها بالتوافق مع ضوابط التشفير المعتمدة بناءً على تصنيفها وحسب المتطلبات التشريعية والتنظيمية ذات العلاقة. (ECC-2-8-3-3).

4- حماية الخوادم

1-4 يجب أن تُمنَع الخوادم غير المحدّثة أو غير الموثوقة من الاتصال بشبكة جامعة الباحة ووضعها في شبكة معزولة لأخذ التحديثات اللازمة لتقليل المخاطر السيبرانية ذات العلاقة والتي قد تؤدي إلى الوصول غير المصرّح به أو دخول البرمجيات الضارة أو تسرّب البيانات.

2-4 يجب استخدام تقنيات وآليات الحماية الحديثة والمتقدمة للحماية من الفيروسات (Virus) والبرامج والأنشطة المشبوهة والبرمجيات الضارة (Malware) وإدارتها بشكل آمن.

3-4 يجب السماح فقط بقائمة محددة من ملفات التشغيل (Whitelisting) للتطبيقات والبرامج للعمل على الخوادم الخاصة بالأنظمة الحساسة (CSCC-2-3-1-1).

4-4 يجب تقييد استخدام وسائط التخزين الخارجية على الخوادم، ويجب الحصول على إذن مسبق من وحدة الامن السيبراني قبل استخدامها، والتأكد من استخدامها بشكل آمن.

5-4 يجب تثبيت الخوادم في المنطقة المناسبة من مخطط/هيكل الشبكة حسب المتطلبات التشغيلية والتشريعية لها لضمان إدارتها وتطبيق الحماية اللازمة عليها بشكل فعّال.

5- المتطلبات التشغيلية لإدارة الخوادم

1-5 يجب إدارة الخوادم مركزياً في جامعة الباحة لكشف المخاطر بصورة أسرع، وتسهيل إدارة ومراقبة الخوادم مثل تقييد الوصول وتثبيت حزم التحديثات وغيرها.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2-5 يجب توفير الحماية اللازمة للخوادم التي تعمل في بيئة الأنظمة الافتراضية (Environment Virtual) وإدارتها بشكل آمن حسب تقييم المخاطر.

3-5 يجب ضبط إعدادات الخوادم وتفعيل إرسال سجلات الأحداث إلى نظام السجلات والمراقبة (SIEM) وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني.

4-5 يجب مزامنة توقيت جميع الخوادم مركزياً (Clock Synchronization) من مصدر دقيق وموثوق ومعتمد.

5-5 يجب توفير المتطلبات اللازمة لتشغيل الخوادم بشكل آمن وملائم، مثل توفير بيئة مناسبة وآمنة وتقييد الوصول المادي إلى منطقة الخوادم للعاملين المصرح لهم فقط ومراقبته.

6-5 يجب على وحدة الامن السيبراني مراقبة مكونات الخوادم التشغيلية والتأكد من فعالية أدائها، وتوافرها، وتوفير سعة تخزينية مناسبة، ونحو ذلك.

6- إدارة الثغرات واختبار الاختراق

1-6 يجب فحص الخوادم واكتشاف الثغرات الموجودة فيها ومعالجتها بناءً على تصنيف الثغرات المكتشفة والمخاطر السيبرانية المترتبة عليها دورياً، ومرة واحدة شهرياً على الأقل بالنسبة لخوادم الأنظمة الحساسة (CSCC-2-9-1-2).

2-6 يجب تنفيذ عمليات اختبار الاختراق على الخوادم دورياً، وكل ثلاثة أشهر على الأقل على خوادم الأنظمة الحساسة (CSCC-2-10-2).

3-6 يجب تثبيت حزم التحديثات والإصلاحات الأمنية لمعالجة الثغرات ورفع مستوى كفاءة الخوادم وأمنها، حسب سياسة إدارة التحديثات والإصلاحات.

7- الحماية المادية والبيئية للخوادم

1-7 يجب رصد ومراقبة الدخول والخروج من مرافق جامعة الباحة، على سبيل المثال الأبواب والأقفال.

2-7 يجب رصد ومراقبة العوامل البيئية كالتدفئة وتكييف الهواء والدخان وأجهزة إنذار الحريق وأنظمة إخماد الحرائق.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

3-7 يجب الالتزام بوضع الضوابط الأمنية المادية المناسبة (مثل كاميرات المراقبة داخل وخارج مركز بيانات جامعة الباحة، وحراس الأمن، وتأمين الكابلات، وغيرها).

8- متطلبات أخرى

1-8 يجب استخدام مؤشر قياس الأداء (Key Performance Indicator "KPI") لضمان التطوير المستمر لحماية الخوادم.

2-8 يجب مراجعة متطلبات الأمن السيبراني الخاصة بإدارة الخوادم سنوياً على الأقل، أو في حال حدوث تغييرات في المتطلبات التشريعية أو التنظيمية أو المعايير ذات العلاقة.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** وحدة الامن السيبراني .

2- **مراجعة السياسة وتحديثها:** وحدة الامن السيبراني .

3- **تنفيذ السياسة وتطبيقها:** عمادة التعلم الإلكتروني وتقنية المعلومات و وحدة الامن السيبراني .

الالتزام بالسياسة

1- يجب على وحدة الامن السيبراني ضمان التزام جامعة الباحة بهذه السياسة دورياً.

2- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في الإلتزام بهذه السياسة

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة أمن الشبكات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بأمن الشبكات الخاصة بجامعة الباحة لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-٥-١ من الضوابط الأساسية للأمن السيبراني ((ECC-2:2024الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الشبكات التقنية الخاصة بجامعة الباحة وتنطبق على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم من في جامعة الباحة.

بنود السياسة

1- البنود العامة

1-1 تحديد وتوثيق جميع أجهزة الشبكة داخل جامعة الباحة والتأكد من أن جميع الأجهزة محدثة ومعتمدة.

2-1 توثيق واعتماد معايير تقنية أمنية (Technical Security Standards) لجميع أجهزة الشبكة المستخدمة داخل جامعة الباحة.

3-1 إدارة صلاحيات الدخول إلى الشبكات الخاصة بجامعة الباحة وفقاً لسياسة إدارة هويات الدخول والصلاحيات، بحيث يكون الاتصال بالشبكة متوفراً عند الحاجة ومتاحاً للمستخدمين المصرح لهم فقط.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2- متطلبات الوصول إلى الشبكة

2-1 تطوير واعتماد إجراءات خاصة بمنح وإلغاء صلاحيات الدخول إلى الشبكة وذلك وفقاً لسياسة إدارة هويات الدخول والصلاحيات الخاصة بجامعة الباحة.

2-2 للحصول على صلاحية الدخول إلى الشبكة، يجب على المستخدم تقديم طلب إلى وحدة الامن السيبراني يوضح فيه نوع الطلب وفترة صلاحيته ومبرراته.

2-3 في حال إضافة أو التعديل على قوائم جدار الحماية، يجب على مسؤول الشبكة توثيق متطلبات الأعمال ومعلومات الطلب في نظام جدار الحماية.

2-4 يجب استخدام اسم المستخدم وكلمة المرور للدخول إلى الشبكة الخاصة بجامعة الباحة وذلك وفقاً لسياسة إدارة هويات الدخول والصلاحيات.

2-5 مراجعة إعدادات وقوائم جدار الحماية (Firewall Rules) دورياً، وكل ستة أشهر على الأقل للأنظمة الحساسة. (CSCC-2-4-1-2)

2-6 توفير الحماية اللازمة عند تصفح الإنترنت والاتصال به، وتقييد الدخول إلى المواقع الإلكترونية المشبوهة، ومواقع مشاركة تخزين الملفات، ومواقع الدخول عن بعد.

2-7 عدم ربط الشبكة اللاسلكية بالشبكة الداخلية لجامعة الباحة، إلا بناءً على دراسة متكاملة للمخاطر المترتبة على ذلك، والتعامل معها بما يضمن حماية الأصول التقنية الخاصة وسرية البيانات وسلامتها، وحماية النظم والتطبيقات المتصلة بجامعة الباحة.

2-8 يُمنع ربط الأنظمة الحساسة بالشبكة اللاسلكية لجامعة الباحة.

2-9 يجب توفير التقنيات اللازمة لوضع القيود وإدارة منافذ وبروتوكولات وخدمات الشبكة.

2-10 يمنع الربط المباشر لأي جهاز بالشبكة المحلية للأنظمة الحساسة قبل فحصه والتأكد من توافر عناصر الحماية المحققة للمستوى المقبول للأنظمة الحساسة (CSCC-2-4-1-3).

3- متطلبات وصول الأطراف الخارجية إلى الشبكة

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

1-3 يخضع منح صلاحية وصول الأطراف الخارجية إلى شبكة جامعة الباحة لمتطلبات الأمن السيبراني المشار إليها في سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية.

2-3 استخدام تقنيات تشفير ومصادقة آمنة لنقل البيانات من الأطراف الخارجية وإليها.

3-3 تحديد مدة زمنية معينة للأطراف الخارجية للدخول إلى شبكة جامعة الباحة.

4-3 مراجعة صلاحيات المستخدمين والأطراف الخارجية دورياً وذلك وفقًا لسياسات الأمن السيبراني المعتمدة في جامعة الباحة.

4- حماية الشبكات

1-4 يجب عزل وتقسيم الشبكات مادياً ومنطقياً باستخدام جدار الحماية (Firewall) ومبدأ الدفاع الأمني متعدد المراحل (Defense-in-Depth). (ECC-2-5-3-1)

2-4 تطبيق العزل المنطقي لشبكة الأنظمة الحساسة (VLAN).

3-4 تطبيق العزل المنطقي بين شبكة بيئة الإنتاج وشبكة بيئة الاختبار والشبكات الأخرى.

4-4 يمنع ربط الأنظمة الحساسة بالإنترنت في حال كانت هذه الأنظمة تقدم خدمة داخلية لجامعة الباحة ولا توجد هناك حاجة ضرورية جداً للدخول على الخدمة من خارج جامعة الباحة. (CSCC-2-4-1-6)

5-4 تطبيق العزل المنطقي بين شبكة الاتصالات الهاتفية عبر الإنترنت (Voice Over IP "VOIP") وشبكة البيانات.

6-4 تقييد استخدام منافذ الشبكة المادية في جميع مرافق جامعة الباحة وذلك باستخدام خاصية حماية المنافذ (Port Security) أو تقنية التحقق من الأجهزة (Port-Based Authentication) لحماية الشبكة من احتمالية ربط أجهزة غير مصرح بها أو أجهزة مشبوهة دون أن يتم كشفها.

7-4 توفير أنظمة الحماية في قناة تصفح الإنترنت للحماية من التهديدات المتقدمة المستمرة (APT Protection) التي تستخدم عادة الفيروسات والبرمجيات الضارة غير المتوقعة مسبقاً (Zero-Day Malware)، وإدارتها بشكل آمن.

8-4 يمنع اتصال الشبكة الداخلية بالإنترنت مباشرةً، ويكون الاتصال عن طريق استخدام موزع اتصالات الإنترنت (Proxy) لتحليل وتصفية البيانات المنتقلة من وإلى جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

9-4 ضبط إعدادات قوائم جدار الحماية بحيث تُحظر جميع أنواع الاتصالات بين أجزاء الشبكة تلقائياً (Explicitly)، ويتم إتاحة قوائم جدار الحماية بناءً على طلب المستخدم ومتطلبات الأعمال.

10-4 يجب توفير التقنيات اللازمة لأمن نظام أسماء النطاقات (DNS).

11-4 يجب توفير أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات (Intrusion Prevention Systems) على جميع أجزاء الشبكة وتحديثها دورياً.

12-4 يجب توفير أنظمة الحماية من التهديدات المتقدمة المستمرة على مستوى الشبكة (Network APT) على شبكة الأنظمة الحساسة.

13-4 يجب تطبيق آليات حماية قناة تصفح الإنترنت من التهديدات المتقدمة المستمرة (APT) والبرمجيات الضارة غير المعروفة مسبقاً وإدارتها بشكل آمن. (ECC-2-5-3-8)

5- يجب توفير وتطبيق أنظمة وآليات الحماية من هجمات تعطيل الشبكات (Distributed Denial of Service Attack "DDoS") على جميع الأنظمة والخدمات الخارجية لجامعة الباحة، مع تطوير خطط للاستجابة والتعافي من هذه الهجمات، وإجراء اختبارات دورية لضمان فعالية الحماية.

6- الأمن المادي والبيئي (ECC-9-3-5-2)

1-6 يجب حفظ أجهزة الشبكات في بيئة آمنة وملائمة، والتأكد من ضبط درجة الحرارة والرطوبة وكذلك وجود مصادر طاقة احتياطية مثل (Uninterruptible Power Supply "UPS").

2-6 يجب تقييد الدخول المادي إلى أجهزة الشبكات للمصرح لهم فقط لحفظ الأجهزة وحمايتها من السرقة أو العبث.

3-6 يجب حفظ سجلات الدخول ومراقبة مناطق أجهزة الشبكات الخاصة بالأنظمة الحساسة (CCTV) ومراجعتها دورياً.

7- متطلبات أخرى

1-7 يجب استخدام مؤشر قياس الأداء (Key Performance Indicator "KPI") لضمان التطوير المستمر لأمن الشبكات.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2-7 يجب مراجعة متطلبات الأمن السيبراني الخاصة بأمن الشبكات سنوياً على الأقل، أو في حال حدوث تغييرات في المتطلبات التشريعية أو التنظيمية أو المعايير ذات العلاقة.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** وحدة الامن السيبراني .

2- **مراجعة السياسة وتحديثها:** وحدة الامن السيبراني .

3- **تنفيذ السياسة وتطبيقها:** عمادة التعلم الالكتروني وتقنية المعلومات و وحدة الامن السيبراني .

الالتزام بالسياسة

1- يجب على وحدة الامن السيبراني ضمان التزام جامعة الباحة بهذه السياسة دورياً.

2- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في الإلتزام بهذه السياسة

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة أمن البريد الإلكتروني

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية البريد الإلكتروني لجامعة الباحة، وذلك من المخاطر السيبرانية والتهديدات الداخلية والخارجية، ويتم ذلك من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم 2-4-1 من الضوابط الأساسية للأمن السيبراني (ECC-2:2024)الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أنظمة البريد الإلكتروني الخاصة بجامعة الباحة وتنطبق على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم من في جامعة الباحة.

بنود السياسة

1- يجب توفير تقنيات حديثة لحماية البريد الإلكتروني وتحليل وتصفية (Filtering) رسائل البريد الإلكتروني وحظر الرسائل المشبوهة، مثل الرسائل الاقتحامية (Spam Emails) ورسائل التصيّد الإلكتروني (Phishing Emails).

2- يجب أن تستخدم أنظمة البريد الإلكتروني أرقام تعريف المستخدم وكلمات المرور مرتبطة، لضمان عزل اتصالات المستخدمين المختلفين.

3- يجب توفير التقنيات اللازمة لتشفير البريد الإلكتروني الذي يحتوي على معلومات مصنفة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

4- يجب تطبيق خاصية التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) للدخول عن بعد والدخول عن طريق صفحة موقع البريد الإلكتروني (Webmail) ، مع تحديد عناصر التحقق المناسبة وعددها بناءً على تقييم الأثر المحتمل لفشل عملية التحقق.

5- يجب أرشفة رسائل البريد الإلكتروني والقيام بالنسخ الاحتياطي دورياً.

6- يجب تحديد مسؤولية البريد الإلكتروني للحسابات العامة والمشتركة (Generic Account)

7- يجب توفير تقنيات الحماية اللازمة من الفيروسات، والبرمجيات الضارة غير المعروفة مسبقا (Zero-Day Protection) على خوادم البريد الإلكتروني؛ والتأكد من فحص الرسائل قبل وصولها لصندوق بريد المستخدم.

8- يجب توثيق مجال البريد الإلكتروني لجامعة الباحة عن طريق استخدام الوسائل اللازمة؛ مثل طريقة إطار سياسة المرسل (Sender Policy Framework) لمنع تزوير البريد الإلكتروني (Email Spoofing). كما يجب التأكد من موثوقية مجالات رسائل البريد الواردة (Incoming message DMARC verification).

9- يجب أن يقتصر الوصول إلى رسائل البريد الإلكتروني على منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في جامعة الباحة .

10- يجب اتخاذ الإجراءات اللازمة؛ لمنع استخدام البريد الإلكتروني لجامعة الباحة في غير أغراض العمل.

11- يمنع وصول مسؤول النظام (System Administrator) إلى معلومات البريد الإلكتروني الخاصة بأي من منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم دون الحصول على تصريح مسبق من صاحب الصلاحيه.

12- يجب تحديد حجم مرفقات البريد الإلكتروني الصادر والوارد، وسعة صندوق البريد لكل مستخدم. وكذلك العمل على الحد من إتاحة إرسال الرسائل الجماعية لعدد كبير من المستخدمين.

13- يجب تذييل رسائل البريد الإلكتروني المرسلة إلى خارج جامعة الباحة بإشعار إخلاء المسؤولية.

14- يجب تطبيق التقنيات اللازمة؛ لحماية سرية رسائل البريد الإلكتروني وسلامتها، وتوافرها أثناء نقلها وحفظها؛ ويجب أن تغطي متطلبات الأمن السيبراني للتشفير بحد أدنى المتطلبات المذكورة في المعايير الوطنية للتشفير الصادرة من الهيئة الوطنية للأمن السيبراني، مع تطبيق مستوى التشفير المناسب بحسب طبيعة ومستوى

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

حساسية البيانات والأنظمة والشبكات وبناءً على تقييم المخاطر.وتشمل هذه الإجراءات استخدام تقنيات التشفير وتقنيات منع تسريب البيانات.

15- يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لنظام البريد الإلكتروني.

16- يجب تعطيل خدمة تحويل البريد الإلكتروني من الخادم (Open Mail Relay).

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** وحدة الامن السيبراني بجامعة الباحه.

2- **مراجعة السياسة وتحديثها:** وحدة الامن السيبراني بجامعة الباحه.

3- **تنفيذ السياسة وتطبيقها:** وحدة الامن السيبراني بجامعة الباحه.

الإلتزام بالسياسة

1- يجب على وحدة الامن السيبراني ضمان إلتزام جامعة الباحة بهذه السياسة بشكل دوري.

2- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس في جامعة الباحة الإلتزام بهذه السياسة.

3- قد يُعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي؛ حسب الإجراءات المتبعة في جامعة الباحة .

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة أمن أجهزة المستخدمين والأجهزة المحمولة والشخصية

الأهداف

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لتقليل المخاطر السيبرانية الناتجة عن استخدام أجهزة المستخدمين (Workstations)، والأجهزة المحمولة (Devices Mobile)، والأجهزة الشخصية للعاملين (Bring Your Own Device "BYOD") داخل جامعة الباحة، وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي سرية المعلومات وسلامتها وتوافرها.

تتبع هذه السياسة المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهي متطلب تشريعي كما هو مذكور في الضوابط رقم ٢-٣-١ و٢-٦-١ من الضوابط الأساسية للأمن السيبراني (ECC-2:2024) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية للعاملين داخل جامعة الباحة وتنطبق على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم من في جامعة الباحة.

بنود السياسة

1- البنود العامة

1-1 يجب حماية البيانات والمعلومات المُخزّنة في أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD) حسب تصنيفها باستخدام الضوابط الأمنية المناسبة لتقييد الوصول إلى هذه المعلومات، ومنع العاملين غير المصرّح لهم من الوصول لها أو الاطلاع عليها.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2-1 يجب تحديث برمجيات أجهزة المستخدمين والأجهزة المحمولة، بما في ذلك أنظمة التشغيل والبرامج والتطبيقات، وتزويدها بأحدث حزم التحديثات والإصلاحات وذلك وفقاً لسياسة إدارة التحديثات والإصلاحات المعتمدة في جامعة الباحة.

3-1 يجب تطبيق ضوابط الإعدادات والتحصين (Configuration and Hardening) لأجهزة المستخدمين والأجهزة المحمولة وفقاً لمعايير الأمن السيبراني.

4-1 يجب عدم منح العاملين صلاحيات هامة وحساسة (Privileged Access) على أجهزة المستخدمين والأجهزة المحمولة، ويجب منح الصلاحيات وفقاً لمبدأ الحد الأدنى من الصلاحيات والامتيازات.

5-1 يجب حذف أو إعادة تسمية حسابات المستخدم الافتراضية في أنظمة التشغيل والتطبيقات.

6-1 يجب مزامنة التوقيت (Clock Synchronization) مركزياً ومن مصدر دقيق وموثوق لجميع أجهزة المستخدمين والأجهزة المحمولة.

7-1 يجب تزويد أجهزة المستخدمين والأجهزة المحمولة برسالة نصيّة (Banner) لإتاحة الاستخدام المصرّح به.

8-1 يجب السماح فقط بقائمة محددة من التطبيقات (Application Whitelisting) ومنع تسرّب البيانات (Data Leakage Prevention) واستخدام أنظمة مراقبة البيانات وغيرها.

9-1 يجب تشفير وسائط التخزين الخاصة بأجهزة المستخدمين والأجهزة المحمولة الهامة والحساسة والتي لها صلاحيات متقدمة وفقاً لمعيار التشفير المعتمد في جامعة الباحة.

10-1 يجب منع استخدام وسائط التخزين الخارجية، ويجب الحصول على إذن مسبق من وحدة الامن السيبراني لامتلاك صلاحية استخدام وسائط التخزين الخارجية.

11-1 يجب عدم السماح لأجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD) المزوّدة ببرمجيات غير محدثة أو منتهية الصلاحية (بما في ذلك أنظمة التشغيل والبرامج والتطبيقات) بالاتصال بشبكة جامعة الباحة لمنع التهديدات الأمنية الناشئة عن البرمجيات منتهية الصلاحية غير المحمية بحزم التحديثات والإصلاحات.

12-1 يجب أن تُمنَع أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD) غير المزوّدة بأحدث برمجيات الحماية من الاتصال بشبكة جامعة الباحة لتجنب حدوث المخاطر السيبرانية التي تؤدي إلى الوصول غير المصرّح به أو دخول البرمجيات الضارة أو تسرّب البيانات. وتتضمّن برمجيات الحماية برامج إلزامية، مثل: برامج

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

الحماية من الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة (Malware)، وجدار الحماية للمستضيف (Host-Based Firewall)، وأنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات في المستضيف (Host-based Intrusion Detection/Prevention)

13-1 يجب ضبط إعدادات أجهزة المستخدمين والأجهزة المحمولة غير المستخدمة بحيث تعرض شاشة توقّف محمية بكلمة مرور في حال عدم استخدام الجهاز (Session Timeout) لمدة 5 دقائق.

14-1 يجب إدارة أجهزة المستخدمين والأجهزة المحمولة مركزياً من خلال خادم الدليل النشط (Active Directory) الخاص بنطاق جامعة الباحة أو نظام إداري مركزي.

15-1 يجب ضبط إعدادات أجهزة المستخدمين والأجهزة المحمولة بإدارة الوحدات التنظيمية المناسبة (Domain Controller) لتطبيق السياسات الملائمة وتثبيت الإعدادات البرمجية اللازمة.

16-1 يجب تنفيذ سياسات النطاق المناسبة (Group Policy) في جامعة الباحة وتطبيقها في جميع أجهزة المستخدمين والأجهزة المحمولة لضمان التزام جامعة الباحة بالضوابط التنظيمية والأمنية.

2- متطلبات الأمن السيبراني لأمن أجهزة المستخدمين

1-2 يجب تخصيص أجهزة المستخدمين للفريق التقني ذي الصلاحيات الهامة، وأن تكون معزولة في شبكة خاصة لإدارة الأنظمة (Management Network) ولا ترتبط بأي شبكة أو خدمة أخرى.

2-2 يجب ضبط إعدادات أجهزة المستخدمين الهامة والحساسة والتي لها صلاحيات متقدمة لإرسال السجلات إلى نظام تسجيل ومراقبة مركزي وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني، مع عدم إمكانية إيقافه عن طريق المستخدم.

3-2 يجب تأمين أجهزة المستخدمين مادياً داخل مباني جامعة الباحة.

3- متطلبات الأمن السيبراني لأمن الأجهزة المحمولة

1-3 يجب منع وصول الأجهزة المحمولة إلى الأنظمة الحساسة إلا لفترة مؤقتة فقط، وذلك بعد إجراء تقييم المخاطر وأخذ الموافقات اللازمة من وحدة الامن السيبراني . (CSCC-2-5-1-1)

2-3 يجب تشفير أقراص الأجهزة المحمولة التي تملك صلاحية الوصول للأنظمة الحساسة تشفيراً كاملاً (Full Disk Encryption). (CSCC-2-5-1-2)

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

4- متطلبات الأمن السيبر اني لأمن الأجهزة الشخصية (BYOD)

1-4 يجب إدارة الأجهزة المحمولة مركزياً باستخدام نظام إدارة الأجهزة المحمولة (Mobile Device Management "MDM").

2-4 يجب فصل وتشفير البيانات والمعلومات الخاصة بجامعة الباحة المخزنة على الأجهزة الشخصية للعاملين (BYOD).

5- متطلبات أخرى

1-5 إجراء نسخ احتياطي دوري للبيانات المخزّنة على أجهزة المستخدمين والأجهزة المحمولة، وذلك وفقاً لسياسة النسخ الاحتياطية المعتمدة في جامعة الباحة.

2-5 تُحذَف بيانات جامعة الباحة المُخزّنة على الأجهزة المحمولة والأجهزة الشخصية (BYOD) في الحالات التالية:

- فقدان الجهاز المحمول أو سرقته.
- انتهاء أو إنهاء العلاقة الوظيفية بين المستخدم وجامعة الباحة.

3-5 يجب نشر الوعي الأمني للعاملين حول آلية استخدام الأجهزة ومسؤولياتهم تجاهها وفقاً لسياسة الاستخدام المقبول المعتمدة في جامعة الباحة وإجراء جلسات توعية خاصة بالمستخدمين ذوي الصلاحيات الهامة والحساسة.

4-5 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لحماية أجهزة المستخدمين والأجهزة المحمولة.

5-5 يجب مراجعة سياسة أمن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية سنوياً، وتوثيق التغييرات واعتمادها.

الأدوار والمسؤوليات

4- **راعي ومالك وثيقة السياسة:** وحدة الامن السيبراني .

5- **مراجعة السياسة وتحديثها:** وحدة الامن السيبراني .

6- **تنفيذ السياسة وتطبيقها:** وحدة الامن السيبراني .

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

الالتزام بالسياسة

1- يجب على وحدة الامن السيبراني ضمان التزام جامعة الباحة بهذه السياسة دورياً.

2- يجب على عمادة التعلم الالكتروني وتقنية المعلومات و وحدة الامن السيبراني في جامعة الباحة الالتزام بهذه السياسة.

قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة الاستخدام الآمن لمستخدمين تطبيقات الويب

مقدمة عامة عن السياسة

يُعد الاستخدام الآمن مجموعة من الإرشادات والقواعد التي تحدد كيفية استخدام الأنظمة الأكاديمية والمواقع الإلكترونية والتطبيقات الجامعية بشكل آمن وصحيح. تحتوي سياسة الاستخدام الآمن على مجموعة من القواعد التي يجب على أعضاء المجتمع الجامعي اتباعها، كاستخدام كلمات مرور قوية وتشغيل برامج مكافحة الفيروسات، ويجب على جميع المستخدمين الالتزام بتلك القواعد والحفاظ على الأمان والحماية في البيئة الأكاديمية.

1.2الهدف من السياسة

تهدف هذه السياسة إلى تحديد معايير الاستخدام الآمن وتقديم إرشادات إلى أعضاء المجتمع الجامعي حول الاستخدام الآمن للأنظمة الأكاديمية والتقنية، لضمان بيئة تعليمية قوية وموثوقة وآمنة، يمكن أن تخفف من المخاطر التي تتعرض لها معلومات الجامعة الأكاديمية والإدارية، والالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة.

1.3التعريفات

- **المجتمع الجامعي** :جميع الطلاب وأعضاء هيئة التدريس والموظفين والباحثين والزوار
- **الأنظمة الأكاديمية** :جميع الأنظمة التعليمية والإدارية التابعة للجامعة
- **المعلومات الأكاديمية** :البيانات التعليمية والبحثية والإدارية الخاصة بالجامعة
- **البوابة الأكاديمية** :النظام الموحد للوصول إلى الخدمات الجامعية الإلكترونية

1.4نطاق السياسة والتطبيق

تسري هذه السياسة على جميع المعلومات الأكاديمية والإدارية التي تحتفظ بها الجامعة سواء في شكل إلكتروني أو مادي بما في ذلك:

- جميع البيانات الأكاديمية والبحثية المنقولة

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

- الاتصالات الداخلية والخارجية للجامعة
- المواقع والتطبيقات الجامعية
- أنظمة إدارة التعلم الإلكتروني
- البوابات الأكاديمية والخدمات الطلابية

كما تسري هذه السياسة طوال دورة حياة جميع البيانات والمعلومات الأكاديمية بدءًا من الإنشاء والتخزين والاستخدام وحتى التخلص منها. ويشمل نطاق هذه السياسة جميع أعضاء المجتمع الجامعي من طلاب وأعضاء هيئة تدريس وموظفين وباحثين ومتعاقدين وخبراء ومستشارين وأعضاء الجهات الخارجية الذين قد يكون لديهم حق الوصول إلى المعلومات الأكاديمية أو معالجتها.

2. بنود السياسة

2.1أمن المعلومات الأكاديمية والشخصية

2.1.1

أُعدت سياسة الخصوصية الجامعية لمساعدة الطلاب وأعضاء هيئة التدريس والموظفين والزوار على تفهم طبيعة البيانات التي تُجمع منهم عند استخدام الأنظمة الأكاديمية وكيفية التعامل معها.

2.1.2

تتخذ إدارة تقنية المعلومات بالجامعة المسؤولة عن إدارة الأنظمة الأكاديمية والتقنية الإجراءات والتدابير المناسبة للحفاظ على المعلومات الأكاديمية والشخصية لضمان حمايتها من الفقدان ومنع الدخول غير المصرح به أو إساءة الاستخدام أو التعديل والإفصاح لغير المصرح لهم، ومن أهم التدابير المعمول بها في الجامعة:

- الإجراءات والتدابير المشددة لحماية أمن المعلومات الأكاديمية والبحثية
- التقنيات والبرامج التي تُستخدم لمنع عمليات الاحتيال والانتهاكات
- منع الدخول غير المصرح به إلى الأنظمة الأكاديمية
- التحديث المنتظم والدوري لإجراءات وضوابط الحماية
- احترام سرية المعلومات الأكاديمية والشخصية لأعضاء المجتمع الجامعي

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2.2جمع المعلومات الأكاديمية

2.2.1

عند استخدام أعضاء المجتمع الجامعي للأنظمة الأكاديمية، يقوم الخادم الخاص بالجامعة بتسجيل عنوان بروتوكول شبكة الإنترنت (IP) الخاص بالمستخدم، وتاريخ ووقت الاستخدام، والعنوان الخاص بأي موقع إلكتروني يُحال منه إلى الأنظمة الجامعية.

2.2.2

يجب استخدام خاصية ملفات ارتباط التعريف (Cookies) للأنظمة والتطبيقات الأكاديمية ومعالجتها أو نقلها بطريقة دقيقة وآمنة وفقاً لمتطلبات العمل الأكاديمي.

2.3استخدام الأنظمة الأكاديمية والتطبيقات التعليمية

تُعد الأنظمة الأكاديمية والتطبيقات التعليمية جزءاً أساسياً من البيئة التعليمية بالجامعة، وتحتوي على بنود إخلاء المسؤولية التي تتضمن تفاصيل واضحة ومحددة للالتزامات والمسؤوليات المتعلقة بهذه الأنظمة والتطبيقات الأكاديمية.

2.3.1الاستخدام المقبول للأنظمة الأكاديمية والتطبيقات التعليمية

- الأنظمة الأكاديمية والتطبيقات التعليمية متاحة لغرض الأنشطة التعليمية والبحثية والإدارية المشروعة
- يُعد الإقرار عند الوصول والدخول للبوابة الأكاديمية موافقة على بنود وشروط الاستخدام الأكاديمي ويجب الالتزام بها
- يتضمن استخدام البوابة الأكاديمية بنوداً وشروطاً تخضع لتحديثات مستمرة حسب متطلبات العمل الأكاديمي
- يصبح أي تعديل أو تحديث من هذه البنود والشروط نافذاً فور اعتماده من قبل إدارة تقنية المعلومات بالجامعة

2.3.2القيود على الاستخدام الأكاديمي

باستخدام الأنظمة الأكاديمية، يقر المستخدم بالامتناع عما يلي:

- تحميل ملفات تحتوي على برمجيات أو مواد غير مملوكة للمستخدم أو لا يملك ترخيصاً أكاديمياً بشأنها
- استخدام الأنظمة الأكاديمية لإرسال رسائل إلكترونية تجارية أو غير مرغوب فيها

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

- تحميل ملفات تحتوي على فيروسات أو بيانات تالفة على الأنظمة الأكاديمية
- نشر أو توزيع مواد تحتوي على تشويه للسمعة أو انتهاك للأنظمة الأكاديمية
- الاشتراك في أنشطة غير مشروعة أو غير قانونية من خلال الأنظمة الجامعية
- استخدام أي وسيلة أو برنامج لاعتراض التشغيل الصحيح للأنظمة الأكاديمية
- القيام بأي إجراء يفرض حملاً غير معقول على البنية التحتية للأنظمة الجامعية

2.3.3استخدام الروابط للأنظمة الأكاديمية

- يُمنع نقل أو نسخ محتويات الأنظمة الأكاديمية دون إذن مسبق من الجامعة
- يمكن وضع روابط خاصة بالأنظمة الأكاديمية في المواقع التعليمية والبحثية المعتمدة
- تحتفظ الجامعة بحق إيقاف أي ارتباط غير مناسب أو غير مصرح به
- لا تتحمل الجامعة مسؤولية المحتويات المتوفرة في المواقع الخارجية

2.3.4الحماية من الفيروسات والبرمجيات الخبيثة

- تبذل الجامعة جهوداً مستمرة لفحص واختبار محتويات الأنظمة الأكاديمية
- يُنصح بتشغيل برامج مضادة للفيروسات بشكل دائم على جميع الأجهزة المستخدمة
- لا تُعتبر الجامعة مسؤولة عن أي تلف قد يحدث للأجهزة أثناء استخدام الأنظمة الأكاديمية

2.3.5التنازل عن المطالبات

- تُوفر الأنظمة الأكاديمية والخدمات التعليمية "كما هي" دون أي ضمانات إضافية
- لا تضمن الجامعة عدم وجود انقطاعات أو أخطاء في الأنظمة الأكاديمية
- أي معلومات يرسلها المستخدم عبر الأنظمة الأكاديمية لا تضمن سريتها المطلقة

2.3.6حدود المسؤولية

- يجب الإحاطة بأن الاتصالات عبر الإنترنت قد تتعرض للتدخل أو الاعتراض
- استخدام الأنظمة الأكاديمية يتم على مسؤولية المستخدم الشخصية
- لا تكون الجامعة مسؤولة عن أي خسارة أو ضرر ناتج عن استخدام الأنظمة الأكاديمية

2.3.7التعويض

- باستخدام الأنظمة الأكاديمية، يقر المستخدم بعدم اتخاذ إجراءات تعويضية ضد الجامعة
- الجامعة غير مسؤولة عن أي مطالبات ناتجة عن إخلال المستخدم بالشروط والأحكام

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2.3.8إنهاء الاستخدام

- يجوز للجامعة إنهاء أو تقييد حق المستخدم في الوصول إلى الأنظمة الأكاديمية
- يتم الإنهاء في حالة مخالفة شروط الاستخدام أو أي سلوك غير مناسب أكاديمياً
- في حالة الإنهاء، لن يكون مصرحاً للمستخدم بالدخول إلى الأنظمة الأكاديمية

2.3.9حقوق الملكية الفكرية

- يُمنع منعاً باتاً أي تعديل لمحتويات الأنظمة الأكاديمية دون إذن مسبق
- المحتوى الأكاديمي والبحثي محمي بموجب حقوق النشر والملكية الفكرية
- لا يجوز استنساخ أو استغلال المحتوى الأكاديمي دون موافقة خطية من الجامعة

2.3.10المرجعية القضائية

يوافق المستخدم على الخضوع للسلطات القضائية بالمملكة العربية السعودية فيما يتعلق بكافة المطالبات والخلافات التي تنشأ عن استخدام الأنظمة الأكاديمية.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة الإستخدام المقبول للأصول

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني؛ لتقليل المخاطر السيبرانية، المتعلقة باستخدام أنظمة جامعة الباحة وأصولها، وحمايتها من التهديدات الداخلية والخارجية، والعناية بالأهداف الأساسية للحماية؛ وهي المحافظة على سرية المعلومة، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم 2-1-3 من الضوابط الأساسية للأمن السيبراني (ECC-2:2024)الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بجامعة الباحة وتنطبق على منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في جامعة الباحة.

بنود السياسة

1- البنود العامة

1-1 يجب التعامل مع المعلومات حسب التصنيف المحدد، وبما يتوافق مع سياسة تصنيف البيانات وسياسة حماية البيانات والمعلومات الخاصة بجامعة الباحة بشكل يضمن حماية سرية المعلومات وسلامتها وتوافرها.

2-1 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.

3-1 يجب عدم ترك المطبوعات على الطابعة المشتركة دون رقابة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

4-1 يجب حفظ وسائط التخزين الخارجية بشكل آمن وملائم، مثل التأكد من ضبط درجة الحرارة بدرجة معينة، وحفظها في مكان معزول وآمن.

5-1 يمنع استخدام كلمة المرور الخاصة بمستخدمين آخرين، بما في ذلك كلمة المرور الخاصة بمدير المستخدم أو مرؤوسيه.

6-1 يجب الالتزام بسياسة المكتب الآمن والنظيف، والتأكد من خلو سطح المكتب، وكذلك شاشة العرض من المعلومات المصنفة.

7-1 يمنع الإفصاح عن أي معلومات تخص جامعة الباحة، بما في ذلك المعلومات المتعلقة بالأنظمة والشبكات لأي جهة أو طرف غير مصرح له سواءً كان ذلك داخلياً أو خارجياً.

8-1 يُمنع نشر معلومات تخص جامعة الباحة عبر وسائل الإعلام، وشبكات التواصل الاجتماعي دون تصريح مسبق من صاحب الصلاحيه.

9-1 يُمنع استخدام أنظمة جامعة الباحة وأصولها بغرض تحقيق منفعة أو أعمال شخصية، أو تحقيق أي غرض لا يتعلق بنشاط وأعمال جامعة الباحة.

10-1 يُمنع ربط الأجهزة الشخصية بالشبكات، والأنظمة الخاصة بجامعة الباحة دون الحصول على تصريح مسبق، وبما يتوافق مع سياسة أمن الأجهزة المحمولة (BYOD).

11-1 يُمنع القيام بأي أنشطة تهدف إلى تجاوز أنظمة الحماية الخاصة بجامعة الباحة، بما في ذلك برامج مكافحة الفيروسات، وجدار الحماية، والبرمجيات الضارة دون الحصول على تصريح مسبق، وبما يتوافق مع الإجراءات المعتمدة لدى جامعة الباحة.

12-1 تحتفظ وحدة الامن السيبراني بجامعة الباحه بحقها في مراقبة الأنظمة والشبكات والحسابات الشخصية المتعلقة بالعمل، ومراجعتها دورياً لمراقبة الالتزام بسياسات الأمن السيبراني ومعاييره.

13-1 يُمنع استضافة أشخاص غير مصرح لهم بالدخول للأماكن الحساسه دون الحصول على تصريح مسبق.

14-1 يجب ارتداء البطاقة التعريفية للعاملين بالمنظمة في جميع مرافق جامعة الباحة.

15-1 يجب تبليغ وحدة الامن السيبراني في حال فقدان المعلومات أو سرقتها أو تسريبها.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2- حماية أجهزة الحاسب الآلي

2-1 يمنع استخدام وسائط التخزين الخارجية دون الحصول على تصريح مسبق من وحدة الامن السيبراني بجامعة الباحه .

2-2 يُمنع القيام بأي نشاط من شأنه التأثير على كفاءة الأنظمة والأصول وسلامتها دون الحصول على إذن مسبق من وحدة الامن السيبراني ، بما في ذلك الأنشطة التي تُمكّن المستخدم من الحصول على صلاحيات وامتيازات أعلى.

2-3 يجب تأمين الجهاز قبل مغادرة المكتب وذلك بقفل الشاشة، أو تسجيل الخروج (Sign out or Lock)، أو إغلاق الجهاز (Shut down) سواء كانت المغادرة لفترة قصيرة أو عند انتهاء ساعات العمل.

2-4 يُمنع ترك أي معلومات مصنفة في أماكن يسهل الوصول إليها، أو الاطلاع عليها من قبل أشخاص غير مصرح لهم.

2-5 يُمنع تثبيت أدوات خارجية على جهاز الحاسب الآلي دون الحصول على إذن مسبق من وحدة الامن السيبراني .

2-6 يجب تبليغ وحدة الامن السيبراني عند الاشتباه بأي نشاط قد يتسبب بضرر على أجهزة الحاسب الآلي الخاصة بجامعة الباحة أو أنظمتها أو أصولها.

3- الاستخدام المقبول للإنترنت والبرمجيات

3-1 يجب إبلاغ وحدة الامن السيبراني في حال وجود مواقع مشبوهة ينبغي حجبها؛ أو العكس.

3-2 يجب ضمان عدم انتهاك حقوق الملكية الفكرية أثناء تنزيل معلومات أو مستندات لأغراض العمل.

3-3 يُمنع استخدام البرمجيات غير المرخصة أو غيرها من الممتلكات الفكرية.

3-4 يجب استخدام متصفح آمن ومصرح به للوصول إلى الشبكة الداخلية أو شبكة الإنترنت.

3-5 يُمنع استخدام التقنيات التي تسمح بتجاوز الوسيط (Proxy) أو جدار الحماية (Firewall) للوصول إلى شبكة الإنترنت.

3-6 يُمنع تنزيل البرمجيات والأدوات أو تثبيتها على أصول جامعة الباحة دون الحصول على تصريح مسبق من عمادة التعلم الإلكتروني وتقنية المعلومات.

3-7 يُمنع استخدام شبكة الإنترنت في غير أغراض العمل، بما في ذلك تنزيل الوسائط والملفات واستخدام برمجيات مشاركة الملفات.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

8-3 يجب تبليغ وحدة الامن السيبراني عند الاشتباه بوجود مخاطر سيبرانية، كما يجب التعامل بحذر مع الرسائل الأمنية التي قد تظهر خلال تصفح شبكة الإنترنت أو الشبكات الداخلية.

9-3 يُمنع إجراء فحص أمني لغرض اكتشاف الثغرات الأمنية، ويشمل ذلك إجراء اختبار الاختراقات، أو مراقبة شبكات جامعة الباحة وأنظمتها، أو الشبكات والأنظمة الخاصة بالجهات الخارجية دون الحصول على تصريح مسبق من وحدة الامن السيبراني .

10-3 يُمنع استخدام مواقع مشاركة الملفات او التواقيع الإلكترونية دون الحصول على تصريح مسبق من من وحدة الامن السيبراني .

11-3 يُمنع زيارة المواقع المشبوهة بما في ذلك مواقع تعليم الاختراق.

4- الاستخدام المقبول للبريد الإلكتروني ونظام الاتصالات

1-4 يُمنع استخدام البريد الإلكتروني أو الهاتف أو الفاكس الإلكتروني في غير أغراض العمل، وبما يتوافق مع سياسات الأمن السيبراني ومعاييره.

2-4 يُمنع تداول رسائل تتضمن محتوى غير لائق أو غير أخلاقي أو غير مقبول، بما في ذلك الرسائل المتداولة مع الأطراف الداخلية والخارجية.

3-4 يجب استخدام تقنيات التشفير عند إرسال معلومات حساسة عن طريق البريد الإلكتروني أو أنظمة الاتصالات.

4-4 يجب عدم تسجيل عنوان البريد الإلكتروني الخاص بجامعة الباحة في أي موقع ليس له علاقة بالعمل.

5-4 يجب تبليغ وحدة الامن السيبراني عند الاشتباه بوجود رسائل بريد إلكتروني تتضمن محتوى قد يتسبب بأضرار لأنظمة جامعة الباحة أو أصولها.

6-4 تحتفظ جامعة الباحة ممثلة ب وحدة الامن السيبراني بحقها في كشف محتويات رسائل البريد الإلكتروني بعد الحصول على التصاريح اللازمة من صاحب الصلاحية وفقاً للإجراءات والتنظيمات ذات العلاقة.

7-4 يُمنع فتح رسائل البريد الإلكتروني والمرفقات المشبوهة أو غير المتوقعة حتى وإن كانت تبدو من مصادر موثوقة.

5- الاجتماعات المرئية والاتصالات القائمة على شبكة الإنترنت

1-5 يُمنع استخدام أدوات أو برمجيات غير مصرح بها لإجراء اتصالات أو عقد اجتماعات مرئية.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2-5 يُمنع إجراء اتصالات أو عقد اجتماعات مرئية لا تتعلق بالعمل دون الحصول على تصريح مسبق.

6- استخدام كلمات المرور

1-6 يجب اختيار كلمات مرور آمنة، والمحافظة على كلمات المرور الخاصة بأنظمة جامعة الباحة وأصولها. كما يجب اختيار كلمات مرور مختلفة عن كلمات مرور الحسابات الشخصية، مثل حسابات البريد الشخصي ومواقع التواصل الاجتماعي.

1-6 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 عمادة التعلم الإلكتروني وتقنية المعلومات و وحدة الامن السيبراني .

2-6 يجب تغيير كلمة المرور للإيميل او الأنظمة ذات العلاقه، عند تزويدك بكلمة مرور جديدة من قبل مسؤول النظام.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** وحدة الامن السيبراني بجامعة الباحه.

2- **مراجعة السياسة وتحديثها:** وحدة الامن السيبراني بجامعة الباحه.

3- **تنفيذ السياسة وتطبيقها:** وحدة الامن السيبراني وجميع العاملين بالعماده.

الالتزام بالسياسة

1- يجب على وحدة الامن السيبراني ضمان إلتزام جامعة الباحة بهذه السياسة بشكل دوري.

2- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في الإلتزام بهذه السياسة.

3- قد يُعرّض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي؛ حسب الإجراءات المُتبعة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة الحماية من هجمات حجب الخدمة الموزعة (DDoS Attacks)

الغرض

الغرض من هذا المعيار هو تحديد متطلبات الأمن السيبراني التفصيلية للحماية من هجمات حجب الخدمة الموزعة (DDoS) في جامعة الباحة وستساعد قدرة جامعة الباحة على تطبيق الضوابط المحددة في معيار الحماية من هجمات حجب الخدمة الموزعة (DDoS) في الحفاظ على توافر وسلامة وسرية معلومات جامعة الباحة وأصولها.

تمت مواءمة هذا المعيار مع متطلبات الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني، وتشمل على سبيل المثال لا الحصر: الضوابط الأساسية للأمن السيبراني (ECC – 1: 2018) وضوابط الأمن السيبراني للأنظمة الحساسة (CSCC – 1: 2019) وغيرها من المتطلبات التشريعية والتنظيمية ذات العلاقة.

نطاق العمل

يغطي هذا المعيار أفضل الممارسات المتبعة لدى جامعة الباحة في نشر واستخدام حل الحماية من هجمات حجب الخدمة الموزعة (DDoS)، وينطبق على جميع الأصول وجميع العاملين (الموظفين والمتعاقدين) في جامعة الباحة

المعايير

1	المتطلبات العامة (General Requirements)
الهدف	نشر حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) بشكل آمن واستخدامه بشكل مناسب عند الحاجة.
المخاطر المحتملة	قد يؤدي الخطأ في ضبط إعدادات حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) إلى عدم توفر خدمات الأعمال المقدمة للعملاء والخدمات الداخلية للشركة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

الإجراءات المطلوبة	
1-1	أن يقوم حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) بتوفير اتفاقية لمستوى الخدمة تنص على مدة مضمونة للحدّ من الهجمات (TTM). وهذا المتطلب مهم بشكل خاص عند نشر الحل كخدمة.
2-1	أن يوفر حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) الحماية لحزمتي بروتوكول الإنترنت الإصدار الرابع (IPv4) وبروتوكول الإنترنت الإصدار السادس (IPv6) على شبكة جامعة الباحة .
3-1	أن يكون هناك اتساق في وقت تشغيل التطبيق والتوافر بالنسبة لحل الحماية من هجمات حجب الخدمة الموزعة (DDoS).
4-1	أن يوفر حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) الحماية للشبكات ولخوادم نظام أسماء النطاقات (DNS) والمواقع الإلكترونية المتاحة للجمهور والمستضافة في بيئة تقنية المعلومات وبروتوكولات الإنترنت الفردية لدى جامعة الباحة .
5-1	أن يوفر حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) حماية متعددة الطبقات من الهجمات على طبقات الشبكة والتطبيقات ومن الهجمات الكمّية وغير الكمّية، إلى جانب التغطية الكاملة لهجمات حجب الخدمة الموزعة المعتمدة على بروتوكول طبقة المنافذ الآمنة (SSL) / بروتوكول أمن طبقة النقل (TLS).
6-1	أن يكون لجميع مديري نظام تقنية المعلومات لدى جامعة الباحة المحددين في مبادئ إدارة صلاحيات الوصول، والذين يحتاجون إلى الوصول إلى سجلات هجمات حجب الخدمة الموزعة (DDoS)، صلاحية وصول إلى قاعدة بيانات السجلات.
7-1	إتاحة نشر حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) بمختلف المنهجيات - الجدول "أ ".

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

8-1	تثبيت جميع التحديثات الأمنية لحل الحماية من هجمات حجب الخدمة الموزعة (DDoS) وفقًا لعملية إدارة التحديثات والإصلاحات.
9-1	أن تقوم جميع قنوات الاتصالات الإدارية باستخدام شبكة مخصصة للإدارة أو اتصالات عبر شبكة الإدارة بحيث تكون موثقة ومشفّرة باستخدام وحدات التشفير المعتمدة وفقًا لمعيار التشفير الوطني (National Cryptography Standard)ومعايير التشفير الداخلية المطبقة لدى جامعة الباحة . ويجب توفير الحماية في حالة الوصول إلى وحدة التحكم الإدارية كطريقة لنشر هجمات حجب الخدمة الموزعة كخدمة (DDoS as a Service).
10-1	وضع خطة للاستجابة لهجمات حجب الخدمة الموزعة (DDoS) والحدّ منها وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.
11-1	على جامعة الباحة تدريب العاملين فيها بصفة دورية لضمان معرفتهم بكيفية اختيار الخدمة المناسبة للحدّ من الهجمات، مع قياس فعالية التدريب بناءً على مراجعة مؤشرات الأداء الرئيسية سنويًا.
2	الوقاية من الهجمات (Attack prevention)
الهدف	أن يمنع حل الحماية من هجمات حجب الخدمة الموزعة (DDoS)، الذي تم ضبط إعداداته بشكل صحيح وإدارته بشكل آمن، محاولات شن تلك الهجمات على البنية التحتية لـ جامعة الباحة.
المخاطر المحتملة	قد يؤدي الخطأ في ضبط إعدادات حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) إلى عواقب وخيمة، مثل حجب حركة مرور البيانات المشروعة وحجب الخدمة.
الإجراءات المطلوبة	
1-2	على جامعة الباحة تحديد جميع الأصول المتاحة من الشبكة العامة وحمايتها، باستخدام حل الحماية من هجمات حجب الخدمة الموزعة (DDoS)، لضمان قدرتها على الاستجابة بفعالية لهجمات حجب الخدمة/حجب الخدمة الموزعة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2-2	تخصيص حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) بما يتناسب مع خصائص القطاع الذي تعمل فيه جامعة الباحة .
3-2	أن يوفر حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) تقارير ولوحات تحكم للهجمات التي تم منعها والإجراءات المتخذة بشأنها.
4-2	أن يوفر حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) حماية متعددة الطبقات، بحيث يحمي طبقة الشبكة وطبقة التطبيقات عند نشره مع جدار حماية تطبيقات الويب (WAF).
5-2	أن يستخدم حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) المعلومات الأمنية المقدمة من المؤسسات الوطنية الموثوقة، مثل الهيئة الوطنية للأمن السيبراني (NCA).
3	الكشف عن الهجمات والتنبيه بها والحدّ منها (Attack detection, alerting and mitigation)
الهدف	أن يكتشف حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) الحالات غير الطبيعية وأن يحدّ من الهجمات باستخدام أسلوب التصفية والتقييد.
المخاطر المحتملة	قد تؤدي عدم كفاية عمليات الكشف عن الهجمات إلى انتشار البرمجيات الضارة وحجب الخدمة وتسرب المعلومات.
الإجراءات المطلوبة	
1-3	على جامعة الباحة تحديد مؤشرات أداء رئيسية لرصد مدى فعالية حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) والتوجهات المتعلقة بهذا الحل.
2-3	أن يكون بإمكان حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) إيقاف انتشار هجمات حجب الخدمة/حجب الخدمة الموزعة ومنح حدوث المزيد من الأضرار للنظام .

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

3-3	أن يَستخدم حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) الأتمتة من أجل الحد من الهجمات الناشئة بشكل سريع.
4-3	أن يتيح حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) تكوين رؤية واضحة آنية حول تهديدات حجب الخدمة الموزعة، مع إمكانية إعداد التقارير وإنشاء الروابط بين الهجمات من خلال تحليلات الهجمات أو التكامل مع نظام إدارة المعلومات والأحداث الأمنية (SIEM).
5-3	أن يصدر عن حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) إشعارات فورية بالهجمات.
6-3	أن يخطر حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) المستخدمين بالإجراءات المتخذة والهجمات التي تم منعها والحد منها.
7-3	ضبط إعدادات التنبيهات بحيث تصدر في بداية الهجوم وفي نهايته وخلاله، وذلك باستخدام مقاييس مخصصة للهجمات.
8-3	أن يستخدم حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) تقنيات التعلّم الآلي والذكاء الاصطناعي لمنع التهديدات الجديدة.
9-3	ضبط إعدادات حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) لإرسال سجلات محددة فقط إلى نظام السجلات المركزي باستخدام بروتوكول سجل النظام (syslog) وبتنسيق الحدث العام (CEF) أو التنسيق الموسع لسجل الحدث (LEEF) أو تنسيق (RFC 5425) المحدد للسجلات.
10-3	أن يحدد حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) عنوان بروتوكول إنترنت معين للسلوك الخبيث، مع إجراء التحليلات الجنائية لتحديد كيفية انتقال التهديدات من جانب إلى آخر داخل البيئة الأمنية.
11-3	أن يراقب حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) نشاط الشبكة باستمرار لرصد أي حدث غير طبيعي في حركة مرور البيانات، مثل النمو غير المعتاد في إنتاجية الشبكة أو استخدام موارد الشبكة بدرجة أعلى من المعتاد.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

4	معايير أخرى (Other Standards)
الهدف	ضبط إعدادات حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) بشكل آمن ونشره واستخدامه بشكل مناسب وفقًا لأفضل الممارسات والتزما بالمعايير والسياسات ذات العلاقة بالبيئة الأمنية.
المخاطر المحتملة	قد يؤدي عدم التزام جامعة الباحة بجميع المعايير والمتطلبات الإلزامية المطبقة إلى تعرضها إلى زيادة حادة في التهديدات في المجالات التي تختص المعايير المذكورة أدناه بتغطيتها .

الإجراءات المطلوبة

تطبيق المعايير التالية فيما يتعلق بحلول الحماية من هجمات حجب الخدمة الموزعة (DDoS):

1-4

1. إدارة هويات الدخول والصلاحيات
2. النسخ الاحتياطي والتعافي من الكوارث
3. التشفير
4. تسجيل الأحداث وسجلات التدقيق
5. الأمن المادي
6. الإعدادات والتحصين الآمن
7. إدارة ومراقبة سجلات الأحداث

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

الجدول "أ" - منهجيات نشر حل الحماية من هجمات حجب الخدمة الموزعة (DDoS)

المنهجية	الوصف
الحماية من هجمات حجب الخدمة الموزعة كخدمة (DDoS as a Service)	تطبيق حلول مقدمي الخدمات. وعادةً ما يتم تنفيذ منهجية "الحماية من هجمات حجب الخدمة الموزعة كخدمة" من خلال إعادة توجيه حركة مرور البيانات على الشبكة إلى مركز معالجة (scrubbing center)خارجي.
داخل الموقع (الأجهزة)	نشر الحل على شبكة جامعة الباحة ، ويتم ذلك من خلال تركيب الأجهزة وتوصيلها بالشبكة.
المنهجية الهجينة (Hybrid)	تجمع هذه المنهجية بين نشر الحل كخدمة ونشره داخل الموقع بهدف الحد من الهجمات الكمية على مقربة من مصدر الهجوم قدر الإمكان، مع الحد من هجمات حجب الخدمة الموزعة (DDoS)على محيط شبكة جامعة الباحةباستخدام موارد مركز المعالجة الخاصة بالخدمة السحابية/مزود خدمة الإنترنت إذا كانت هجوم حجب الخدمة الموزع يتجاوز قدرات الأجهزة الموجودة داخل الموقع .

الأدوار والمسؤوليات

4- **مالك المعيار:** المشرف على وحدة الأمن السيبراني .

5- **مراجعة المعيار وتحديثه:** وحدة الأمن السيبراني.

6- **تنفيذ المعيار وتطبيقه:** إدارة تقنية المعلومات و وحدة الأمن السيبراني.

7- **قياس الالتزام بالمعيار:** وحدة الأمن السيبراني.

التحديث والمراجعة

يجب على وحدة الأمن السيبراني مراجعة المعيار سنويًا على الأقل أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في جامعة الباحة أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بالمعيار

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

4- يجب على المشرف على وحدة الأمن السيبراني التأكد من التزام جامعة الباحة بهذا المعيار دوريًا.

5- يجب على كافة العاملين في جامعة الباحةالالتزام بهذا المعيار.

6- قد يعرض أي انتهاك لهذا المعيار صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة إدارة هويات الدخول والصلاحيات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة هويات الدخول والصلاحيات على الأصول المعلوماتية والتقنية الخاصة بجامعة الباحة لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية، وذلك من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-٢-١ من الضوابط الأساسية للأمن السيبراني ((ECC-2:2024الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بجامعة الباحة، وتنطبق على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم من في جامعة الباحة.

بنود السياسة

1- إدارة هويات الدخول والصلاحيات (Identity and Access Management)

1-1 إدارة الصلاحيات

1-1-1 توثيق واعتماد إجراء لإدارة الوصول يوضح آلية منح صلاحيات الوصول للأصول المعلوماتية والتقنية وتعديلها وإلغائها في جامعة الباحة، ومراقبة هذه الآلية والتأكد من تطبيقها.

2-1-1 إنشاء هويات المستخدمين (User Identities) وفقاً للمتطلبات التشريعية والتنظيمية الخاصة بجامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

3-1-1 التحقق من هوية المستخدم (Authentication) والتحقق من صحتها قبل منح المستخدم صلاحية الوصول إلى الأصول المعلوماتية والتقنية.

4-1-1 توثيق واعتماد مصفوفة (Matrix) لإدارة تصاريح وصلاحيات المستخدمين (Authorization) بناءً على مبادئ التحكم بالدخول والصلاحيات التالية:

1-4-1-1 مبدأ الحاجة إلى المعرفة والاستخدام (Need-to-Know and Need-to-Use).

2-4-1-1 مبدأ فصل المهام (Segregation of Duties).

3-4-1-1 مبدأ الحد الأدنى من الصلاحيات والامتيازات (Least Privilege).

5-1-1 تطبيق ضوابط التحقّق والصلاحيات على جميع الأصول التقنية والمعلوماتية في جامعة الباحة من خلال نظام مركزي آلي للتحكّم في الوصول، مثل بروتوكول النفاذ إلى الدليل البسيط (Lightweight Directory Access Protocol "LDAP").

6-1-1 منع استخدام الحسابات المشتركة (Generic User) للوصول إلى الأصول المعلوماتية والتقنية الخاصة بجامعة الباحة.

7-1-1 ضبط إعدادات الأنظمة ليتم إغلاقها تلقائياً بعد فترة زمنية محدّدة (Session Timeout)، (يوصى ألا تتجاوز الفترة 15 دقيقة).

8-1-1 تعطيل حسابات المستخدمين غير المستخدمة خلال فترة زمنية محدّدة (يوصى ألا تتجاوز الفترة 90 يوماً).

9-1-1 ضبط إعدادات جميع أنظمة إدارة الهويات والوصول لإرسال السجلات إلى نظام تسجيل ومراقبة مركزي وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني.

10-1-1 عدم منح المستخدمين صلاحيات الوصول أو التعامل المباشر مع قواعد البيانات للأنظمة الحساسة، حيث يكون ذلك من خلال التطبيقات فقط، ويستثنى من ذلك مشرفي قواعد البيانات (Database Administrators). [CSCC-2-2-1-7]

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

11-1-1 توثيق واعتماد إجراءات واضحة للتعامل مع حسابات الخدمات (Service Account) والتأكد من إدارتها بشكل آمن مابين التطبيقات والأنظمة، وتعطيل الدخول البشري التفاعلي (Interactive Login) من خلالها. (CSCC-2-2-1-7)

2-1 منح حق الدخول

1-2-1 متطلبات حق الدخول لحسابات المستخدمين

1-1-2-1 منح صلاحية الدخول بناءً على طلب المستخدم من خلال نموذج أو عن طريق النظام المعتمد من قبل مديره المباشر ومالك النظام (System Owner) يُحدّد فيه اسم النظام ونوع الطلب والصلاحية ومدتها (في حال كانت صلاحية الدخول مؤقتة).

2-1-2-1 منح المستخدم حق الوصول إلى الأصول المعلوماتية والتقنية الخاصة بجامعة الباحة بما يتوافق مع الأدوار والمسؤوليات الخاصة به.

3-1-2-1 اتباع آلية موحدة لإنشاء هويات المستخدمين بطريقة تتيح تتبع النشاطات التي يتم أداؤها باستخدام "هوية المستخدم" (User ID) وربطها مع المستخدم، مثل كتابة <الحرف الأول من الاسم الأول> نقطة <الاسم الأخير>، أو كتابة رقم الموظف المعرف مسبقاً لدى الإدارة العامة للموارد البشرية.

4-1-2-1 تعطيل إمكانية تسجيل دخول المستخدم من أجهزة حاسبات متعدّدة في نفس الوقت (Concurrent Logins).

2-2-1 متطلبات حق الوصول للحسابات الهامة والحسّاسة

بالإضافة إلى الضوابط المذكورة في قسم متطلبات حق الوصول لحسابات المستخدمين، يجب أن تُطبَق الضوابط المُوضّحة أدناه على الحسابات ذات الصلاحيات الهامة والحسّاسة:

1-2-2-1 تعيين حق وصول مستخدم فردي للمستخدمين الذين يطلبون الصلاحيات الهامة والحسّاسة (Administrator Privilege) ومنحهم هذا الحق بناءً على مهامهم الوظيفية، مع الأخذ بالاعتبار مبدأ فصل المهام.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2-2-2-1 يجب تفعيل سجل كلمة المرور (Password History) لتتبع عدد كلمات المرور التي تم تغييرها.

3-2-2-1 تغيير أسماء الحسابات الافتراضية، وخصوصاً الحسابات الحاصلة على صلاحيات هامة وحسّاسة مثل "الحساب الرئيسي" (Root) وحساب "مدير النظام" (Admin) وحساب "مُعرّف النظام الفريد" (Sys id).

4-2-2-1 منع استخدام الحسابات ذات الصلاحيات الهامة والحسّاسة في العمليات التشغيلية اليومية.

5-2-2-1 التحقّق من حسابات المستخدمين ذات الصلاحيات الهامة والحسّاسة على الأصول التقنية والمعلوماتية من خلال آلية التحقّق من الهوية متعدد العناصر (Multi-Factor Authentication "MFA") ، مع تحديد عناصر التحقق المناسبة وعددها بناءً على نتائج تقييم الأثر المحتمل لفشل عملية التحقق وتخطيها.باستخدام طريقتين على الأقل من الطرق التالية:

- المعرفة (شيء يعرفه المستخدم "مثل كلمة المرور").
- الحيازة (شيء يملكه المستخدم فقط "مثل برنامج أو جهاز توليد أرقام عشوائية أو الرسائل القصيرة المؤقتة لتسجيل الدخول"، ويطلق عليها "One-Time-Password").
- الملازمة (صفة أو سمة حيوية متعلقة بالمستخدم نفسه فقط "مثل بصة الإصبع").

6-2-2-1 يجب أن يتطلب الوصول إلى الأنظمة الحساسة والأنظمة المستخدمة لإدارة الأنظمة الحساسة ومتابعتها استخدام التحقق من الهوية متعدد العناصر (MFA) لجميع المستخدمين.

3-2-1 الدخول عن بُعد إلى شبكات جامعة الباحة

1-3-2-1 منح صلاحية الدخول عن بعد للأصول المعلوماتية والتقنية بعد الحصول على إذن مسبق من وحدة الامن السيبراني وتقييد الدخول باستخدام التحقق من الهوية متعدد العناصر (MFA) ، مع تحديد عناصر التحقق المناسبة بناءً على تقييم المخاطر.

2-3-2-1 حفظ سجلات الأحداث المتعلقة بجميع جلسات الدخول عن بُعد الخاصة ومراقبتها حسب حساسية الأصول المعلوماتية والتقنية.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

3-1 إلغاء وتغيير حق الوصول

1-3-1 يجب على الإدارة العامة للموارد البشرية تبليغ وحدة الامن السيبراني لاتخاذ الإجراء اللازم عند انتقال المستخدم أو تغيير مهامه أو إنهاء/انتهاء العلاقة الوظيفية بين المستخدم وجامعة الباحة. وتقوم عمادة التعلم الالكتروني وتقنية المعلومات بإيقاف أو تعديل صلاحيات الدخول الخاصة بالمستخدم بناءً على مهامه الوظيفية الجديدة.

2-3-1 في حال تم إيقاف صلاحيات المستخدم، يمنع حذف سجلات الأحداث الخاصة بالمستخدم ويتم حفظها وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني.

2- مراجعة هويات الدخول والصلاحيات

1-2 مراجعة هويات الدخول (User IDs) والتحقق من صلاحية الوصول إلى الأصول المعلوماتية والتقنية وفقاً للمهام الوظيفية للمستخدم بناءً على مبادئ التحكم بالدخول والصلاحيات دورياً، ومراجعة هويات الدخول على الأنظمة الحساسة مرة واحدة كل ثلاثة أشهر على الأقل.

2-2 مراجعة الصلاحيات الخاصة (User Profile) بالأصول المعلوماتية والتقنية بناءً على مبادئ التحكم بالدخول والصلاحيات دورياً، ومراجعة الصلاحيات الخاصة بالأنظمة الحساسة مرة واحدة سنوياً على الأقل.

3-2 يجب تسجيل وتوثيق جميع محاولات الوصول الفاشلة والناجحة ومراجعتها دورياً.

3- إدارة كلمات المرور

1-3 تطبيق سياسة آمنة لكلمة المرور ذات معايير عالية لجميع الحسابات داخل جامعة الباحة، ويتضمّن الجدول أدناه أمثلة على ضوابط كلمات المرور لكل مستخدم:

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

ضوابط كلمات المرور	جميع المستخدمين (All Users)	حسابات المستخدمين ذات الصلاحيات الهامة والحسّاسة (Privileged Users)	حسابات الخدمات (Service Account)
الحدّ الأدنى لعدد أحرف كلمة المرور	8 أحرف أو أرقام أو رموز	12 حرفاً أو رقماً أو رمزاً	8 أحرف أو أرقام أو رموز
سجل كلمة المرور	تذكّر 5 كلمات مرور	تذكّر 5 كلمات مرور	تذكّر 5 كلمات مرور
الحد الأعلى لعمر كلمة المرور	45 يوماً	45 يوماً	45 يوماً
مدى تعقيد كلمة المرور	مُفعّل	مُفعّل	مُفعّل
مثال على تعقيد كلمة المرور	D_dyW5$_	R@rS%7qY#b!u	r?M4d5V=
مدة إغلاق الحساب	30 دقيقة أو حتى يقوم النظام بفك الإغلاق	30 دقيقة أو حتى يقوم النظام بفك الإغلاق	30 دقيقة أو حتى يقوم النظام بفك الإغلاق
حد إغلاق الحساب	5 محاولات غير صحيحة لتسجيل الدخول	5 محاولات غير صحيحة لتسجيل الدخول	لا توجد محاولات
إعادة ضبط عداد إغلاق الحساب بعد مرور فترة معينة	30 دقيقة (يقوم المدير بفك إغلاق الحساب المغلق يدوياً)	30 دقيقة (يقوم المدير بفك إغلاق الحساب المغلق يدوياً)	لا يوجد
استخدام التحقق متعدد العناصر	مُفعل على الدخول عن بعد فقط	مُفعل	غير مُفعل

2-3 معايير كلمات المرور

1-2-3 يجب أن تتضمّن كلمة المرور (8) أحرف على الأقل.

2-2-3 يجب أن تكون كلمة المرور معقّدة (Complex Password) وتتضمّن ثلاثة رموز من الرموز التالية على الأقل:

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

3-2-2-1 أحرف كبيرة (Upper Case Letters).

3-2-2-2 أحرف صغيرة (Lower Case Letters).

3-2-2-3 أرقام (1235).

3-2-2-4 رموز خاصّة (@#%*).

3-2-3 يجب إشعار المستخدمين قبل انتهاء صلاحية كلمة المرور لتذكيرهم بتغيير كلمة المرور قبل انتهاء الصلاحية.

3-2-4 يجب ضبط إعدادات كافة الأصول المعلوماتية والتقنية لطلب تغيير كلمة المرور المؤقتة عند تسجيل المستخدم الدخول لأول مرة.

3-2-5 يجب تغيير جميع كلمات المرور الافتراضية لجميع الأصول المعلوماتية والتقنية قبل تثبيتها في بيئة الإنتاج.

3-2-6 يجب تغيير كلمات مرور السلاسل النصية (Community String) الافتراضية (مثل: «Public» و«Private» و«System») الخاصة ببروتوكول إدارة الشبكة البسيط (SNMP)، ويجب أن تكون مختلفة عن كلمات المرور المستخدمة لتسجيل الدخول في الأصول التقنية المعنية.

3-3 حماية كلمات المرور

3-3-1 يجب تشفير جميع كلمات المرور للأصول المعلوماتية والتقنية الخاصة بجامعة الباحة بصيغة غير قابلة للقراءة أثناء إدخالها ونقلها وتخزينها وذلك وفقاً لسياسة التشفير.

3-3-2 يجب إخفاء (Mask) كلمة المرور عند إدخالها على الشاشة.

3-3-3 يجب تعطيل خاصية "تذكّر كلمة المرور" (Remember Password) على الأنظمة والتطبيقات الخاصة بجامعة الباحة.

3-3-4 منع استخدام الكلمات المعروفة (Dictionary) في كلمة المرور كما هي.

3-3-5 يجب تسليم كلمة المرور الخاصة بالمستخدم بطريقة آمنة وموثوقة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

6-3-3 إذا طلب المستخدم إعادة تعيين كلمة المرور عن طريق الهاتف أو الإنترنت أو أي وسيلة أخرى، فلا بد من التحقّق من هوية المستخدم قبل إعادة تعيين كلمة المرور.

7-3-3 يجب حماية كلمات المرور الخاصة بحسابات الخدمة والحسابات ذات الصلاحيات الهامة والحسّاسة وتخزينها بشكل آمن في موقع مناسب (داخل مغلف مختوم في خزنة) أو استخدام التقنيات الخاصة بحفظ وإدارة الصلاحيات الهامة والحسّاسة (Privilege Access Management Solution).

4- متطلبات أخرى

1-4 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لإدارة هويات الدخول والصلاحيات.

2-4 يجب مراجعة تطبيق متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات دورياً.

3-4 يجب مراجعة هذه السياسة سنوياً على الأقل، أو في حال حدوث تغييرات في المتطلبات التشريعية أو التنظيمية أو المعايير ذات العلاقة.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** وحدة الامن السيبراني .

2- **مراجعة السياسة وتحديثها:** وحدة الامن السيبراني .

3- **تنفيذ السياسة وتطبيقها:** عمادة التعلم الالكتروني وتقنية المعلومات والإدارة العامة للموارد البشرية و وحدة الامن السيبراني .

الالتزام بالسياسة

1- يجب على عمادة التعلم الإلكتروني وتقنية المعلومات ضمان التزام جامعة الباحة بهذه السياسة دورياً.

2- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في الإلتزام بهذه السياسة

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة الأمن السيبراني للموارد البشرية

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان التأكد من أن مخاطر ومتطلبات الأمن السيبراني المتعلقة بالعاملين (موظفين ومتعاقدين) في جامعة الباحة تعالج بفعالية قبل وأثناء وعند انتهاء/إنهاء عملهم.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٩-١ من الضوابط الأساسية للأمن السيبراني (ECC-2:2024)الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأنظمة الخاصة بجامعة الباحة وتنطبق على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم من في جامعة الباحة.

بنود السياسة

البنود العامة

1-1 يجب تحديد متطلبات الأمن السيبراني المتعلقة ب جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم من في جامعة الباحة.

2-1 يجب شغل جميع وظائف الأمن السيبراني من قبل مواطن متفرغ وذوي كفاءة في مجال الأمن السيبراني.

3-1 يجب تنفيذ ضوابط الأمن السيبراني الخاصة بالموارد البشرية خلال دورة حياة عمل الموظف (Lifecycle) في جامعة الباحة والتي تشمل المراحل التالية:

- قبل التوظيف

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

- خلال فترة العمل
- عند انتهاء فترة العمل أو إنهائها

4-1 يجب على العاملين في جامعة الباحة فهم أدوارهم الوظيفية، والشروط والمسؤوليات ذات العلاقة بالأمن السيبراني، والموافقة عليها.

5-1 يجب تضمين مسؤوليات الامن السيبراني وبنود المحافظة على سرية المعلومات (Non-Disclosure Agreement) في عقود العاملين في جامعة الباحة (لتشمل خلال وبعد انتهاء/إنهاء العلاقة الوظيفية مع جامعة الباحة).

6-1 يجب إدراج المخالفات ذات العلاقة بالأمن السيبراني في لائحة مخالفات الموارد البشرية في جامعة الباحة.

7-1 يُمنع الاطلاع على المعلومات الخاصة بالموظفين دون تصريح مسبق.

8-1 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لمتطلبات الأمن السيبراني المتعلق بالموارد البشرية.

قبل التوظيف

1-2 يجب على العاملين التعهد بالالتزام بسياسات الأمن السيبراني قبل منحهم صلاحية الوصول إلى أنظمة جامعة الباحة.

2-2 يجب تحديد أدوار الموظفين ومسؤولياتهم مع الأخذ في الحسبان تطبيق مبدأ عدم تعارض المصالح.

3-2 يجب تحديد أدوار الموظفين ومسؤولياتهم المتعلقة بالأمن السيبراني في الوصف الوظيفي.

4-2 يجب أن تشمل الأدوار والمسؤوليات المتعلقة بالأمن السيبراني الآتي:

- حماية جميع أصول جامعة الباحة من الوصول غير المصرح به، أو تخريب تلك الأصول.
- تنفيذ جميع الأنشطة المطلوبة المتعلقة بالأمن السيبراني.
- الالتزام بسياسات الأمن السيبراني ومعاييره الخاصة بجامعة الباحة.
- الالتزام ببرنامج زيادة مستوى الوعي بالمخاطر السيبرانية.

5-2 يجب إجراء مسح أمني للعاملين في وظائف الأمن السيبراني، والوظائف التقنية ذات الصلاحيات الهامة والحساسة، والوظائف ذات العلاقة بالأنظمة الحساسة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

أثناء العمل

1-3 يجب تقديم برنامج توعوي، يختص بزيادة مستوى الوعي بالأمن السيبراني؛ بما في ذلك سياسات الأمن السيبراني ومعاييره، بشكل دوري.

2-3 يجب على الإدارة العامة للموارد البشرية إبلاغ الإدارات ذات العلاقة عن أي تغيير في أدوار العاملين أو مسؤولياتهم بهدف اتخاذ الإجراءات اللازمة المتعلقة بإلغاء صلاحيات الوصول أو تعديلها.

3-3 يجب التأكد من تطبيق متطلبات الأمن السيبراني الخاصة بالموارد البشرية.

4-3 يجب إدراج مدى الالتزام بالأمن السيبراني ضمن جوانب تقييم الموظفين.

5-3 يجب التأكد من تطبيق مبدأ الحاجة إلى المعرفة (Need-to-know) في تكليف المهمات.

انتهاء الخدمة أو إنهاؤها

1-4 يجب تحديد إجراءات انتهاء الخدمة المهنية أو إنهائها بشكل يغطي متطلبات الأمن السيبراني.

2-4 يجب على الإدارة العامة للموارد البشرية إبلاغ الوحدات ذات العلاقة في حال اقتراب موعد انتهاء العلاقة الوظيفية أو إنهائها لاتخاذ الإجراءات اللازمة.

3-4 يجب التأكد من إعادة جميع الأصول الخاصة بجامعة الباحة وإلغاء صلاحيات الدخول للعاملين في آخر يوم عمل لهم وقبل حصولهم على المخالصات اللازمة.

4-4 يجب تحديد المسؤوليات والواجبات التي ستبقى سارية المفعول بعد انتهاء خدمة العاملين في جامعة الباحة، بما في ذلك اتفاقية المحافظة على سرية المعلومات، على أن يتم إدراج تلك المسؤوليات والواجبات في جميع عقود العاملين.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** وحدة الامن السيبراني .

2- **مراجعة السياسة وتحديثها:** وحدة الامن السيبراني .

3- **تنفيذ السياسة وتطبيقها:** الإدارة العامة للموارد البشرية.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

الالتزام بالسياسة

1- يجب على وحدة الامن السيبراني ضمان التزام جامعة الباحة بهذه السياسة دورياً.

2- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في الإلتزام بهذه السياسة

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة، إلى إجراء تأديبي؛ حسب الإجراءات المتبعة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير؛ لتقليل المخاطر السيبرانية، وحماية الأصول المعلوماتية لجامعة الباحة من التهديدات (Threats) الداخلية والخارجية، عن طريق استخدام نظام إدارة سجلات الأحداث، ومراقبة الأمن السيبراني.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١٢-١ من الضوابط الأساسية للأمن السيبراني ((ECC-2:2024الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أنظمة إدارة سجلات الأحداث، ومراقبة الأمن السيبراني الخاصة بجامعة الباحة، وتنطبق على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم من في جامعة الباحة.

بنود السياسة

1- البنود العامة

1-1 يجب توفير تقنيات إدارة المعلومات، والأحداث الأمنية (Security Information and Event Management "SIEM"***) اللازمة، لجمع سجلات الأحداث السيبرانية للأصول المعلوماتية، والأنظمة والتطبيقات، وقواعد البيانات والشبكات، وأنظمة الحماية في جامعة الباحة. ويجب أن تحتوي هذه السجلات على المعلومات الآتية بوصفها حداً أدنى:***

1-1-1 نوع الحدث (Event Type)

2-1-1 مكان الحدث، أو النظام الذي تم تنفيذ الحدث عليه(Location of Event or System))

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

3-1-1 وقت الحدث وتاريخه (Date and Time of Event)

4-1-1 المستخدم أو الأداة المستخدمة لتنفيذ الحدث

5-1-1 حالة الحدث أو نتيجته (Success vs. Failure)

2- الأحداث المراد تسجيلها

1-2 يجب أن تفعّل الأنظمة المراد مراقبتها سجلات الأحداث عند وقوع أحد الأحداث، بحد أدنى؛ ما يلي:

1-1-2 الأحداث (Event Logs) الخاصة بالأمن السيبراني على جميع المكونات التقنية للأنظمة الحساسة (أنظمة التشغيل، قواعد البيانات، التخزين، التطبيقات، والشبكات).

2-1-2 الأحداث (Event Logs) الخاصة بالأمن السيبراني للشبكة الصناعية والاتصالات المرتبطة بها.

3-1-2 الأحداث الخاصة بالحسابات التي تمتلك صلاحيات مهمة وحساسة على الأصول المعلوماتية.

4-1-2 الأحداث الخاصة بالتصفح والاتصال بالإنترنت، والشبكة اللاسلكية.

5-1-2 نقل المعلومات عبر وسائط التخزين الخارجية.

6-1-2 إجراء تغييرات غير مشروعة على السجلات، وملفات الأنظمة الحساسة من خلال تقنيات إدارة تغييرات الملفات (File Integrity Management "FIM").

7-1-2 تغيير إعدادات النظام، أو الشبكة، أو الخدمات، بما في ذلك تنزيل حزم التحديثات والإصلاحات، أو غيرها من التغييرات على البرامج المثبتة.

8-1-2 أنشطة مشبوهة، مثل الأنشطة التي يكتشفها نظام منع التسلل (Intrusion Prevention System "IPS")

2-2 يجب إعداد إجراءات ومعايير أمنية تطبق أفضل الممارسات؛ لحفظ سجلات الأحداث بطريقة تضمن سلامتها من التعديل، أو الحذف، أو الوصول غير المصرح به.

3-2 يجب مراقبة سجلات الأحداث، وتحليلها دورياً حسب تصنيفها، بما في ذلك مراقبة سلوك مستخدم الأنظمة الحساسة وتحليله.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

4-2 يجب مزامنة التوقيت (Clock Synchronization) مركزياً، ومن مصدر دقيق وموثوق، لجميع الأنظمة التي تتم مراقبتها.

5-2 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لنظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني.

6-2 يجب أرشفة سجلات الأحداث، والقيام بالنسخ الاحتياطي دورياً.

7-2 يجب أن تكون مدة الاحتفاظ بسجلات الأحداث السيبرانية 12 شهراً على الأقل، و18 شهراً بالنسبة للأنظمة الحساسة بحد أدنى، وبما يتوافق مع السياسات الداخلية، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** وحدة الامن السيبراني .

2- **مراجعة السياسة وتحديثها:** وحدة الامن السيبراني .

3- **تنفيذ السياسة وتطبيقها:** عمادة التعلم الالكتروني وتقنية المعلومات و وحدة الامن السيبراني .

الالتزام بالسياسة

1- يجب على وحدة الامن السيبراني ضمان التزام جامعة الباحة بهذه السياسة بشكل دوري.

2- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في الإلتزام بهذه السياسة

3- قد يُعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة إدارة حزم التحديثات والإصلاحات

الأهداف

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة حزم التحديثات والإصلاحات للأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة وأجهزة معالجة المعلومات الخاصة بجامعة الباحة لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تتبع هذه السياسة المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهي متطلب تشريعي كما هو مذكور في الضابط رقم ٢-٣-٣-٣ من الضوابط الأساسية للأمن السيبراني (ECC-2:2024) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة وأجهزة معالجة المعلومات وأجهزة وأنظمة التحكم الصناعي الخاصة بجامعة الباحة، وتنطبق على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم من في جامعة الباحة.

بنود السياسة

1- يجب إدارة حزم التحديثات والإصلاحات (Patch Management) بشكل يضمن حماية الأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة وأجهزة معالجة المعلومات.

2- يجب تنزيل حزم التحديثات والإصلاحات من مصادر مرخصة وموثوقة وفقاً للإجراءات المتبعة داخل جامعة الباحة.

3- يجب استخدام أنظمة تقنية موثوقة وآمنة لإجراء مسح دوري للكشف عن الثغرات وحزم التحديثات ومتابعة تطبيقها.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

4- يجب على عمادة التعلم الالكتروني وتقنية المعلومات اختبار حزم التحديثات والإصلاحات في البيئة الاختبارية (Test Environment) قبل تثبيتها على الأنظمة والتطبيقات وأجهزة معالجة المعلومات في بيئة الإنتاج (Production Environment)، للتأكد من توافق حزم التحديثات والإصلاحات مع الأنظمة والتطبيقات.

5- يجب وضع خطة للاسترجاع (Rollback Plan) وتطبيقها في حال تأثير حزم التحديثات والإصلاحات سلباً على أداء الأنظمة أو التطبيقات أو الخدمات.

6- يجب على اللجنة الإشرافية للأمن السيبراني التأكد من تطبيق حزم التحديثات والإصلاحات دورياً.

7- يجب منح الأولوية لحزم التحديثات والإصلاحات التي تعالج الثغرات الأمنية حسب مستوى المخاطر المرتبطة بها.

8- يجب جدولة التحديثات والإصلاحات بما يتماشى مع مراحل الإصدارات البرمجية التي يطرحها المورد.

9- يجب تنصيب التحديثات والإصلاحات مرّة واحدة شهرياً على الأقل للأنظمة الحسّاسة المتصلة بالإنترنت، ومرّة واحدة كل ثلاثة أشهر للأنظمة الحسّاسة الداخلية. (CSCC-2-3-1-3)

10- يجب تنصيب التحديثات والإصلاحات للأصول التقنية على النحو التالي:

نوع الأصل	مدة التكرار لتنصيب التحديثات	
	الأصول المعلوماتية والتقنية	الأصول المعلوماتية والتقنية للأنظمة الحساسة
أنظمة التشغيل	شهرياً	شهرياً
قواعد البيانات	ثلاثة أشهر	شهرياً
أجهزة الشبكة	ثلاثة أشهر	شهرياً
التطبيقات	ثلاثة أشهر	شهرياً

11- يجب أن تتبع عملية إدارة التحديثات والإصلاحات متطلّبات عملية إدارة التغيير.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

12- في حال وجود ثغرات أمنية ذات مخاطر عالية، يجب تنصيب حزم التحديثات والإصلاحات الطارئة وفقاً لعملية إدارة التغيير الطارئة (Emergency Change Management).

13- يجب تنزيل التحديثات والإصلاحات على خادم مركزي (Server Centralized Patch Management) قبل تنصيبها على الأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة وأجهزة معالجة المعلومات، ويُستثنى من ذلك حزم التحديثات والإصلاحات التي لا يتوفر لها أدوات آلية مدعومة.

14- بعد تنصيب حزم التحديثات والإصلاحات، يجب استخدام أداوات مستقلة وموثوقة للتأكد من أن الثغرات تمت معالجتها بشكل فعال.

15- يجب استخدام مؤشر قياس الأداء (Key Performance Indicator "KPI") لضمان التطوير المستمر لإدارة حزم التحديثات والإصلاحات.

16- يجب مراجعة سياسة إدارة حزم التحديثات والإصلاحات وإجراءاتها سنوياً، وتوثيق التغييرات واعتمادها.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** وحدة الامن السيبراني .

2- **مراجعة السياسة وتحديثها:** وحدة الامن السيبراني .

3- **تنفيذ السياسة وتطبيقها:** عمادة التعلم الالكتروني وتقنية المعلومات.

الالتزام بالسياسة

1- يجب على عمادة التعلم الإلكتروني وتقنية المعلومات ضمان التزام جامعة الباحة بهذه السياسة بشكل مستمر.

2- يجب على وحدة الامن السيبراني وعمادة التعلم الالكتروني وتقنية المعلومات في جامعة الباحة الالتزام بهذه السياسة.

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة، إلى إجراء تأديبي؛ حسب الإجراءات المتبعة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة الأمن السيبراني المتعلق بالأطراف الخارجية

الأهداف

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني لضمان حماية الأصول المعلوماتية والتقنية في جامعة الباحة من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية بما في ذلك خدمات الإسناد لتقنية الملعومات والخدمات المدارة وفقا للسياسات والإجراءات التنظيمية الخاصة بجامعة الباحة.

تتبع هذه السياسة المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهي متطلب تشريعي كما هو مذكور في الضابط رقم ١-١-٤ من الضوابط الأساسية للأمن السيبراني (ECC-2:2024) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تنطبق هذه السياسة على جميع الخدمات المقدمة من الأطراف الخارجية لجامعة الباحة، وتنطبق على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم من في جامعة الباحة.

بنود السياسة

1- البنود العامة

1-1 يجب توثيق واعتماد إجراءات موحدة لإدارة علاقة جامعة الباحة مع الأطراف الخارجية قبل وأثناء وبعد انتهاء العلاقة التعاقدية.

2-1 يجب تحديد واختيار الأطراف الخارجية المقدمة للخدمات بعناية ووفقاً للسياسات والإجراءات التنظيمية لجامعة الباحة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

3-1 يجب إجراء تقييم للمخاطر على الأطراف الخارجية والخدمات المقدمة والتأكد من سلامتها، وذلك بمراجعة مشاريع الأطراف الخارجية داخل جامعة الباحة ومراجعة سجلات الأحداث السيبرانية الخاص بخدمة الطرف الخارجي (إن أمكن) قبل وأثناء العلاقة وبشكل دوري.

4-1 يجب إعداد العقود والاتفاقيات مع الأطراف الخارجية بشكل يضمن التزام الطرف الخارجي بتطبيق متطلبات وسياسات الأمن السيبراني لجامعة الباحة والمتطلبات التشريعية والتنظيمية ذات العلاقة.

5-1 يجب مراجعة العقود والاتفاقيات مع الأطراف الخارجية من قبل إدارة الشؤون القانونية للتأكد من أن تكون بنود الاتفاقية ملزمة أثناء فترة العقد وبعد انتهاءها وأن مخالفتها يعرض الطرف الخارجي للمساءلة قانونياً.

6-1 يجب أن تشمل العقود والاتفاقيات على بنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) والحذف الآمن من قِبَل الطرف الخارجي لبيانات جامعة الباحة عند انتهاء الخدمة.

7-1 يجب مراجعة متطلبات الأمن السيبراني مع الأطراف الخارجية بشكل دوري.

8-1 يجب مراجعة سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية سنوياً، وتوثيق التغييرات واعتمادها.

2- متطلبات الأمن السيبراني الخاصة بخدمات الإسناد لتقنية المعلومات "Outsourcing" أو الخدمات المدارة "Managed Services" المقدمة من قبل الأطرف الخارجية

1-2 للحصول على خدمات إسناد لتقنية المعلومات أو خدمات مدارة، فإنه يجب اختيار الطرف الخارجي بعناية، ويجب أن يتم التحقق من الآتي:

1-1-2 إجراء تقييم لمخاطر الأمن السيبراني، والتأكد من وجود مايضمن السيطرة على تلك المخاطر، قبل توقيع العقود والاتفاقيات أو عند تغيير المتطلبات التشريعية والتنظيمية ذات العلاقة.

2-1-2 يجب أن تكون مراكز عمليات خدمات الأمن السيبراني المدارة للتشغيل والمراقبة والتي تستخدم طريقة الوصول عن بعد موجودة بالكامل داخل المملكة. (ECC-4-1-3-2)

3-1-2 خدمات الإسناد على الأنظمة الحساسة يجب أن تكون عن طريق شركات وجهات وطنية، وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة. (CSCC-4-1-1-2)

3- متطلبات الأمن السيبراني المتعلقة بموظفي الأطراف الخارجية

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

1-3 يجب أن يتم إجراء المسح الأمني (Screening or Vetting) لشركات خدمات الإسناد، ولموظفي خدمات الإسناد، والخدمات المدارة العاملين على الأنظمة الحساسة. (CSCC-4-1-1-1)

2-3 يجب تضمين مسؤوليات الأمن السيبراني وبنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) في عقود موظفي الأطراف الخارجية (لتشمل خلال وبعد انتهاء/ إنهاء العلاقة الوظيفية مع جامعة الباحة).

4- التوثيق وضوابط الوصول

1-4 يجب أن تُطوّر الأطراف الخارجية وتتبع عملية رسمية وموثّقة بعناية لمنح وإلغاء حق الوصول إلى جميع الأنظمة المعلوماتية والتقنية التي تُعالِج أو تنقل أو تخزّن معلومات جامعة الباحة بما يتماشى مع متطلّبات الأمن السيبراني وأهداف ضوابط الأمن السيبراني الخاصة بـ جامعة الباحة.

2-4 يجب توفير إمكانية الوصول إلى معلومات جامعة الباحة ومعالجتها بطريقة آمنة ومراقبة.

3-4 يجب تطبيق الضوابط المتعلّقة بكلمات المرور على جميع المستخدمين الذين يملكون حق الوصول إلى معلومات جامعة الباحة بما يتماشى مع متطلّبات الأمن السيبراني وأهداف ضوابط الأمن السيبراني الخاصة بـ جامعة الباحة.

4-4 يجب تطبيق نظام التحقّق من الهوية متعدّد العناصر على إمكانية الوصول إلى الأنظمة الحسّاسة التي تُعالج المعلومات الخاصة بـ جامعة الباحة أو تنقلها أو تُخزّنها.

5-4 يجب إلغاء حقوق الوصول فور انتهاء/إنهاء خدمات أي موظف يعمل لدى الأطراف الخارجية ويملك حق الوصول إلى المعلومات أو الأصول المعلوماتية والتقنية الخاصة بـ جامعة الباحة أو في حال تغيير دوره الوظيفي الذي لا يتطلّب استمرارية وصوله إليها.

6-4 يجب أن تقوم الأطراف الخارجية بمراجعة حقوق الوصول بوتيرة دورية وفقًا لسياسات الأمن السيبراني المعتمدة في جامعة الباحة.

7-4 يجب تخزين كلّ سجلات التدقيق والحفاظ عليها وتوفيرها بناءً على طلب جامعة الباحة.

5- متطلبات الأمن السيبراني المتعلقة بإدارة التغيير

1-5 يجب أن تتبع الأطراف الخارجية عملية إدارة التغيير الرسمية والمناسبة وفقاً لسياسات وإجراءات جامعة الباحة وبما يتوافق مع متطلّبات الأمن السيبراني.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2-5 يجب مراجعة واختبار التغيير التي أجريت على الأصول المعلوماتية والتقنية الخاصة بجامعة الباحة قبل تطبيقها على بيئة الإنتاج (Production Environment).

3-5 يجب إبلاغ الأطراف المعنية في جامعة الباحة بالتغييرات الرئيسية التي مخطط إجراءها وكذلك التي أجريت على الأصول المعلوماتية والتقنية الخاصة بجامعة الباحة.

6- متطلبات إدارة حوادث الأمن السيبراني واستمرارية الأعمال

1-6 يجب ان تتضمن بنود العقود والاتفاقيات مع الأطراف الخارجية على متطلبات متعلقة بالإبلاغ عن حوادث الأمن السيبراني وإبلاغ جامعة الباحة في حال تعرض الطرف الخارجي إلى حادثة أمن سيبراني.

2-6 يجب تحديد وتوثيق إجراءات التواصل بين الطرف الخارجي و جامعة الباحة في حال تعرض الطرف الخارجي إلى حادثة أمن سيبراني، ومراجعة وتحديث هذه الإجراءات بشكل دوري.

3-6 يجب وضع خطة مناسبة لاستمرارية الأعمال لتفادي عدم توافر الخدمات المقدمة لجامعة الباحة وفقاً لمتطلّبات خطّة استمرارية الأعمال والتعافي من الكوارث الخاصة بجامعة الباحة.

7- متطلبات حماية البيانات والمعلومات

1-7 يجب أن تقوم الأطراف الخارجية بمعالجة بيانات ومعلومات جامعة الباحة وتخزينها وإتلافها وفقاً لسياسة ومعيار حماية البيانات والمعلومات المعتمدين في جامعة الباحة.

2-7 يجب تطبيق ضوابط تشفير مناسبة لحماية بيانات ومعلومات جامعة الباحة وضمان الحفاظ على سريّتها وسلامتها وتوافرها وفقاً لمعيار التشفير المعتمد في جامعة الباحة.

3-7 يجب عمل نُسخ احتياطية من بيانات ومعلومات جامعة الباحة بشكل دوري ووفقاً لسياسة إدارة النسخ الاحتياطية الخاصة بجامعة الباحة.

4-7 يجب عدم معالجة أو تخزين أو استخدام بيانات ومعلومات جامعة الباحة الموجودة في الأنظمة الحسّاسة والبيانات الشخصية (Data privacy)، والتي تُعالجها الأطراف الخارجية - في بيئة الاختبار إلا بعد استخدام ضوابط مشددة لحماية تلك البيانات مثل: تقنيات تعتيم البيانات (Data Masking) أو تقنيات مزج البيانات (Data Scrambling) أو تقنيات إخفاء البيانات (Data Anonymization). (CSCC-2-6-1-1)

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

5-7 يجب عدم نقل بيانات ومعلومات جامعة الباحة الموجودة في الأنظمة الحسّاسة - والتي تُعالجها الأطراف الخارجية - خارج بيئة الإنتاج. (CSCC-2-6-1-5)

6-7 يجب تصنيف بيانات ومعلومات جامعة الباحة الموجودة في الأنظمة الحسّاسة - والتي تُعالجها الأطراف الخارجية - وفقاً لسياسة تصنيف البيانات والمعلومات المعتمدة في جامعة الباحة. (CSCC-2-6-1-2)

8- التدقيق

1-8 يجب أن تُجري جامعة الباحة تدقيقًا للعمليات والأنظمة ذات الصلة متى كان ذلك ضرورياً أو مناسباً.

2-8 يجب أن تتعاون جميع مرافق الطرف الخارجي وموظفيه بصورة كاملة مع أنشطة مراجعة سجل الأحداث والتدقيق التي تقوم بها جامعة الباحة بما يشمل المراجعات المُنفّذة.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** وحدة الامن السيبراني .

2- **تحديث السياسة ومراجعتها:** وحدة الامن السيبراني .

3- **تنفيذ السياسة وتطبيقها:** وحدة الامن السيبراني وعمادة التعلم الالكتروني وتقنية المعلومات و الإدارة العامة للموارد البشرية و إدارة الشؤون القانونية و إدارة المشتريات.

الالتزام بالسياسة

1- يجب على عمادة التعلم الإلكتروني وتقنية المعلومات ضمان التزام جامعة الباحة بهذه السياسة بشكل دوري.

2- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في الإلتزام بهذه السياسة

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة لإجراء تأديبي حسب الإجراءات المتبعة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة إختبار الإختراق

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير في تقييم واختبار مدى فعالية قدرات تعزيز الأمن السيبراني في جامعة الباحة وذلك من خلال محاكاة تقنيات وأساليب الهجوم السيبراني الفعلية، ولاكتشاف نقاط الضعف الأمنية غير المعروفة والتي قد تؤدي إلى الاختراق السيبراني لجامعة الباحة من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١١-١ من الضوابط الأساسية للأمن السيبراني ((ECC-2:2024الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأنظمة الحساسة ومكوناتها التقنية، وجميع الخدمات المقدمة خارجياً (عن طريق الإنترنت) ومكوناتها التقنية، ومنها: البنية التحتية، والمواقع الإلكترونية، وتطبيقات الويب، وتطبيقات الهواتف الذكية واللوحية، والبريد الإلكتروني والدخول عن بعد في جامعة الباحة، وتنطبق على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم من في جامعة الباحة.

بنود السياسة

1- المتطلبات العامة

1-3 يجب على جامعة الباحة إجراء اختبار الاختراق (Penetration Testing) دورياً، لتقييم واختبار مدى فعالية قدرات تعزيز الأمن السيبراني.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2-3 تحدد وحدة الامن السيبراني الأنظمة والخدمات والمكونات التقنية التي يجب إجراء اختبار الاختراق عليها وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

3-3 يجب على جامعة الباحة إجراء اختبار الاختراق على جميع الخدمات المقدمة خارجياً ومكوناتها التقنية دورياً. (ECC-2-11-3-1)

4-3 يجب التأكد من أن اختبار الاختراق لا يؤثر على الأنظمة والخدمات المقدمة في جامعة الباحة.

5-3 يجب على جامعة الباحة إجراء اختبار الاختراق على الأنظمة الحساسة ومكوناتها التقنية كل ستة أشهر؛ على الأقل. (CSCC-2-10-2)

6-3 يجب إجراء اختبار الاختراق لاكتشاف نقاط الضعف الأمنية بكافة صورها والتي تشمل نقاط الضعف التي تنتج عادةً عن أخطاء في تطوير التطبيقات (Application Development Error) وضبط إعدادات النظام بشكل غير آمن (Configurations Faults) وإمكانية استغلال ثغرة محددة (Exploitability of Identified Vulnerability).

7-3 يجب تطوير إجراءات خاصة باختبار الاختراق واعتمادها ونشرها، مع الأخذ بالاعتبار عدم تأثيرها على سير الأعمال الخاصة بجامعة الباحة.

8-3 يجب على وحدة الامن السيبراني تحديد أو الموافقة على أساليب اختبار الاختراق والأدوات والتقنيات التي يستخدمها فريق اختبار الاختراق الداخلي أو الخارجي قبل بدء عملية اختبار الاختراق.

9-3 في حال تفويض طرف خارجي للقيام باختبار الاختراق نيابة عن جامعة الباحة، يجب التحقق من تطبيق جميع متطلبات الأمن السيبراني المتعلقة بالأطراف الخارجية ووفقاً لسياسة الأمن السيبراني المتعلّق بالأطراف الخارجية المعتمدة في جامعة الباحة.

10-3 يجب تصنيف نتائج اختبار الاختراق بناءً على خطورتها، ومعالجتها حسب المخاطر السيبرانية المترتبة عليها ووفقاً لمنهجية إدارة المخاطر المعتمدة لدى جامعة الباحة.

11-3 يجب وضع خطة عمل لمعالجة نتائج اختبار الاختراق يوضح فيها تأثير المخاطر وآلية معالجتها والمسؤول عن تطبيقها والفترة الزمنية اللازمة لتنفيذها.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2- متطلبات أخرى

2-1 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لعمليات اختبار الاختراق.

2-2 يجب مراجعة تطبيق متطلبات الأمن السيبراني لعمليات اختبار الاختراق في جامعة الباحة دورياً. (ECC-2-11-4)

3-2 يجب مراجعة هذه السياسة مرة واحدة في السنة؛ على الأقل.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** وحدة الامن السيبراني .

2- **مراجعة السياسة وتحديثها:** وحدة الامن السيبراني .

3- **تنفيذ السياسة وتطبيقها:** عمادة التعلم الالكتروني وتقنية المعلومات و وحدة الامن السيبراني .

الالتزام بالسياسة

1- يجب على عمادة التعلم الإلكتروني وتقنية المعلومات ضمان التزام جامعة الباحة بهذه السياسة دورياً.

2- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في الإلتزام بهذه السياسة

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة إدارة الثغرات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان اكتشاف الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعال؛ وذلك لمنع احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية أو تقليلها، وكذلك التقليل من الآثار المترتبة على أعمال جامعة الباحة وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١٠-١ من الضوابط الأساسية للأمن السيبراني ((ECC-2:2024الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية في جامعة الباحة، وتنطبق على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم من في جامعة الباحة.

بنود السياسة

1- المتطلبات العامة

1-1 يجب على جامعة الباحة إجراء فحص الثغرات (Vulnerabilities Assessment) دورياً، لاكتشاف وتقييم الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعال.

2-1 تحدد وحدة الامن السيبراني الأنظمة والخدمات والمكونات التقنية التي يجب إجراء فحص الثغرات عليها وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

3-1 يجب على وحدة الامن السيبراني التأكد من استخدام أساليب وأدوات موثوقة لاكتشاف الثغرات.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

4-1 يجب تطوير واعتماد إجراءات خاصة بتنفيذ فحص واكتشاف الثغرات وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

5-1 في حال تفويض طرف خارجي للقيام بفحص واكتشاف الثغرات نيابة عن جامعة الباحة، يجب التحقق من تطبيق جميع متطلبات الأمن السيبراني المتعلقة بالأطراف الخارجية وفقاً لسياسة الأمن السيبراني المتعلّق بالأطراف الخارجية المعتمدة في جامعة الباحة.

2- متطلبات تقييم الثغرات

1-2 يجب فحص واكتشاف الثغرات قبل نشر الخدمات أو الأنظمة على الإنترنت أو عند القيام بأي تغيير على الأنظمة الحساسة وفقاً لسياسة الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية.

2-2 يجب تصنيف الثغرات حسب خطورتها، ومعالجتها حسب المخاطر السيبرانية المترتبة عليها وفقاً لمنهجية إدارة المخاطر المعتمدة لدى جامعة الباحة.

3-2 يجب على جامعة الباحة إجراء تقييم الثغرات لجميع الأصول التقنية ومعالجتها دورياً. (ECC-2-10-3-1)

4-2 يجب على جامعة الباحة إجراء تقييم الثغرات للمكونات التقنية للأنظمة الحساسة الداخلية ومعالجتها كل ثلاثة أشهر؛ على الأقل. (CSCC-2-9-1-3)

5-2 يجب على جامعة الباحة إجراء تقييم الثغرات للمكونات التقنية للأنظمة الحساسة الخارجية والمتصلة بالإنترنت مرة واحدة شهرياً. (CSCC-2-9-1-2)

3- متطلبات معالجة الثغرات

1-3 بعد الانتهاء من تقييم الثغرات، يجب إعداد تقرير يوضح الثغرات المكتشفة وتصنيفها والتوصيات المقترحة لمعالجتها.

2-3 بعد إرسال تقرير تقييم الثغرات ومعالجتها من قبل الأطراف المعنية، يجب إجراء فحص واكتشاف الثغرات المكتشفة مرة أخرى للتأكد من معالجتها.

3-3 يجب استخدام حزم التحديثات والإصلاحات من مصادر موثوقة وآمنة ووفقاً لسياسة حزم التحديثات والإصلاحات.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

4-3 يجب إصلاح وإغلاق الثغرات الحرجة (Critical Vulnerabilities) المكتشفة حديثاً، مع اتباع آليات إدارة التغيير المتبعة لدى جامعة الباحة. (CSCC-2-9-1-3)

5-3 في حال تعذر إصلاح وإغلاق الثغرة الأمنية لأي سببٍ كان، يجب تطبيق ضوابط أخرى مثل إيقاف تشغيل الخدمة المتعلقة بالثغرة الأمنية، أو توفير ضابط حماية بديل (Compensating Control) مثل التحكم بالوصول عن طريق جدران الحماية وغيرها من الحلول، ومراقبة الثغرة الأمنية للهجمات الفعلية، وإبلاغ فريق الاستجابة للحوادث بهذه الثغرة واحتمالية استغلالها.

4- متطلبات أخرى

1-4 يجب على جامعة الباحة التواصل والاشتراك مع مصادر أمن سيبراني موثوقة توفر المعلومات الاستباقية (Threat Intelligence)، ومجموعات خاصة ذات اهتمامات مشتركة وخبراء خارجيين في المواضيع المعنية من أجل جمع المعلومات حول التهديدات الجديدة وكيفية الحد من الثغرات الموجودة. (ECC-2-10-3-5)

2-4 يجب مراجعة تطبيق متطلبات الأمن السيبراني لإدارة الثغرات التقنية لجامعة الباحة دورياً.

3-4 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لإدارة الثغرات.

4-4 يجب مراجعة هذه السياسة مرة واحدة في السنة؛ على الأقل.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** وحدة الامن السيبراني .

2- **مراجعة السياسة وتحديثها:** وحدة الامن السيبراني .

3- **تنفيذ السياسة وتطبيقها:** عمادة التعلم الالكتروني وتقنية المعلومات و وحدة الامن السيبراني .

الالتزام بالسياسة

1- يجب على عمادة التعلم الإلكتروني وتقنية المعلومات ضمان التزام جامعة الباحة بهذه السياسة بشكل دوري.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في الإلتزام بهذه السياسة

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة إدارة حوادث وتهديدات الأمن السيبراني

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة حوادث وتهديدات الأمن السيبراني الخاصة بجامعة الباحة لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-2:2024) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بجامعة الباحة، وتنطبق على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم من في جامعة الباحة.

بنود السياسة

1- المتطلبات العامة

1-1 يجب على جامعة الباحة توفير التقنيات اللازمة لتحديد حوادث الأمن السيبراني واكتشافها في الوقت المناسب أو من خلال استلام البلاغات من العاملين أو المستفيدين من خدمات جامعة الباحة وإدارتها بشكل فعال.

2-1 يجب على جامعة الباحة التعامل مع تهديدات الأمن السيبراني استباقياً باعتماد وسائل دفاع وقائية من أجل منع أو تقليل الآثار المترتبة على سرية المعلومات أو سلامتها أو توافرها.

3-1 تشمل حوادث الأمن السيبراني على سبيل المثال لا الحصر ما يلي:

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

1-3-1 التغييرات غير المصرح بها في إعدادات أجهزة المستخدمين المكتبية و/أو المحمولة، والتغييرات في إعدادات الخوادم.

2-3-1 الإصابة بالبرمجيات الضارة.

3-3-1 التغييرات في التطبيقات من حيث المظهر (المظهر غير الاعتيادي) والتعديلات على صلاحيات المستخدم مثل رفع مستوى الوصول.

4-3-1 الوصول غير المصرح به إلى البيانات، و/أو تعديلها دون تصاريح أو صلاحيات المستخدمين.

5-3-1 محاولات الحصول على معلومات يمكن استخدامها في تنفيذ الهجمات، مثل فحص منافذ الشبكة (Port Scans)، والهندسة الاجتماعية (Attacks Social Engineering)، وفحص مجال شبكة محددة (Targeted Scans Across IP Range)، وغيرها.

6-3-1 التفعيل غير المصرح به لحسابات مستخدمين موقوفة أو محذوفة.

4-1 يجب توثيق واعتماد خطة استجابة للحوادث توضح إجراءات التعامل مع حوادث الأمن السيبراني، والأدوار والمسؤوليات الخاصة بفريق الاستجابة، وصلاحيات اتخاذ القرارات الهامة، وآلية التواصل مع الجهات الداخلية والخارجية وكذلك آليات التصعيد. (ECC-2-13-3-1)

5-1 في حال اكتشاف حادثة أمن سيبراني في جامعة الباحة، يجب على فريق الاستجابة للحوادث اتخاذ الخطوات اللازمة للتعامل مع الحادثة التي تم اكتشافها فوراً والتي تشمل تحليل بيانات الحادثة وتحديد أثرها.

6-1 في حال اكتشاف حادثة أمن سيبراني، يجب تحليل المعلومات المتاحة ذات العلاقة مثل سجلات النظام والشبكة، والسجلات الصادرة من المنتجات الأمنية ذات الصلة (مثل السجلات الصادرة من حلول الحماية من البرمجيات الضارة، ومن جدار الحماية، ومن أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات).

7-1 يجب معالجة الأدلة اللازمة (على سبيل المثال، جمع الأدلة وفقاً للقيود القانونية وحمايتها من التلاعب) وينبغي توثيقها وحفظها بصورة محمية حتى لا تفقد جدواها في التحليل، ثم تحليلها دون تدميرها أو تعديل صورتها الأصلية.

8-1 في حال وقوع حادثة أمن سيبراني، يجب التحقيق في أسباب حدوثها والاستعانة بالمختصين مثل خبراء التحليل الجنائي الرقمي (Digital Forensics Analysts) وفرق الاستجابة للحوادث السيبرانية.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

1-9 يجب مراجعة خطة الاستجابة للحوادث مرة واحدة في السنة؛ على الأقل.

1-10 يجب تصنيف حوادث الأمن السيبراني بناءً على مستوى خطورتها ومدى تأثيرها على أعمال جامعة الباحة. (ECC-2-13-3-2)

1-11 يتم تصنيف حوادث الأمن السيبراني وفقاً للجدول أدناه:

جدول 1: تصنيف حوادث الأمن السيبراني

مستوى الخطورة	الوصف	الوقت المستهدف للاستجابة	الوقت المستهدف لحل الحادثة
مرتفع جداً	ضرر جسيم يؤثر بشكل مباشر على سمعة جامعة الباحة ومصداقيتها، أو يؤثر على العديد من وحدات الأعمال الوظيفية فيها أو موقع الأعمال بصورة كبيرة، مما يستدعي تفعيل إجراءات استمرارية الأعمال.	فوراً	ساعتان
مرتفع	انقطاع كبير يؤثر على وحدات الأعمال الوظيفية أو الخدمات الرئيسية أو الموقع.	ساعة	5-4 ساعات
متوسط	تأثير متوسط في سير عمل وحدات الأعمال الوظيفية أو المواقع أو أصول تقنية المعلومات، إضافة إلى تأثير يتراوح ما بين المتوسط والمرتفع على وحدات الأعمال غير الهامة في جامعة الباحة.	3-2 ساعات	9-8 ساعات
منخفض	تأثير بسيط على عدد قليل من الموارد، ويمكن تحمل الحادثة لفترة معينة من الزمن.	5 ساعات	24 ساعة

2- الإبلاغ عن حوادث الأمن السيبراني

2-1 يجب رفع الوعي الأمني للعاملين في جامعة الباحة وتوضيح مسؤولياتهم تجاه حوادث الأمن السيبراني أو التهديدات، وذلك للإبلاغ فوراً عن أي حوادث أو تهديدات متعلقة بالأمن السيبراني.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2-2 يجب على جامعة الباحة تحديد جهة اتصال داخلية للإبلاغ عن الحوادث سواءً عن طريق الهاتف أو البريد الإلكتروني.

3-2 يجب أن تحدد جامعة الباحة الحوادث والتهديدات التي يجب الإبلاغ عنها ووقت الإبلاغ عنها والأطراف التي يجب إبلاغها، مثل صاحب الصلاحية و وحدة الامن السيبراني وفرق الاستجابة للحوادث داخل جامعة الباحة والإدارات المسؤولة عن الأصول المعلوماتية والتقنية.

4-2 قبل الإفصاح عن أي معلومات متعلقة بالحوادث الأمنية إلى أطراف خارجية، يجب الحصول على الموافقات اللازمة بما يتوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

5-2 يجب إبلاغ الهيئة الوطنية للأمن السيبراني عن حوادث الأمن السيبراني. (ECC-2-13-3-3)

6-2 يجب على جامعة الباحة إطلاع الهيئة الوطنية للأمن السيبراني على تبليغات الحوادث ومؤشرات وتقارير الانتهاكات. (ECC-2-13-3-4)

3- الاستجابة للحوادث والتعافي من حوادث الأمن السيبراني

1-3 يجب على فريق الاستجابة للحوادث في وحدة الامن السيبراني كتابة تقرير مفصل عن حوادث الأمن السيبراني، ويجب أن يشمل التقرير نوع الحادثة وفئتها والعاملين الذين أبلغوا عن الحادثة أو الأدوات المستخدمة في اكتشافها، والخدمات أو الأصول أو المعلومات المتأثرة بها، وكيفية اكتشاف الحادثة، وأي وثائق أو موارد أخرى متعلقة بالحادثة.

2-3 يجب أن يتم إشراك الموردين في حل الحوادث أو استعادة الخدمات عند الحاجة.

3-3 يجب أن تتضمن إجراءات التعافي من حوادث الأمن السيبراني تحديد الثغرات التي تم استغلالها خلال الحادثة ومعالجتها بالتدابير الفنية والإدارية اللازمة، على سبيل المثال:

1-3-3 تطبيق الضوابط الأمنية الإضافية (Compensating Controls).

2-3-3 تنصيب حزم التحديثات والإصلاحات المحدثة.

3-3-3 استعادة النسخ الاحتياطية للنظام.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

4-3-3 إعادة ضبط إعدادات الأنظمة الأمنية، مثل نظام جدار الحماية وأنظمة الكشف عن الاختراق.

4-3 يجب على وحدة الامن السيبراني حفظ تقارير الحادثة (التي تتضمن معلومات حول الاختراقات الأمنية والحوادث مثل المعلومات المتعلقة بالأفراد والإدارات وأنظمة معينة و/أو منهجية الهجمات) بمكان آمن وتقييد الوصول إليها.

5-3 يجب تصعيد الحادثة، في حال عدم حلها في الوقت الزمني المحدد، وفقاً لتصنيف الحوادث وإجراءات التعامل معها وآلية التصعيد المعتمدة.

6-3 في حال تطلبت معالجة حادثة سيبرانية إجراء تغييرات على المكونات التقنية، يجب الالتزام بإجراءات إدارة التغيير المعتمدة لدى جامعة الباحة.

7-3 بعد التعامل مع الحادثة، يجب على فريق الاستجابة للحوادث في وحدة الامن السيبراني عقد اجتماعات لمناقشة الدروس المستفادة (Lessons Learned) مع الإدارات ذات العلاقة لتحسين طرق التعامل مع حوادث الأمن السيبراني في المستقبل، وكذلك التعامل مع تهديدات الأمن السيبراني استباقياً من أجل منع أو تقليل الآثار المترتبة على أعمال جامعة الباحة.

4- المعلومات الاستباقية بشأن التهديدات

1-4 يجب الاشتراك مع مقدمي المعلومات الاستباقية (Threat Intelligence) للاطلاع المستمر على الحوادث والتهديدات المتعلقة بالأمن السيبراني والتعامل مع تلك المعلومات بشكل مباشر. (ECC-2-13-3-5)

2-4 يجب حفظ المعلومات الاستباقية بشأن التهديدات وتنظيمها في قاعدة بيانات مرنة وملائمة لصياغة ملاحظات العمل والبيانات الوصفية للمؤشرات، مثل قاعدة المعرفة (Knowledge Base).

3-4 يجب تحديث أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات (Intrusion Prevention and Detection Systems) بالمعلومات الاستباقية المتعلقة بالتهديدات والتأكد من إمكانية تلك الأنظمة من اكتشاف التهديدات والتعامل معها بشكل فعال.

5- متطلبات أخرى

1-5 يجب مراجعة متطلبات الأمن السيبراني الخاصة بإدارة حوادث وتهديدات الأمن السيبراني دورياً. (ECC-2-13-4)

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2-5 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لإدارة حوادث وتهديدات الأمن السيبراني.

3-5 يجب مراجعة هذه السياسة مرة واحدة في السنة؛ على الأقل.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** وحدة الامن السيبراني .

2- **مراجعة السياسة وتحديثها:** وحدة الامن السيبراني .

3- **تنفيذ السياسة وتطبيقها:** عمادة التعلم الالكتروني وتقنية المعلومات و وحدة الامن السيبراني .

الالتزام بالسياسة

1- يجب على عمادة التعلم الإلكتروني وتقنية المعلومات ضمان التزام جامعة الباحة بهذه السياسة بشكل مستمر.

2- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في الإلتزام بهذه السياسة

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة أمن قواعد البيانات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية قواعد البيانات (Database) الخاصة بجامعة الباحة لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط ١-٣-٢ من الضوابط الأساسية للأمن السيبراني ((ECC-2:2024الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أنظمة قواعد البيانات الخاصة بجامعة الباحة، وتنطبق على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم من في جامعة الباحة.

بنود السياسة

1- البنود العامة

1-12 يجب تحديد وتوثيق جميع أنظمة قواعد البيانات المستخدمة داخل جامعة الباحة والعمل على توفير البيئة المناسبة لحمايتها من المخاطر البيئية والتشغيلية.

1-13 يجب تطوير واعتماد معايير التقنية الأمنية لأنظمة قواعد البيانات داخل جامعة الباحة وتطبيقها من قبل مشرفي قواعد البيانات.

1-14 فيما عدا مشرفي قواعد البيانات، يمنع الوصول أو التعامل المباشر مع قواعد البيانات الخاصة بالأنظمة الحساسة، ويتم ذلك من خلال التطبيقات فقط. (CSCC-2-2-1-8)

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

15-1 يتم منح حق الوصول إلى قواعد البيانات وفقاً لسياسة إدارة هويات الدخول والصلاحيات.

16-1 يمنع نسخ أو نقل قواعد البيانات الخاصة بالأنظمة الحساسة من بيئة الإنتاج إلى أي بيئة اخرى. (CSCC-2-6-1-5)

2- الإجراءات الأمنية المطلوبة لاستضافة قواعد البيانات

4-5 التحديد الواضح لمتطلبات استمرارية الأعمال والتعافي من الكوارث الخاصة بقواعد البيانات المستضافة في العقود المعنية مع مزوّد الخدمة السحابية، والتي تتضمّن الأدوار والمسؤوليات المتبادلة من حيث النسخ الاحتياطية والاستجابة للحوادث وخطة التعافي من الكوارث وغيرها.

5-5 توفير العزل المنطقي بين قواعد البيانات الخاصة بجامعة الباحة وقواعد البيانات المستضافة الأخرى.

6-5 تقييد صلاحية الوصول الإداري إلى قواعد البيانات باستخدام وسيلة تشفير مُحكَمة مثل بروتوكول النقل الأمن (SSH)، أو الشبكات الخاصة الافتراضية (VPN)، أو طبقة المنافذ الآمنة (SSL)/أمن طبقة النقل (TLS)، وذلك وفقاً لسياسة التشفير المعتمدة في جامعة الباحة.

3- المتطلبات المتعلّقة بإدارة التغييرات على أنظمة قواعد البيانات

1-3 يجب أن تتم التغييرات على قواعد البيانات (مثل ترحيل قواعد البيانات، والنقل إلى بيئة الإنتاج) وفقاً لعملية إدارة التغيير المعتمدة في جامعة الباحة.

2-3 يتم تثبيت التحديثات والإصلاحات على نظام قواعد البيانات وفقاً لسياسة إدارة حزم التحديثات والإصلاحات المعتمدة في جامعة الباحة.

3-3 التأكد من استخدام أنظمة قواعد بيانات موثوقة ومعتمدة ومرخصة.

4-3 التأكد من وجود خطة واضحة للتعافي من الكوارث خاصة بأنظمة قواعد البيانات.

5-3 يجب على جامعة الباحة توقيع اتفاقية مستوى الخدمة للدعم مع المورّدين فيما يتعلّق بنظام إدارة قواعد البيانات في بيئة الإنتاج.

6-3 تطبيق التجزئة والتشفير على قواعد البيانات المخزنة وفقاً لسياسة التصنيف وسياسة التشفير المعتمدة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

4- مراقبة سجلات الأحداث المتعلقة بنظام قواعد البيانات

4-1 تفعيل وحفظ سجلات الأحداث الخاصة بنظام قواعد البيانات وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني المعتمدة في جامعة الباحة.

4-2 يجب على وحدة الامن السيبراني مراقبة سجلات الأحداث المتعلقة بقواعد البيانات الخاصة بالأنظمة الحساسة، ومراقبة سلوك المستخدمين.

4-3 يجب على وحدة الامن السيبراني مراقبة سجلات الأحداث الخاصة بمشرفي قواعد البيانات ومراقبة سلوكهم ومراجعتها دورياً.

5- المتطلبات التشغيلية

5-1 توفير المتطلبات اللازمة لتشغيل قواعد البيانات بشكل آمن وملائم، مثل توفير بيئة مناسبة وآمنة، وتقييد الوصول المادي إلى الأنظمة والسماح بذلك للعاملين المصرح لهم فقط.

5-2 يجب على عمادة التعلم الالكتروني وتقنية المعلومات مراقبة أنظمة قواعد البيانات التشغيلية والتأكد من جودة أدائها، وتوافرها، وتوفير سعة تخزينية مناسبة، ونحوه.

5-3 مزامنة التوقيت (Clock Synchronization) مركزياً ومن مصدر دقيق وموثوق لجميع أنظمة قواعد البيانات. (ECC-2-3-3-4)

6- متطلبات أخرى

6-1 استخدام مؤشر قياس الأداء (Key Performance Indicator "KPI") لضمان التطوير المستمر لنظام إدارة قواعد البيانات.

2-6 مراجعة متطلبات الأمن السيبراني الخاصة بإدارة قواعد البيانات سنوياً على الأقل، أو في حال حدوث تغييرات في المتطلبات التشريعية أو التنظيمية أو المعايير ذات العلاقة.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** وحدة الامن السيبراني .

2- **مراجعة السياسة وتحديثها:** وحدة الامن السيبراني .

3- **تنفيذ السياسة وتطبيقها:** عمادة التعلم الالكتروني وتقنية المعلومات و وحدة الامن السيبراني .

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

الالتزام بالسياسة

1- يجب على عمادة التعلم الإلكتروني وتقنية المعلومات ضمان التزام جامعة الباحة بهذه السياسة دورياً.

2- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في الإلتزام بهذه السياسة

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة حماية تطبيقات الويب

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية تطبيقات الويب الخارجية الخاصة بجامعة الباحة، لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١٥-١ من الضوابط الأساسية للأمن السيبراني (ECC-2:2024) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع تطبيقات الويب الخارجية الخاصة بجامعة الباحة، وتنطبق على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم من في جامعة الباحة.

بنود السياسة

1- المتطلبات العامة

1-1 يجب أن تتبع تطبيقات الويب الخارجية التي يتم شراؤها أو تطويرها داخلياً مبدأ المعمارية متعددة المستويات (Multi-tier Architecture). (ECC-2-15-3-2)

2-1 يجب استخدام مبدأ المعمارية متعددة المستويات لتطبيقات الويب الخارجية للأنظمة الحساسة على ألا يقل عدد المستويات عن 3 مستويات (3-tier Architecture). (CSCC-2-12-2)

3-1 يجب التأكد من استخدام بروتوكولات الاتصالات الآمنة فقط، مثل بروتوكول نقل النص التشعبي الآمن (HTTPS) وبروتوكول نقل الملفات الآمن (SFTP) وأمن طبقة النقل (TLS) وغيرها. (ECC-2-15-3-3)

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

4-1 يجب استخدام نظام جدار الحماية لتطبيقات الويب (Web Application Firewall "WAF") لحماية تطبيقات الويب الخارجية من الهجمات الخارجية. (ECC-2-15-3-1)

5-1 يجب تطبيق العزل المنطقي لبيئة التطوير (Development Environment) وبيئة الاختبار (Testing Environment) عن بيئة الإنتاج (Production Environment).

6-1 يجب استخدام تقنيات حماية البيانات والمعلومات في تطبيقات الويب الخارجية ووفقاً لسياسة حماية البيانات والمعلومات وسياسة التصنيف.

7-1 في حال شراء تطبيقات ويب من طرف خارجي، يجب التأكد من التزام المورد بسياسات ومعايير الأمن السيبراني في جامعة الباحة.

8-1 يجب تطبيق الحد الأدنى على الأقل لمعايير أمن التطبيقات وحمايتها (Ten OWASP Top) لتطبيقات الويب الخارجية للأنظمة الحساسة. (CSCC-2-12-1-2)

2- متطلبات حق الوصول (Access Right)

1-2 يجب استخدام التحقّق من الهوية متعدّد العناصر (Multi-Factor Authentication) لعمليات دخول المستخدمين على تطبيقات الويب الخارجية، مع تحديد عناصر التحقق المناسبة وعددها بناءً على نتائج تقييم الأثر المحتمل لفشل عملية التحقق وتخطيها. (ECC-2-15-3-5)

2-2 يجب توثيق واعتماد معايير أمنية لتطوير تطبيقات الويب، وتشمل كحد أدنى إدارة الجلسات بشكل آمن (Secure Session Management) وموثوقية الجلسات (Authenticity)، وإقفالها (Lockout)، وإنهاء مهلتها (Timeout). (CSCC-2-12-1-1)

3-2 ينبغي أن يقتصر حق الوصول إلى منظومات الإنتاج، وأن يتم التحكم به وفقاً للمسؤوليات الوظيفية.

4-2 يجب نشر سياسة الاستخدام الآمن لجميع مستخدمي تطبيقات الويب الخارجية. (ECC-2-15-3-4)

3- متطلبات تطوير أو شراء تطبيقات الويب

1-3 يجب إجراء تقييم لمخاطر الأمن السيبراني عند التخطيط لتطوير أو شراء تطبيقات الويب وقبل إطلاقها في بيئة الإنتاج ووفقاً لسياسة إدارة مخاطر الأمن السيبراني المعتمدة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2-3 قبل استخدام المعلومات المحمية في بيئة الاختبار، يجب الحصول على إذن مسبق من وحدة الامن السيبراني واستخدام ضوابط مشددة لحماية تلك البيانات، مثل: تقنيات مزج البيانات (Data Scrambling) وتقنيات تعتيم البيانات (Data Masking)، وحذفها مباشرة بعد الانتهاء من استخدامها.

3-3 يجب حفظ شفرة المصدر (Source Code) بشكل آمن وتقييد الوصول إليها للمصرح لهم فقط.

4-3 يجب إجراء اختبار الاختراق لتطبيق الويب الخارجي في بيئة الاختبار وتوثيق النتائج والتأكد من معالجة جميع الثغرات قبل إطلاق التطبيق على بيئة الإنتاج.

5-3 يجب إجراء فحص الثغرات للمكونات التقنية لتطبيقات الويب والتأكد من معالجتها بتثبيت حزم التحديثات والإصلاحات المعتمدة لدى جامعة الباحة.

6-3 يجب اعتماد تطبيقات الويب من قبل اللجنة التقنية الاستشارية للتغيير (CAB) قبل إطلاقها في بيئة الإنتاج.

4- متطلبات أخرى

1-4 يجب مراجعة متطلبات الأمن السيبراني الخاصة بحماية تطبيقات الويب الخارجية دورياً. (ECC-2-15-4)

2-4 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لحماية تطبيقات الويب الخارجية.

3-4 تتم مراجعة هذه السياسة مرة واحدة في السنة؛ على الأقل.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** وحدة الامن السيبراني .

2- **مراجعة السياسة وتحديثها:** وحدة الامن السيبراني .

3- **تنفيذ السياسة وتطبيقها:** عمادة التعلم الالكتروني وتقنية المعلومات و وحدة الامن السيبراني .

الالتزام بالسياسة

1- يجب على عمادة التعلم الإلكتروني وتقنية المعلومات ضمان التزام جامعة الباحة بهذه السياسة بشكل مستمر.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في الإلتزام بهذه السياسة

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة التشفير

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان الاستخدام السليم والفعال للتشفير لحماية الأصول المعلوماتية الإلكترونية الخاصة بجامعة الباحة وللتقليل من المخاطر السيبرانية والتهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-٨-١ من الضوابط الأساسية للأمن السيبراني ((ECC-2:2024الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية الإلكترونية الخاصة بجامعة الباحة، وتنطبق على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم من في جامعة الباحة.، بما في ذلك الجهات التي تتعامل معها والأطراف الخارجية.

بنود السياسة

1- البنود العامة

1-1 يجب على جامعة الباحة تطوير وتوثيق واعتماد إجراءات ومعايير خاصة بالتشفير بناءً على حاجة العمل وعلى تقييم المخاطر في جامعة الباحة وبحيث يتوافق المستوى الأمني مع المعايير الوطنية للتشفير الصادرة من قبل الهيئة الوطنية للأمن السيبراني. وتشمل هذه الإجراءات على حلول التشفير المعتمدة والقيود المطبقة عليها (تقنياً

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

وتنظيمياً)، وطرق استخدامها وآلية إصدار المفاتيح ونشرها واستعادتها، بالإضافة إلى إدارة النسخ الاحتياطية للمفاتيح وإجراءات إتلاف مفاتيح التشفير. (ECC-2-8-3-1)

2-1 يجب تشفير البيانات أثناء النقل والتخزين بناءً على تصنيفها وحسب السياسات والإجراءات التنظيمية لجامعة الباحة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

3-1 يجب استخدام طرق وخوارزميات ومفاتيح وأجهزة تشفير محدثة وفقاً لما تصدره الهيئة بهذا الشأن. (CSCC-2-7-1-3)

4-1 يجب تشفير جميع بيانات الأنظمة الحساسة، أثناء النقل (Data-In-Transit). (CSCC-2-7-1-1)

5-1 يجب تشفير جميع بيانات الأنظمة الحساسة، أثناء التخزين (Data-at-Rest) على مستوى الملفات، وقاعدة البيانات، أو على مستوى أعمدة محددة داخل قاعدة البيانات. (CSCC-2-7-1-2)

6-1 يجب تحديد وتوثيق الأدوار والمسؤوليات المتعلقة بإدارة البنية التحتية لمفاتيح التشفير (Key Management Infrastructure "KMI")، للأدوار التالية على الأقل:

1-6-1 مسؤول مفاتيح وأنظمة التشفير (Keying Material Manager) باعتباره وحدة الامن السيبراني .

2-6-1 مشرفو التشفير المسؤولون عن حماية مفاتيح التشفير (Key Custodians).

3-6-1 الجهات المعنية بإصدار الشهادات (Certification Authorities "CAs")، بحيث تكون موثوقة وآمنة.

4-6-1 الجهات المعنية بتسجيل الشهادات (Registration Authorities "RAs")، بحيث تكون موثوقة وآمنة.

2- الاستخدام الآمن للتشفير

1-2 يجب تحديد وتوثيق كافة حلول التشفير المستخدمة (بما في ذلك الخوارزميات والبرامج والوحدات (Modules) والمكتبات (Libraries) ومكونات التشفير الأخرى) وتقييمها واعتمادها من قبل وحدة الامن السيبراني قبل تطبيقها في جامعة الباحة.

2-2 يجب التأكد من تطبيق التشفير وفقاً لحلول التشفير المعتمدة لدى جامعة الباحة.

3-2 يُمنع استخدام خوارزميات التشفير المطورة داخلياً وفقاً لدليل التشفير الخاص بمشروع أمان تطبيق الويب المفتوح (OWASP).

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2-4 يجب استخدام طرق التحقق الآمن (مثل استخدام مفاتيح التشفير العامة والتواقيع الرقمية والشهادات الرقمية) للحد من المخاطر السيبرانية ووفقاً لحلول التشفير المعتمدة في جامعة الباحة.

2-5 يجب استخدام التحقق من هوية المستخدم لنقل البيانات السرية للغاية إلى أطراف خارجية باستخدام شهادات التشفير الرقمية (Digital Certificates) المعتمدة، ووفقاً لسياسة حماية البيانات والمعلومات المعتمدة في جامعة الباحة.

2-6 يجب استخدام وسيلة تحقق من الهوية متعددة العناصر (Multi-Factor Authentication "MFA") للتحقق من صلاحية المستخدم للوصول إلى الأنظمة الحساسة وفقاً لسياسة حماية البيانات والمعلومات المعتمدة لدى جامعة الباحة، مع تحديد عناصر التحقق المناسبة بناءً على تقييم المخاطر.

3- إدارة مفاتيح التشفير

3-1 يجب إدارة مفاتيح التشفير بطريقة آمنة خلال عمليات دورة حياتها (Key Lifecycle Management) والتأكد من استخدامها بشكل سليم وفعّال. (ECC-2-8-3-2)

3-2 يجب أن يتم إصدار شهادات التشفير عن طريق جهة إصدار الشهادات الداخلية في جامعة الباحة للخدمات المحلية أو عن طريق جهة خارجية موثوقة.

3-3 يجب حفظ معلومات المفاتيح الخاصة (Private Key) في مكان آمن (وخاصة إذا كانت تستخدم للتوقيع الإلكتروني)، ومنع الوصول غير المصرح به، بما في ذلك جهات إصدار الشهادات.

3-4 يجب توفير التقنيات اللازمة لحماية مفاتيح التشفير عند تخزينها (Tamper Resistant Safe).

3-5 يجب حماية المفاتيح الخاصة (Private Key) من خلال تأمينها بكلمة مرور و/أو من خلال تخزينها على وسيط آمن، ووفقاً لإجراءات التشفير المعتمدة.

3-6 يجب تصنيف مفاتيح التشفير الخاصة باعتبارها معلومات "سرية للغاية" وفقاً لسياسة تصنيف البيانات المعتمدة في جامعة الباحة.

3-7 يجب تفعيل سجلات الأحداث لحلول إدارة مفاتيح التشفير ومراقبتها دورياً.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

3-8 يجب تحديد مدة لاستخدام مفاتيح التشفير وتاريخ الإنشاء وتاريخ الانتهاء لكل مفتاح.

3-9 يجب تجديد مفاتيح التشفير قبل انتهاء صلاحيتها.

3-10 يجب استخدام قائمة محدثة لشهادات التشفير الملغية (Certificate Revocation List) وذلك لضمان عدم استخدام شهادات التشفير منتهية الصلاحية أو التي تعرضت لانتهاك أمني في التعاملات مستقبلاً.

3-11 في حال تعرض مفتاح التشفير الخاص (Private Key) المُستخدم من قبل جامعة الباحة إلى انتهاك أمني أو في حال عدم توفر المفتاح (بسبب تلف وسائط تخزين المفاتيح)، يجب إبلاغ الجهة المعنية بإصدار الشهادات على الفور لإلغائه وإعادة إصدار مفتاح التشفير الخاص (Private Key).

3-12 يجب إلزام الجهة المعنية بإصدار الشهادات، في حال تعرضت مفاتيح التشفير الخاصة بها (Keys Private) إلى انتهاك أمني، بإبلاغ جامعة الباحة وإلغاء جميع الشهادات فوراً واستبدال المفتاح الخاص بالجهة المعنية بإصدار الشهادات.

3-13 في حال عدم إمكانية تبادل المفاتيح بشكل آمن وموثوق عبر شبكات الاتصالات، يجب نقل مفاتيح التشفير باستخدام قنوات بديلة آمنة ومستقلة (out-of-band channels).

3-14 يجب مراجعة وتحديث متطلبات طول مفاتيح التشفير بناءً على آخر التطورات التقنية ذات العلاقة مرة في السنة على الأقل وبما يتوافق مع معايير التشفير الوطنية.

3-15 مشرفو التشفير هم المسؤولون عن حماية مفاتيح التشفير (Key Custodians) وهم المصرح لهم فقط باستبدال مفاتيح التشفير عند الحاجة.

3-16 يُمنع حفظ مفاتيح التشفير على الذاكرة الرئيسية أو حفظها بنفس الأنظمة المطبق عليها التشفير. وعوضاً عن ذلك، يُوصى بحفظها على أجهزة مستقلة (Peripheral Hardware Devices)، مثل أجهزة حماية مفاتيح التشفير (Hardware Security Modules "HSM")، وأنظمة تخزين المفاتيح (Key Loaders)، أو أي أجهزة أخرى مخصصة لهذا الغرض.

4- متطلبات أخرى

4-1 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر للاستخدام السليم والفعال للتشفير.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2-4 يجب مراجعة كافة متطلبات الأمن السيبراني الخاصة بالتشفير دورياً. (ECC-2-8-4)

3-4 تتم مراجعة هذه السياسة مرة واحدة في السنة؛ على الأقل.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** وحدة الامن السيبراني .

2- **مراجعة السياسة وتحديثها:** وحدة الامن السيبراني .

3- **تنفيذ السياسة وتطبيقها:** عمادة التعلم الالكتروني وتقنية المعلومات و وحدة الامن السيبراني .

الالتزام بالسياسة

1- يجب على وحدة الامن السيبراني ضمان التزام جامعة الباحة بهذه السياسة دورياً.

2- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في الإلتزام بهذه السياسة

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة إدارة مخاطر الأمن السيبراني

الأهداف

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لإدارة مخاطر الأمن السيبراني في جامعة الباحة، وذلك وفقاً لاعتبارات سرية الأصول المعلوماتية والتقنية وتوافرها وسلامتها.

تتبع هذه السياسة المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهي متطلب تشريعي كما هو مذكور في الضابط رقم ١-٥-١ من الضوابط الأساسية للأمن السيبراني (ECC-2:2024) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية وأنظمة وأجهزة التحكم الصناعي الخاصة بجامعة الباحة وإجراءات عمل جامعة الباحة، وتنطبق على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم من في جامعة الباحة.

بنود السياسة

1- البنود العامة

1-1 يجب تطوير وتوثيق واعتماد منهجية إدارة مخاطر الأمن السيبراني (Cybersecurity Risk Management Methodology) وإجراءات إدارة مخاطر الأمن السيبراني في جامعة الباحة، ويجب مواءمتها مع الإطار الوطني لمخاطر الأمن السيبراني (National Cybersecurity Risk Management Framework) ويمكن استخدام المعايير والأطر التوجيهية المعتمدة دولياً (مثل: ISO27005، وISO31000، وNIST) في تطوير منهجية إدارة مخاطر الأمن السيبراني.

2-1 يجب أن تغطي منهجية إدارة مخاطر الأمن السيبراني بحد أدنى ما يلي:

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

1-2-1 تحديد الأصول ومعرفة أهميتها.

2-2-1 تحديد وتقييم المخاطر التي تمس أعمال أو أصول أو العاملين في جامعة الباحة (مثل: الآثار المترتبة على جامعة الباحة الناتجة عن المخاطر السيبرانية).

3-2-1 تحديد التهديدات والثغرات المتعلقة بالأمن السيبراني التي قد تؤثر على الأصول المعلوماتية والتقنية وتقييمها.

4-2-1 تحديد أساليب التعامل مع المخاطر السيبرانية.

5-2-1 ترتيب تدابير الحدّ من المخاطر السيبرانية حسب الأولية ووفق إجراءات محدّدة.

6-2-1 تصنيف مستويات المخاطر السيبرانية وتعريفها بناءً على مستوى التأثير واحتمالية حدوث التهديد لجامعة الباحة.

7-2-1 إنشاء سجل مخاطر الأمن السيبراني لتوثيق المخاطر ومتابعتها.

8-2-1 تحديد الأدوار والمسؤوليات لإدارة مخاطر الأمن السيبراني والتعامل معها.

3-1 يجب تنفيذ تقييم المخاطر دورياً لضمان حماية الأصول المعلوماتية والتقنية والتعامل مع المخاطر حسب الأولوية.

4-1 يجب أن تكون إدارة مخاطر الأمن السيبراني متوافقة مع إدارة المخاطر المؤسسية (Risk Enterprise Management "ERM") في جامعة الباحة.

2- المراحل الرئيسية لإدارة المخاطر السيبرانية

1-2 تحديد المخاطر (Risk Identification): يجب أن تُحدّد وحدة الامن السيبراني الأحداث أو الظروف التي من الممكن أن تنتهك سريّة الأصول المعلوماتية والتقنية وسلامتها وتوافرها، ويشمل ذلك على وجه الخصوص تحديد الأصول المعلوماتية والتقنية، والتهديدات التي من المحتمل أن تتعرّض لها والثغرات ذات الصلة، والضوابط المعتمدة، ومن ثمّ تحديد الآثار الناتجة عن فقدان سريّة هذه الأصول وسلامتها وتوافرها.

2-2 تقييم المخاطر (Risk Assessment):

1-2-2 يجب على وحدة الامن السيبراني تنفيذ إجراءات تقييم مخاطر الأمن السيبراني بحد أدنى في الحالات التالية:

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2-2-1-1 في المراحل الأولى من المشاريع التقنية.

2-2-1-2 قبل إجراء تغيير جوهري في البنية التقنية.

2-2-1-3 عند التخطيط للحصول على خدمات طرف خارجي.

2-2-1-4 عند التخطيط وقبل إطلاق منتجات وخدمات تقنية جديدة.

2-2-2 يجب إعادة تقييم المخاطر وتحديثها على النحو التالي:

2-2-2-1 دورياً لجميع الأصول المعلوماتية والتقنية، وسنوياً على الأقل للأنظمة الحسّاسة. (CSCC-1-1-2-1)

2-2-2-2 بعد وقوع حادث متعلّق بالأمن السيبراني ينتهك سلامة الأصول المعلوماتية والتقنية وتوافرها وسريّتها.

2-2-2-3 بعد الحصول على نتائج تدقيق مهمّة أو معلومات استباقية.

2-2-2-4 في حال التغيير على الأصول المعلوماتية والتقنية.

2-2-3 يجب أن تغطي عملية تقييم المخاطر ما يلي:

2-2-3-1 تقييم المخاطر (Risk Analysis): يجب أن تُقيّم وحدة الامن السيبراني احتمالية وقوع التهديدات والآثار الناتجة عنها، وأن تستخدم نتائج هذا التقييم لتحديد المستوى العام لهذه المخاطر. ويجب أن تعتمد وحدة الامن السيبراني منهجية كميّة (Quantitative) أو نوعيّة (Qualitative) لإجراء تقييم المخاطر.

2-2-3-2 تقدير المخاطر (Risk Evaluation): يجب أن تُقدِّر وحدة الامن السيبراني حجم المخاطر السيبرانية بالتوافق مع معايير تقدير المخاطر المؤسسية المعتمدة في جامعة الباحة، وتحديد أساليب التعامل معها حسب الأولوية.

2-3 معالجة المخاطر (Risk Treatment):

2-3-1 يجب أن تحدد وحدة الامن السيبراني خيارات معالجة المخاطر حسب القائمة التالية:

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2-1-3-1 معالجة المخاطر أو تقليلها (Risk Mitigation): معالجة أو تقليل درجة الخطر من خلال تطبيق الضوابط الأمنية اللازمة لتقليل احتمال الحدوث أو التأثير أو كليهما، والتي تساعد في احتواء المخاطر والمحافظة عليها ضمن مستويات مقبولة.

2-1-3-2 تجنّب المخاطر (Risk Avoidance): التخلص من الخطر بتجنب الاستمرار بمصدر الخطر.

2-1-3-2-1 مشاركة المخاطر أو تحويلها (Risk Transfer): مشاركة المخاطر مع طرف ثالث لديه الإمكانيات في التعامل مع المخاطر بشكل أكثر فعالية، أو التأمين على الأصول المعلوماتية والتقنية في حال تعرضها لمخاطر سيبرانية.

2-1-3-2-2 تقبّل المخاطر وتحمّلها (Risk Acceptance): مستوى الخطر مقبول ولكن يجب المراقبة باستمرار في حال حدوث تغيير.

2-3-2 يجب تحديد خيارات معالجة المخاطر وتوثيقها بناءً على نتائج تقييم المخاطر وتكلفة التنفيذ والمنافع المتوقّعة.

2-4 متابعة المخاطر (Risk Oversight):

2-4-1 لمتابعة المخاطر يجب أن تُعِدّ وحدة الامن السيبراني سجلاً للمخاطر وأن تحافظ عليه لتوثيق مخرجات عملية إدارة المخاطر. على أن يشمل بحد أدنى على المعلومات التالية:

2-1-4-1 عملية تحديد المخاطر.

2-1-4-2 نطاق المخاطر.

2-1-4-3 المسؤول أو صاحب المخاطر.

2-1-4-4 وصف للمخاطر بما في ذلك أسبابها وآثارها.

2-1-4-5 تحليل للمخاطر يُوضّح التأثيرات الناتجة عن المخاطر ونطاقها الزمني.

2-1-4-6 تقييم وتصنيف للمخاطر يشتمل على احتمالية المخاطر وحجمها وتصنيفها الإجمالي في حال حدوثها.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2-1-4-7 خطّة التعامل مع المخاطر تتضمّن إجراء التعامل معها والشخص المسؤول عنها وجدولها الزمني.

2-1-4-8 وصف الخطر المتبقي.

2-4-2 يجب استخدام مؤشر قياس الأداء (Key Performance Indicator "KPI") لضمان فعالية إدارة مخاطر الأمن السيبراني.

2-4-3 يجب على وحدة الامن السيبراني جمع الأدلة المتعلقة بحالة المخاطر السيبرانية ومراجعتها بشكل دوري.

3- مستوى المخاطر المقبول (Risk Appetite)

3-1 يجب تحديد معايير تقبّل المخاطر وتوثيقها، وفقاً لمستوى المخاطر وتكلفة معالجة الخطر مقابل تأثيره.

3-2 يجب تطبيق ضوابط إضافية من أجل تقليل المخاطر إلى مستوى مقبول في حال عدم استيفاء الخطر المتبقي لمعايير تقبّل المخاطر.

3-3 في حال تجاوز معايير تقبّل المخاطر، يتم التصعيد لصاحب الصلاحية لاتخاذ الإجراءات أو القرارات اللازمة.

4- متطلبات أخرى

4-1 يجب مراجعة منهجية وإجراءات إدارة مخاطر الأمن السيبراني وتحديثها على فترات زمنية مخطط لها (أو في حال حدوث تغييرات في المتطلبات التشريعية والتنظيمية والمعايير ذات العلاقة)، كما يجب توثيق التغييرات واعتمادها.

4-2 يجب مراجعة سياسة إدارة مخاطر الأمن السيبراني سنوياً، وتوثيق التغييرات واعتمادها.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** وحدة الامن السيبراني .

2- **مراجعة السياسة وتحديثها:** وحدة الامن السيبراني .

3- **تنفيذ السياسة وتطبيقها:** وحدة الامن السيبراني .

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

الالتزام بالسياسة

1- يجب على وحدة الامن السيبراني ضمان التزام جامعة الباحة بهذه السياسة دورياً.

2- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في الإلتزام بهذه السياسة

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية الأصول المعلوماتية والتقنية الخاصة بجامعة الباحة على خدمات الحوسبة السحابية والاستضافة Cloud Computing (Services and Hosting). وذلك، لضمان معالجة المخاطر السيبرانية أو تقليلها من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٤-٢-١ 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 الخاصة بجامعة الباحة على خدمات الحوسبة السحابية التي تتم استضافتها أو معالجتها أو إدارتها بواسطة أطراف خارجية، وتنطبق على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم من في جامعة الباحة.

بنود السياسة

1- البنود العامة

1-1 فيما يتعلق بمتطلبات توطين البيانات وسيادة البيانات وخصوصيتها، يجب على جامعة الباحة الرجوع إلى الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA) والالتزام بجميع الضوابط والمتطلبات والتوجيهات الصادرة منها، باعتبارها الجهة المختصة تنظيمياً بهذه المتطلبات في المملكة العربية السعودية. ويجب على وحدة الأمن السيبراني التنسيق مع الهيئة السعودية للبيانات والذكاء الاصطناعي بشكل دوري لضمان الامتثال لأي تحديثات أو متطلبات

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

جديدة.تُطبَق جميع متطلبات الأمن السيبراني الخاصة بالأطراف الخارجية في سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية على جميع مقدمي خدمات الحوسبة السحابية والاستضافة.

2-1 يجب على وحدة الامن السيبراني التحقق من كفاءة وموثوقية مقدم خدمات الحوسبة السحابية والاستضافة بالإضافة إلى حصوله على ترخيص ووجود سجل رسمي له داخل المملكة العربية السعودية.

3-1 يجب تطبيق متطلبات الأمن السيبراني الخاصة بخدمات الحوسبة السحابية والاستضافة وفقاً للسياسات والإجراءات التنظيمية الخاصة بجامعة الباحة والمتطلبات التشريعية والتنظيمية ذات العلاقة.

4-1 يجب على جامعة الباحة إجراء تقييم لمخاطر الأمن السيبراني المترتبة على استضافة التطبيقات أو الخدمات في الحوسبة السحابية قبل اختيار مقدم خدمات الحوسبة السحابية والاستضافة.

5-1 يجب أن يكون موقع استضافة الأنظمة الحساسة، أو أي جزء من مكوناتها التقنية، داخل جامعة الباحة، أو في خدمات الحوسبة السحابية المقدمة من قبل جهة حكومية، أو شركة وطنية محققة لضوابط الهيئة الوطنية للأمن السيبراني المتعلقة بخدمات الحوسبة السحابية والاستضافة، مع مراعاة تصنيف البيانات المستضافة. (CSCC-4-2-1-1)

6-1 يجب على وحدة الامن السيبراني تطوير وتوثيق واعتماد إجراءات خاصة باستخدام الخدمات السحابية.

7-1 يجب أن تتضمن عقود مقدمي خدمات الحوسبة السحابية والاستضافة بحد أدنى ما يلي:

1-7-1 متطلبات الأمن السيبراني وبنود اتفاقية مستوى الخدمة (Service Level Agreement "SLA").

2-7-1 بنود المحافظة على سرية المعلومات (Non-disclosure Clauses) بما في ذلك حذف البيانات وإتلافها بالاتفاق بين مقدم الخدمة وجامعة الباحة بناء على تصنيف تلك البيانات ومع مراعاة سياسة تصنيف البيانات.

3-7-1 متطلبات استمرارية الأعمال والتعافي من الكوارث.

4-7-1 يجب أن تتضمن عقود مقدمي خدمات الحوسبة السحابية والاستضافة إمكانية جامعة الباحة إنهاء الخدمة دون مبرر أو اشتراطات .

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

8-1 يجب مراجعة تطبيق متطلبات الأمن السيبراني مع مقدمي خدمات الحوسبة السحابية والاستضافة دورياً، مرة واحدة في السنة، على الأقل.

2- متطلبات الأمن السيبراني المتعلقة باستضافة/تخزين البيانات

1-2 يجب حماية بيانات جامعة الباحة من قبل مقدمي خدمات الحوسبة السحابية والاستضافة بما يتوافق مع مستوى تصنيفها، وذلك بتطبيق الضوابط الأمنية المناسبة. (ECC-1-3-2-4)

2-2 يجب على مقدمي خدمات الحوسبة السحابية والاستضافة إعادة البيانات (بصيغة قابلة للاستخدام) وحذفها بشكل غير قابل للاسترجاع عند إنهاء/انتهاء الخدمة. (ECC-4-2-3-1)

3-2 يجب على وحدة الامن السيبراني التأكد من فصل البيئة الخاصة بجامعة الباحة (ويشمل ذلك الخوادم الافتراضية، والشبكات وقواعد البيانات) عن غيرها من البيئات التابعة لجهات أخرى في خدمات الحوسبة السحابية. (ECC-4-2-3-2)

4-2 يجب الحصول على موافقة وحدة الامن السيبراني لاستضافة الأنظمة الحساسة أو أي جزء من مكوناتها التقنية.

5-2 يجب على جامعة الباحة التأكد من تطبيق متطلبات خصوصية البيانات على البيانات المستضافة في الحوسبة السحابية.

6-2 يجب تشفير البيانات والمعلومات المنقولة إلى الخدمات السحابية، أو المخزنة فيها، أو المنقولة منها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة في جامعة الباحة.

7-2 يجب على جامعة الباحة التأكد من أن مقدم خدمات الحوسبة السحابية والاستضافة يقوم بعمل النسخ الاحتياطي دورياً وحماية النسخ الاحتياطية وفقاً لسياسة النسخ الاحتياطية المعتمدة في جامعة الباحة.

8-2 يجب على جامعة الباحة التأكد من أن مقدم خدمات الحوسبة السحابية والاستضافة لا يمكنه الاطلاع على البيانات المخزنة وأن صلاحية الوصول الخاصة بمقدم الخدمة محدودة بالصلاحيات اللازمة للقيام بأنشطة إدارة خدمة الاستضافة وصيانتها، أو حسب متطلبات الأعمال.

9-2 يجب على مقدم خدمات الحوسبة السحابية والاستضافة تقييد الدخول إلى الخدمات السحابية الخاصة بجامعة الباحة على المستخدمين المصرح لهم فقط وباستخدام وسائل التحقق من هوية المستخدم وفقاً لسياسة إدارة هويات الدخول والصلاحيات المعتمدة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2-10 يجب على مقدم خدمات الحوسبة السحابية والاستضافة توفير التقنيات والأدوات اللازمة لجامعة الباحة لإدارة ومراقبة خدماتها السحابية.

2-11 يجب على وحدة الامن السيبراني وإدارة الشؤون القانونية تضمين بنود متطلبات الأمن السيبراني المتعلقة باستضافة البيانات في العقد مع مقدم خدمة الحوسبة السحابية.

3- متطلبات أخرى

3-1 يجب على جامعة الباحة التأكد من تفعيل سجلات الأحداث على الأصول المعلوماتية المستضافة.

3-2 يجب على جامعة الباحة مراقبة سجلات الأحداث الخاصة بالأمن السيبراني دورياً.

3-3 يجب على جامعة الباحة التأكد من مزامنة التوقيت (Clock Synchronization) الخاص بالبنية التحتية للخدمة السحابية مع التوقيت الخاص بجامعة الباحة.

3-4 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لحماية الأصول المعلوماتية والتقنية على خدمات الحوسبة السحابية.

3-5 يجب مراجعة متطلبات الأمن السيبراني الخاصة بخدمات الحوسبة السحابية والاستضافة دورياً.

3-6 يجب مراجعة هذه السياسة مرة واحدة في السنة؛ على الأقل.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** وحدة الامن السيبراني .

2- **مراجعة السياسة وتحديثها:** وحدة الامن السيبراني .

3- **تنفيذ وتطبيق السياسة:** عمادة التعلم الالكتروني وتقنية المعلومات و وحدة الامن السيبراني .

الالتزام بالسياسة

1- يجب على عمادة التعلم الإلكتروني وتقنية المعلومات ضمان التزام جامعة الباحة بهذه السياسة بشكل دوري.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في الإلتزام بهذه السياسة

3- قد يعرض أي

4- انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة الأمن السيبراني المتعلق بالأمن المادي

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان التأكد من أن مخاطر ومتطلبات الأمن السيبراني المتعلقة بالأمن المادي في جامعة الباحة تطبق بفعالية.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١٤-١ من الضوابط الأساسية للأمن السيبراني (ECC-2:2024) الصادرة من الهيئة الوطنية للأمن السيبراني. حيث يلزم الجهات حماية الأصول المعلوماتية والتقنية من الوصول المادي غير المصرّح به والفقدان والسرقة والتخريب، وبما يحقق سلامة وتوافر وحماية بيانات ومعلومات الفعالية.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأنظمة والأصول المعلوماتية والمعدات والأجهزة الخاصة بجامعة الباحة وتنطبق على جميع العاملين في جامعة الباحة.

بنود السياسة

1- يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية من الوصول المادي غير المصرّح به، على أن تشمل بحد أدنى ما يلي:

1-1 التحكم بالوصول للأماكن الحساسة مثل (مراكز البيانات، مراكز التعافي، أماكن معالجة المعلومات، مراكز المراقبة، غرف اتصالات الشبكة، مناطق الإمداد الخاصة بالأجهزة والمكونات التقنية).

2-1 مراقبة ومراجعة سجلات الدخول والخروج مثل (الدوائر التلفزيونية المغلقة CCTV).

3-1 حماية السجلات ومصادر المعلومات من الوصول غير المصرّح به.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

4-1 أمن واتلاف وإعادة استخدام الأصول المادية التي تحتوي على معلومات مصنّفة وتشمل (الوثائق الورقية ووسائط التخزين والحفظ).

5-1 أمن الأجهزة والمعدات داخل المباني وخارجها.

6-1 تطوير وتطبيق إجراءات الاستجابة للطوارئ وخطط الإخلاء لمباني ومرافق الجهة في حال الاشتباه أو وقوع أي حوادث مادية أو بيئية.

7-1 منع دخول السوائل والمواد الخطرة للأماكن الحساسة.

8-1 التحكم بدرجة حرارة الأماكن الحساسة للحفاظ على كفاءة أداء الأنظمة.

9-1 منع دخول الأفراد غير المصرّح لهم دخول القاعات والغرف المصنّفة والحصول على تصريح مسبق استناداً على مبدأ "الحاجة إلى المعرفة " و "الحاجة إلى الوصول" و "الحد الأدنى من الصلاحيات".

10-1 صيانة المعدات والأجهزة داخل المباني وخارجها بشكل دوري.

2- يجب تنفيذ ضوابط لحماية الكابلات الصوتية والاتصالات والشبكة والطاقة ضد الأضرار المادية، بعد دراسة المخاطر المحتملة. كما يجب أن تغطي هذه الضوابط بحد أدنى ما يلي:

1-2 حماية كابلات الاتصالات وشبكة البيانات من زراعه أجهزه تنصت (Wiretapping).

2-2 عدم تمديد كابلات الاتصالات وشبكة البيانات في مناطق تمكن أطراف خارجية من الوصول إليها.

3-2 حماية وعزل كابلات الاتصالات وشبكة البيانات بكفاءة من الضرر أو الاعتراض غير المصرح به، وضمان تمديدها عبر مناطق آمنة ومحمية.

4-2 عزل كابلات الكهرباء والطاقة عن كابلات الاتصالات وشبكة البيانات.

5-2 استخدام مصادر طاقة متعددة وغير منقطعة لدعم التشغيل المستمر للأنظمة والمرافق الحساسة (مثل مراكز البيانات)

3- تنفيذ تقييم لمخاطر الأمن المادي من قبل الجهات المسؤولة عن الأمن المادي عبر تحليل البيئة المادية والمناطق المحيطة لرصد التهديدات الأمنية وتهديدات السلامة ومعرفة مواطن الضعف ومعالجتها لحماية الأصول المعلوماتية من التعرض لهذه التهديدات.

4- على إدارة الأمن الجامعي تطوير واعتماد لائحة وإجراءات الأمن المادي والسلامة الخاصة بجامعة الباحة أو بأي حدث أو فعالية تشارك في تنظيمها. بحيث تشمل تحديداً دقيقاً للواجبات، والمهام، لتكون بمثابة إطار عام لخدمة السلامة، والوقاية، والإنقاذ، ومكافحة الحريق، والإسعاف، ودليلاً مرشداً في سبيل حماية الأرواح والأصول والمعلومات.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

5- تنفيذ المسح الأمني وتفتيش الحضور للاجتماعات المصنّفة، على أن يتم توفير أجهزة الكشف عن المعادن والمواد الخطيرة.

6- تصنيف جميع مرافق الجهة استناداً على تصنيف المعلومات التي يتم تداولها ومعالجتها فيها.

7- عدم منح الأطراف الخارجية صلاحية وصول مادي لمرافق الجهة إلا بعد تحقيق اشتراطات أمنية، على أن يتم مراقبة وصولهم ومرافقتهم في الأماكن التي تتطلب ذلك.

8- يجب أن تقتصر صلاحية إدارة نظام الوصول المادي على أشخاص بامتيازات محددة يمكن تدقيقها ومراجعتها.

9- مراجعة وتحديث صلاحيات الوصول المادي للمناطق الحساسة بشكل دوري.

10- توعية منسوبي الجهة حول أفضل الممارسات المتعلقة بالأمن المادي مثل سياسة المكتب النظيف وضمان التزامهم بها.

11- يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لمتطلبات الأمن السيبراني المتعلق بالأمن المادي.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** وحدة الامن السيبراني .

2- **مراجعة السياسة وتحديثها:** وحدة الامن السيبراني .

3- **تنفيذ السياسة وتطبيقها:** إدارة الأمن الجامعي.

الالتزام بالسياسة

1- يجب على وحدة الامن السيبراني ضمان التزام جامعة الباحة بهذه السياسة بشكل مستمر.

2- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في الإلتزام بهذه السياسة

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة إستخدام الشبكة الخاصة الافتراضية (VPN)

الأهداف

تلبي هذه السياسة حاجة جامعة الباحة إلى فرض بعض المسؤوليات أثناء انشاء مجموعة من المُستخدمين المفصولين عن بقية مُستخدمي الشبكة، وأعضاء هذه المجموعة قادرون على الاتصال فيما بينهم وكأنهم في شبكة خاصّة

كما تهدف هذه السياسة إلى تحديد الضوابط اللازمة لإستخدام الشبكة الخاصة الافتراضية قبل جامعة الباحة

بنود السياسة

1- ضوابط الشبكة الخاصة الافتراضية

- على الموظفين الذين يمتلكون امتيازات VPN ضمان عدم السماح للمستخدمين الغير مرخصين بالوصول إلى الشبكات الداخلية للجهة جامعة الباحه.
- يجب التحكم في استخدام VPN باستخدام مصادقة كلمة المرور لمرة OTP واحدة مع كلمة مرور قوية.
- Dual (split) tunnelingغير مسموح به، ومسموح بالاتصال بشبكة واحد فقط.
- يجب ان يتم إعداد Gateways VPN وإدارتها بواسطة مجموعات شبكة الجهة التشغيلية بجامعة الباحه.
- يجب على جميع أجهزة الكمبيوتر المتصلة بشبكات الجهة الداخلية عبر VPN أو أي جهاز آخر أن تستخدم أحدث برامج مكافحة الفيروسات التي تعد معيارًا للمنظمة توفير عنوان URL لهذا البرنامج وهذا يشمل أجهزة الكمبيوتر الشخصية.
- يجب ان يتم فصل مستخدمي VPN تلقائيًا عن شبكة الجهة بعد ثلاثين دقيقة من عدم الإستخدام inactivity Modeكما يجب على المستخدم تسجيل الدخول مرة أخرى لإعادة الاتصال بالشبكة
- يجب ان لا تتجاوز مدة الاتصال من خلال شبكة VPN ال 24 ساعة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

- يجب على مستخدمي أجهزة الكمبيوتر غير المملوكة لجامعة الباحة الامتثال لسياسات الشبكة والشبكة الخاصة بجامعة الباحة وتخضع لنفس القواعد واللوائح الصادرة من جامعة الباحه.
- يجب الموافقة على أي استثناء لهذه السياسة من قبل فريق Information Security مقدمًا.
- يجب على فريق Information Security بالتحقق من الامتثال لهذه السياسة وإصدار التقارير الدورية لإدارة الأمن السيبراني ممثلة ب وحدة الامن السيبراني .
- تحصيل الموافقات الإدارية اللازمة من أصحاب الصلاحيات في جامعة الباحة و وحدة الامن السيبراني .
- يجب إقرار المنسوبين بقرائة سياسة الشبكة الخاصة الافتراضية والامتثال لها.

2- الضوابط الأمنية لأجهزة المنسوبين الشخصية

يجب على (الإدارات المعنية) التأكد من تفعيل الضوابط الأمنية التالية عند إستخدام الشبكة الخاصة الافتراضية:

- استخدام قنوات تشفير الاتصال مثل "الشبكة الافتراضية الخاصة "(VPN) أو "بروتوكول طبقة المقابس الآمنة " (SSL) أو "حزمة بروتوكول الإنترنت الأمنية "(IPsec) عند الدخول إلى أنظمة الجهة من خلال أجهزة المستخدمين بعد تحصيل الموافقات الإدارية اللازمة من أصحاب الصلاحيات في جامعة الباحة
- استخدام خاصية المصادقة متعدد العوامل (Multi-Factor Authentication) عند محاولة المستخدم للدخول إلى الأنظمة والبيانات الحساسة.
- تعريف برنامج مضاد البرمجيات الخبيثة على أجهزة المستخدمين الشخصية بحيث يتم إدارة برنامج مضاد البرمجيات الخبيثة على أجهزة المستخدمين بشكل مركزي من قبل الإدارات المعنية في الجهة.
- تعريف سياسات كلمات المرور المركبة على الأجهزة الشخصية.
- مراقبة التحديثات الأمنية المحملة على أجهزة المنسوبين الشخصية، بحيث يتم خلالها إرسال تنبيهات للمستخدمين لتثبيت التحديثات الأمنية خلال فترة زمنية محددة. يجب أيضا، على الإدارات المعنية فصل أي جهاز غير محدث..

نطاق العمل وقابلية التطبيق

تنطبق هذه السياسة على على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم من في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

الأدوار والمسؤوليات

1- **راعي ومالك الوثيقة:** وحدة الامن السيبراني بجامعة الباحه .

2- **مراجعة الوثيقة وتحديثها:** وحدة الامن السيبراني بجامعة الباحه.

3- **تنفيذ الوثيقة وتطبيقها:** وحدة الامن السيبراني بجامعة الباحه.

الالتزام بالسياسة

1- يجب على وحدة الامن السيبراني ضمان التزام جامعة الباحة بهذه السياسة دورياً.

2- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في الإلتزام بهذه السياسة

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة الباحة وكذلك نظام مكافحة الجرائم المعلوماتية.

الوثائق ذات العلاقة

يتم ربط و موائمة سياسة إستخدام الأجهزة الشخصية مع التشريعات الصادرة عن الجهات المختصة بما في ذلك السياسات الصادرة عن الهيئة الوطنية للأمن السيبراني. ويتم تعبية وتوقيع النماذج المخصصه لهذا الغرض من قبل طالبي خدمة الإتصال عبر الشبكة الخاصة الإفتراضية.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة استخدام مواقع التواصل الاجتماعي

الأهداف

الغرض من هذه السياسة هو ضبط استخدام مواقع التواصل الاجتماعي التابعة لجامعة الباحة. ويجب استخدامها فيما يعود بالنفع على الجامعة ومنسوبيها وقطاعاتها المختلفة وبما لا يخل بأي شكل من الأشكال بسمعة الجامعة ومنسوبيها أو يعرضهم للمساءلة القانونية لذا يجب التأكد من اتباع سياسات النشر المذكورة في هذه الوثيقة.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم 2-4-1 من الضوابط الأساسية للأمن السيبراني ((ECC-2:2024الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة الحسابات الخاصة بالجهات التابعة لجامعة الباحة، وعلى حسابات منسوبي الجامعة ممن يمثل الجامعة رسميا أو تدل معلوماته الشخصية على انتمائه لجامعة الباحة.

تعريفات:

1. مواقع التواصل الاجتماعي :هي مواقع تتيح للمستخدمين التواصل افتراضيا ومشاركة مختلف الأحداث مثل المناسبات اليومية، والقضايا السياسية والقضايا الاجتماعية. وهذا سهل عملية نشر المحتوى المرسل من المستخدم بصيغ عدة مثل النصوص والصور وملفات الفيديو. ومن الأمثلة على مواقع التواصل الاجتماعي مواقع الفيس بوك، وتوتير، والانستجرام، سناب شات.
2. أنماط الاتصال :هي عبارة عن نوع من البروتوكولات التي تحدد العلاقة ما بين المرسل والمستقبل. وفي هذا الدليل تم تقسيم أنماط الاتصال إلى نوعين وهما:

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

- حساب أحادي التواصل - هو الحساب الذي من خلاله تستطيع الجهة نشر الأخبار فقط ولا تتفاعل مع الجمهور. يهدف هذا النوع من التواصل إلى تمكين الجهة من نشر الأخبار العامة مثل الفعاليات والإنجازات العلمية .
- حساب ثنائي التواصل - هو الحساب الذي من خلاله تستطيع الجهة التواصل مع الجمهور والرد على استفساراتهم. هذا النوع من التواصل يهدف إلى الرد على استفسارات الجمهور وفتح قناة اتصال غير تقليدية معهم فتكون الجهة أكثر قربًا لهم وأكثر معرفة لمشكلهم.

أنواع الحسابات:

تنقسم الحسابات بناءً على اعتبارات متعددة مثل مهام الجهة والمسميات الوظيفية وحاجات الجهة ومنسوبيها، وهي:

1. حساب الجهة - هو الحساب الذي ينتمي للجهة التابعة لجامعة الباحة (كلية، عمادة، مركز...)، ويحمل اسم وشعار الجهة الرسمي .
2. حساب المنصب الإداري - هو الحساب الذي من خلاله يستطيع المكلف الإداري التواصل مع الجمهور ليتسنى له الرد على الاستفسارات العامة، وهذا الحساب يرتبط بالمنصب الإداري بشكل دائم بمعنى أنه في حال انتهاء فترة التكليف الإداري للعضو الحالي فإن الحساب يستخدم من العضو الجديد.
3. حساب شخصي - هو الحساب التابع لشخص بحيث يحمل اسمه الشخصي أو يوضح انتسابه لجامعة الباحة أو يستخدم صفته (أستاذ مساعد، أستاذ مشارك، عميد، وكيل، مدير مركز ...) ولا يمكن للجامعة التحكم به .

مبادئ وتوجيهات عامة:

- لا يمكن التحدث الرسمي باسم الجامعة بدون قرار إداري صريح من الإدارة العليا للجامعة يسمح بذلك، وما يتم مشاركته قد ينعكس إيجابا أو سلبا على سمعة الجامعة أو الجهة التي ترتبط بها .
- يجب عدم نشر الوثائق أو المعلومات التي تصنف على أنها سرية أو سرية للغاية .

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

- يجب عدم نشر الوثائق أو المعلومات التي تتعلق بالجامعة في مواقع التواصل الاجتماعي إلا بعد التنسيق مع المسؤول الإعلامي بالجامعة أو الإدارة العليا للجامعة. ويجب تذكُّر أن ما تنشره يبقى متاحًا وليس بالإمكان التراجع عما تم نشره حتى لو تم إعادة صياغته أو حذفه.
- يجب التأكُّد من المعلومة قبل النشر وربطها بالمصدر وأن المعلومة ضمن نطاق المسؤولية، وتذكر أنك تتحمل مسؤولية أي شيء تشارك به.
- يجب مراعاة نظام الحقوق الفكرية الخاص بوزارة الثقافة والإعلام السعودية. ويجب مراعاة نظام مكافحة الجرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقم م/17 بتاريخ 1428/3/28 والالتزام بتطبيق ما ذكر فيه.
- لا تجوز الإساءة إلى أي شخص أو متابعة حسابات عنصرية أو إباحية أو حسابات تثير الفتن أو تتعارض مع سياسات الدولة، أو تتعارض مع مصالح الجامعة.
- يجب ألاَّ يستغل المنصب الإداري في المصالح الشخصية.

الضوابط:

حساب الجهة

- يعد حساب الجهة ملكًا خاصًا للجامعة.
- يتحمل مشرف حساب الجهة كافة المسؤولية عما ينشر.
- يعتبر حساب الجهة حسابًا أحادي التواصل، ويكون قناة تواصل لنشر الأخبار العامة المتعلقة بالجهة أو الجامعة من فعاليات وأنشطة وإنجازات اجتماعية وعلمية.
- يجب ألا يتم عمل إعادة نشر للحسابات الشخصية أو حسابات المنصب الإداري، ويمكن إعادة النشر لحسابات الجهات الأخرى بالجامعة حين توفر محتوى له ارتباط يفيد متابعي حساب الجهة.
- عدم التسويق لجهات أخرى أو أشخاص خارج الجامعة بإعادة نشر محتوى مشاركاتهم.
- عدم متابعة أي حسابات لا علاقة لها بأنشطة الجامعة أو الانضمام لأي نشاط اجتماعي.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

- يجب على مشرف حسابات التواصل الاجتماعي الخاصة بالجهة أن يخصص الوقت المناسب لمراجعة حسابات التواصل الاجتماعي الخاصة بهذه الجهة يوميا مع إضافة محتويات جديدة مرة أسبوعيا على الأقل حتى يكون الحساب فعالاً بصورة نشطة.
- يجب على مسؤول الجهة التأكد من أن المعلومات والمحتويات التي يتم نشرها على حسابات التواصل الاجتماعي مناسبة للجمهور وتعكس وجهة نظر ورؤية الجهة والجامعة.
- يجب أن يأخذ الشكل العام والمعلومات الشخصية للحساب الطابع الرسمي في العبارات والرسومات والصور المستخدمة بما لا يتنافى مع حقوق النشر الفكرية.

حساب المنصب الإداري

- يعد حساب المنصب الإداري ملكًا خاصًا للجامعة.
- يتحمل المكلف الإداري المسؤولية الكاملة عما ينشر.
- يجب أن تكون درجة تأهيل وفهم الشخص المسؤول عن الحساب عالية للقضايا التي سيتواصل بشأنها ويناقشها مع الجمهور عبر مواقع التواصل الاجتماعي ويجب استشارة المتحدث الرسمي للجامعة أو الجهة المختصة في حالة عدم معرفة الرد المناسب.
- يجب أن يكون بث الأخبار والإعلانات الحصرية من خلال حساب الجهة وليس من حساب المنصب الإداري، ويمكن من خلال حساب المنصب الإداري عمل إعادة نشر لمحتوى حساب الجهة

حساب شخصي

- لا يجوز استخدام شعار الجامعة أو أرقام التواصل الخاصة بالجامعة أو أي معلومات خاصة بالجامعة في التعريف الشخصي.
- إذا عرّف الشخص نفسه في مواقع التواصل الاجتماعي كمنسوب بالجامعة أو تم ذكر الصفة (أستاذ مساعد، أستاذ مشارك عميد، وكيل، مدير مركز ...) يجب توضيح أن الحساب يمثله كشخص ولا يمثل جامعة الباحة.
- لا يسمح بأن يتم التواصل باسم الجامعة أو تمثيلها أبدا من خلال الحساب الشخصي، فلا يحق للمكلف الاداري التواصل مع الجمهور بصفته الإدارية من خلال حسابه الشخصي.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

- لا يحق للشخص نشر الوثائق الخاصة بالجامعة من خلال حسابه الشخصي.
- لا يحق للشخص نشر الأخبار والإعلانات قبل أن تصدر عن الجهة المسؤولة أو المتحدث الرسمي باسم الجامعة.

ضوابط اختيار مشرف لإدارة حسابات مواقع التواصل الاجتماعي:

عند اختيار مشرف لإدارة حسابات التواصل الاجتماعي بالجهة (الكلية - المعهد – العمادة - الإدارة) يتم تطبيق الشروط التالية:

- المهارات اللغوية التي يملكها.
- مستوى معرفته بمواقع التواصل الاجتماعي وإلمامه بطرق التواصل التي توفرها.
- مدى استعداد الموظف للتواصل مع الجمهور في أوقات محددة مسبقاً داخل وقت الدوام من العمل الرسمي وقدرته على التعامل مع المواقف التي قد تتطلب رداً فورياً في هذه الأوقات وذلك حسب استراتيجية الجهة في الردود.
- ضرورة موافقة اللجنة التنفيذية لإدارة حسابات التواصل الاجتماعي بالجامعة على المرشح من الجهة كمشرف على الحساب.

مهام مشرف الحساب:

تحدد مهام مشرف الحساب في إطار الأمور التالية:

- قيادة مهام تصميم وتنفيذ الاستراتيجيات والسياسات الخاصة بالمشاركات في حسابات التواصل الاجتماعي (سواء الخاصة بالجهة أو الخاصة بالجامعة ككل أو التي تتضمنها هذه الوثيقة)، وتصميم مؤشرات لقياس الأداء في الحسابات حسب ما هو موضح في هذه الوثيقة.
- إنتاج المحتوى الذي سوف يستخدم على مختلف مواقع التواصل الاجتماعي، مع التركيز على محتوى الوسائط المتعددة، الذي غالبا ما يتطلب التواصل مع أقسام وإدارات الجهة المختلفة من أجل توفير المعلومات الضرورية لإنتاج المحتوى (والانتباه إلى حقوق الملكية الفكرية عند استخدام الوسائط المتعددة أو المعلومات).

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

- متابعة حسابات الجهة ومتابعة ما يذكره الجمهور عنها وما يتم نشره عن الجهة من أحداث وأنشطة وفعاليات، بالإضافة إلى تحليل ما يتم رصده، وتقديم تقارير لإدارة الجهة مع مقترحات التطوير إن وجدت. ورفع نسخة الجهة المسؤولة عن الإشراف على خطط وسياسيات استخدام مواقع التواصل الاجتماعي بالجامعة.
- قياس مؤشرات الأداء الخاصة بالجهة (الكلية- المعهد- لإدارة- العمادة) بشكل دوري (بناء على خطة زمنية يتم الاتفاق عليها على حسب نشاط الحساب) وعمل تقارير بذلك وتحليلها والرفع بها لإدارة الجهة حتى تتم الاستفادة منها، وإرسال نسخة منها إلى الجهة المسؤولة عن الإشراف على خطط وسياسات استخدام مواقع التواصل الاجتماعي بالجامعة.

ضوابط إنشاء حساب فرعي:

قد تستدعي الحاجة لإنشاء حساب فرعي لتغطية مناسبة (مثل مؤتمر أو مسابقة) ولهذا لابد من مراعاة الأمور التالية:

- نوع الحساب يخضع إلى شروط وضوابط أنواع الحسابات المذكورة سابقاً.
- عند تعيين مشرف على الحساب الفرعي فإنه يخضع لشروط المشرف على الحساب كما ذكر سابقاً.
- عندما يكون لدى الجهة برنامج متخصص أو خدمة معينة لها جمهور عريض، أو تسلسل هرمي كبير مما يتطلب وجود عدة حسابات رسمية تابعة لها، في مثل هذه الحالات تحتاج هذه الجهة أن يكون هناك تنسيق مع الجهة المسؤولة عن الإشراف على خطط وسياسات استخدام مواقع التواصل الاجتماع بالجامعة (اللجنة التنفيذية لحسابات التواصل الاجتماعي بالجامعة) في الآلية المتبعة حتى لا تتعارض رسالة الجهة من حيث التحديثات والأخبار ولضمان تناسق الرسائل التي يتم بثها.
- عند الانتهاء من الحساب الفرعي المؤقت لابد من التنسيق الجهة المسؤولة عن الإشراف على خطط وسياسات استخدام مواقع التواصل الاجتماع بالجامعة من أجل الاستفادة من المحتويات التي تم تقديمها فيه.

حذف حسابات مواقع التواصل الاجتماعي:

عند رغبة الجهة في حذف حساب من حساباتها في مواقع التواصل الاجتماعي، تطبق البنود التالية:

- ألاَّ يتم الحذف أو التعطيل بصورة مفاجئة وإنما ينبغي أن يكون ذلك تدريجيا عبر إبلاغ قرار الحذف أو التعطيل إلى المستخدمين عبر الموقع الالكتروني الرسمي وعلى نفس الحساب قبل تنفيذه بوقت مبكر بحيث لا يقل عن شهرين والتنسيق وضرورة الرفع للجنة التنفيذية لحسابات التواصل الاجتماعي بالجامعة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

- اتخاذ الترتيبات اللازمة حتى تتولى قنوات التواصل الاجتماعي الأخرى التعامل مع الخدمات التي كانت تقدم عبر الحساب الذي سوف يتم إغلاقه.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** وحدة الامن السيبراني بجامعة الباحه.

2- **مراجعة السياسة وتحديثها:** وحدة الامن السيبراني بجامعة الباحه.

3- **تنفيذ السياسة وتطبيقها:** وحدة الامن السيبراني بجامعة الباحه.

الإلتزام بالسياسة

1- يجب على وحدة الامن السيبراني ضمان إلتزام جامعة الباحة بهذه السياسة بشكل دوري.

2- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس في جامعة الباحة الإلتزام بهذه السياسة.

3- قد يُعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي؛ حسب الإجراءات المتبعة في جامعة الباحة .

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة النسخ الاحتياطي

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني في إطار متسق لتطبيقه على عملية النسخ الاحتياطي، بحيث تعطي هذه السياسة معلومات محددة للمساعدة في منع حدوث فقد في بيانات جامعة الباحه بضمان توفر نسخ احتياطية ومفيدة عند الحاجة إليها – سواء كان ذلك لمجرد استرداد ملف معين أو عند الحاجة إلى استرداد كامل لأنظمة

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم 2-9-1 من الضوابط الأساسية للأمن السيبراني ((ECC-2:2024الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع البيانات المخزنة على أنظمة وجميع أجهزة الكمبيوتر سواء أجهزة الكمبيوتر المحمولة وأجهزة سطح المكتب، وعلى جميع الخوادم التي تملكها جامعة الباحة، وتنطبق على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم من في جامعة الباحة.

بنود السياسة

1- المتطلبات العامة

1-1 يجب على جامعة الباحة تحديد البيانات الأكثر أهمية لها وذلك من خلال عملية تصنيف البيانات ومن خلال مراجعة أصول المعلومات، حيث يجب تحديد البيانات الهامة والحرجة بحيث يمكن منحها أولوية أعلى أثناء عملية النسخ الاحتياطي.

2- البيانات التي يتم نسخها احتياطياً

1-2 جميع البيانات التي تقرر جامعة الباحه أنها هامة وحساسة لأعمال **ومن ذلك بيانات** الموظفين بالجامعة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

2-2 جميع المعلومات المخزنة على خادم الملفات التابعة لجامعة الباحه وتقع على عاتق المستخدم ضمان نقل أي بيانات ذات أهمية إلى خادم الملفات.

3-2 جميع البيانات المخزنة على خوادم الشبكة، والتي قد تتضمن خوادم الويب وخوادم قواعد البيانات ووحدات التحكم في النطاق والجدران النارية وخوادم الوصول عن بعد.

3- تخزين النسخ الاحتياطي

1-3 عند التخزين في موقع بجامعة الباحه يجب أن تخزن وسائط النسخ الاحتياطي في اماكن مقاومة للحريق في منطقة مؤمنة بضوابط تحكم بالدخول.

2-3 يجب الحفاظ على الفصل الجغرافي بين أماكن حفظ النسخ الاحتياطية وموقع جامعة الباحه، بمسافة مناسبة وذلك للحماية من الحرائق أو الفيضانات أو الكوارث الإقليمية أو الكبيرة الأخرى، للابتعاد عن أي ضرر في حالة حدوث كارثة في الموقع الرئيسي.

3-3 عند نقل وسائط النسخ الاحتياطي أو حفظها خارج الموقع يجب ضمان -وبشكل معقول- عدم تعرضها للكوارث كالسرقة أو النار،كما يجب اختيار أماكن تخزين تستخدم أساليب حماية من الكوارث البيئية وتخضع للتحكم في الوصول لضمان سلامة وسائط النسخ الاحتياطي .

4-3 يسمح بالنسخ الاحتياطي عبر الإنترنت إذا كانت الخدمة تلبي المعايير المحددة هنا.

4- تكرار النسخ الاحتياطي

1-4 يجب إجراء عملية النسخ الاحتياطي على فترات منتظمة.

2-4 الآلية التي يتم بها تكرار عملية النسخ الاحتياطي هي ما يضمن استعادة البيانات بنجاح، يتعين على جامعة الباحه جدولة مواعيد مناسبة لعملية النسخ الاحتياطي متسقة مع طبيعة عمل المؤسسة؛ بحيث يمكن استعادة بيانات كافية لاستمرار العمل في حالة وقوع حادث مفاجئ، ولكي يمكن تجنب عبء لا لزوم له على المستخدمين والشبكة ومسؤول النسخ الاحتياطي.

3-4 يجب تذكير جميع الموظفين بأن كلاً منهم مسؤول بصورة شخصية عن البيانات الموجودة على أجهزة كمبيوتر سطح المكتب أو الكمبيوتر المحمول التي في عهدتهم، ويقع على عاتقهم مسؤولية تخزين جميع البيانات المهمة الموجودة لديهم على وسائط النسخ الاحتياطي المستخدمة في جامعة الباحه

4-4 يجب تحديد المستوى الذي تكون عنده المعلومات ضرورية ويتعين تخزين نسخ احتياطية لها.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

5-4 يجب اختبار وتوثيق إجراءات استعادة البيانات، كما يجب أن تحدد الوثائق من هو المسؤول عن عملية استعادة البيانات وكيف يتم تنفيذها وتحت أي ظروف يجب تنفيذها والمدة التي تستغرقها كامل العملية بدأً من الطلب وانتهاءً إلى استعادة البيانات، من المهم للغاية أن تكون الإجراءات واضحة وموجزة بحيث لا تكون مربكة ويساء تفسيرها في وقت الأزمات من قبل القراء بخلاف مسؤول النسخ الاحتياطي.

5 – الاحتفاظ بالنسخ الاحتياطي

1-5 يجب أن تحدد جامعة الباحه الوقت اللازم للاحتفاظ بالنسخ الاحتياطي، وما عدد النسخ المخزنة من البيانات المنسوخة احتياطياً الكافية للحد من المخاطر بكفاءة مع الحفاظ على البيانات المطلوبة.

2-5 يجب الاحتفاظ بنسخ احتياطية وفقًا لجدول الحفظ والتخلص من النسخ الاحتياطي، يحدد الجدول حالة البيانات فيما إذا كان يمكن التخلص منها أو إعادة تدويرها أو إبقاؤها في مخزن الأرشيف.

6- النسخ المخزنة

النسخ المخزنة يجب أن تخزن مع وصف قصير يتضمن المعلومات التالية:

6- 1تاريخ النسخ الاحتياطي / اسم المؤرِد / نوع طريقة النسخ الاحتياطي (كامل / تزايدي).

2-6 يجب الاحتفاظ بسجل للحركات المادية والإلكترونية لجميع النسخ الاحتياطية، يجب أن تشير الحركة المادية والإلكترونية للنسخ الاحتياطية إلى(النسخة الاحتياطية الأولية وطريقة نقلها إلى التخزين- أي حركة للنسخ الاحتياطية من موقع التخزين الخاص بها إلى موقع آخر).

3-6 يجب توفير النسخ المخزنة فور ورود طلب معتمد، يجب أن تتم الموافقة على طلب البيانات المخزنة من قبل شخص مخول له، يقوم بترشيحه مدير الإدارة المختصة، كما يجب أن تتضمن طلبات البيانات المخزنة ما يلي(تعبئة نموذج يوضح تفاصيل الطلب، بما في ذلك النسخة المطلوبة وأين ومتى يرغب مقدم الطلب في استلامها والغرض من طلب النسخة - الإقرار بأن النسخة الاحتياطية سيتم إرجاعها أو إتلافها فور الانتهاء من استخدامها).

4-6 تقديم إيصال تسليم كدليل على أن النسخة الاحتياطية قد تم إرجاعها.

5-6 يجب توفير مستوى حماية مناسب للمعلومات المخزنة في موقع التخزين الاحتياطي وفقاً للمعايير المطبقة في الموقع الرئيسي، كما ينبغي أن تمتد الضوابط المطبقة على وسائط النسخ الاحتياطي في الموقع الرئيسي لتشمل موقع التخزين الاحتياطي.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

7- اختبار عملية استعادة البيانات

7-1 يجب أن يتم فحص والقيام بإجراءات استعادة النسخ الاحتياطية بشكل منتظم لضمان فعاليتها وللتحقق من إمكانية استكمال اجراءات عملية الاستعادة في الوقت المحدد والإبلاغ عن قدرتها على استعادة البيانات.

7-2 يجب اختبار وسائط النسخ الاحتياطي بانتظام لضمان الاعتماد عليها للاستخدام الطارئ عند الضرورة.

7-3 يجب اختبار استعادة النسخ الاحتياطي عند إجراء أي تغيير قد يؤثر على نظام النسخ الاحتياطي.

7-4 سيتم مراجعة معلومات سجل الأحداث الناتجة من كل مهمة نسخ احتياطي يومياً للأغراض التالية:

- للتحقق من الأخطاء وتصحيحها
- لمراقبة مدة عملية النسخ الاحتياطي
- لتحسين أداء النسخ الاحتياطي حيثما أمكن

8- وسائط النسخ الاحتياطي

8-1 يجب حماية وسائط النسخ الاحتياطي من الوصول غير المصرح به أو سوء الاستخدام أو العبث بها، بما في ذلك الحماية الكافية لتجنب أي ضرر مادي ينشأ أثناء عملية نقلها أو تخزينها. لذا يجب على جميع الموظفين المسؤولين عن معالجة النسخ الاحتياطي للبيانات الآتي :

- أثبات هوية ذو صلة
- إذن تخويل ذو صلة

8-2 عند الحاجة إلى ضوابط خاصة لحماية المعلومات السرية أو الحساسة، ينبغي مراعاة ما يلي:

- استخدام أماكن تخزين آمنة
- التسليم باليد
- في الحالات الحرجة يتم تقسيم ما سيتم تسليمه إلى أجزاء يرسل كل جزء عبر طريق مختلفة عن غيره

8-3 يجب تخريد جميع وسائط النسخ الاحتياطية بشكل مناسب، يتم تخريد الوسائط والتخلص منها كما هو موضح أدناه:

- يجب تجهيز وسائط النسخ الاحتياطي للتخلص منها.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

- يجب أن لا تحتوي الوسائط على نسخ احتياطية يمكن إعادة استخدامها (فعالة).
- يجب ضمان عدم الوصول لمحتويات الوسائط الحالية أو السابقة وقراءتها أو استرجاعها من قبل طرف غير مصرح له.
- يجب العمل على أن تتلف وسائط النسخ الاحتياطي ماديا بحيث لا يمكن استعادة محتوياتها قبل التخلص منها.

4-8 أنواع معينة من وسائط النسخ الاحتياطي لها عمر وظيفي محدود، إذ أنه بعد مدة معينة من الخدمة لن يكون بالإمكان اعتبار هذه الوسائط موثوقًا بها. عند وضع وسائط النسخ الاحتياطي في الخدمة يجب تسجيل التاريخ عليها، ليتم إيقافها عن الخدمة بعد أن يتجاوز وقت استخدامها مواصفات المصنع.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** وحدة الامن السيبراني .

2- **مراجعة السياسة وتحديثها:** وحدة الامن السيبراني

3- **تنفيذ السياسة وتطبيقها:** عمادة التعلم الالكتروني وتقنية المعلومات و وحدة الامن السيبراني

الالتزام بالسياسة

1- يجب على وحدة الامن السيبراني ضمان التزام جامعة الباحة بهذه السياسة بشكل دوري.

2- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في الإلتزام بهذه السياسة

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة تصنيف المعلومات

الأهداف

الغرض من هذه السياسة هو تصف سياسة تصنيف المعلومات المبادئ التي يجب اتباعها لحماية المعلومات، وذلك من خلال تحديد كيف ولمن يمكنك نشر هذه المعلومات بتصنيف معين من أجل الحفاظ على خصوصية وسلامة وتوفر أصول المعلومات بجامعة الباحة . ومن خلال إنشاء هذا النظام، ستحدد هذه السياسات متطلبات التعامل مع البيانات لتوفير أساسيات حمايتها في جامعة الباحة .

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم 2-1-5 من الضوابط الأساسية للأمن السيبراني ((ECC-2:2024الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع البيانات أو المعلومات التي يتم إنشاؤها أو جمعها أو تخزينها أو معالجتها في جامعة الباحة، سواء كانت في شكل إلكتروني أو غير إلكتروني، وبصرف النظر عن مكان وجود هذه البيانات أو نوع الجهاز المخزنة به، وبالتالي ينبغي أن يستخدمها جميع الموظفين، والأطراف الأخرى التي تتعامل مع البيانات التي تحتفظ بها جامعة الباحة أو تخصها. كما تنطبق على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم من في جامعة الباحة.

بنود السياسة

يجب وضع جميع البيانات في جامعة الباحة في أحد التصنيفات التالية:

- **سرية مقيدة:** (تعرّف البيانات السرية على أنها عالية الحساسية، ويسبب الكشف عنها أو فقدانها أو تدميرها أضرار كبيرة لشخص أو أكثر أو جهة العمل). ويمكن أن تشمل ما يلي:

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

- البيانات الشخصية للموظفين أو العملاء في جهة العمل، مثل ارقام الهوية الوطنية وأرقام جواز السفر وأرقام رخصة القيادة، والسجلات الطبية.
- بيانات المصادقة: مثل مفاتيح التشفير الخاصة، واسم المستخدم وكلمة المرور.
- السجلات المالية: مثل أرقام الحسابات المالية.
- المواد التجارية: مثل الوثائق أو البيانات التي تكون ملكية فكرية فريدة أو محددة.
- البيانات القانونية: بما في ذلك البيانات المصرح بها للجهات القانونية فقط.

- حساسة داخلية: (وهي البيانات ذات المخاطر المنخفضة ونشرها أو فقدها أو تدميرها لن يكون له تأثير كبير على الأشخاص أو جهة العمل، ولكن لا يجوز نشرها خارج جهة العمل)، وغالباً تشتمل على ما يلي:
  - البريد الإلكتروني، معظم الرسائل يمكن حذفها أو نشرها دون أن تتسبب في أضرار (باستثناء البريد الإلكتروني من الأشخاص الذين يتم تحديدهم في التصنيف السري).
  - الوثائق والملفات التي لا تتضمن بيانات سرية.
  - أي بيانات مصنفة على أنها غير سرية. ويمكن أن تشمل معظم بيانات الأعمال، حيث أن معظم الملفات التي يتم إدارتها أو استخدامها يومياً يمكن تصنيفها على أنها حساسة. ومن أمثلة هذه البيانات محاضر الاجتماعات وخطط العمل والتقارير الداخلية للمشاريع.

- عامة (غير مقيدة): (وهي البيانات التي يمكن الكشف عنها للعامة وتشمل البيانات والملفات التي لا تعتبر حرجة بالنسبة لاحتياجات وعمليات العمل، والتي يتم نشرها عمداً لاستخدامها حيث يكون تأثيرها محايداً أو إيجابياً على جامعة الباحة، مثل المواد التوعوية أو الإعلانات).

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** وحدة الامن السيبراني .

2- **مراجعة السياسة وتحديثها:** وحدة الامن السيبراني

3- **تنفيذ السياسة وتطبيقها:** عمادة التعلم الالكتروني وتقنية المعلومات و وحدة الامن السيبراني

الالتزام بالسياسة

1- يجب على وحدة الامن السيبراني ضمان التزام جامعة الباحة بهذه السياسة بشكل دوري.

2- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في الإلتزام بهذه السياسة

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

سياسة حماية البيانات

الأهداف

الغرض من هذه السياسة هو حماية البيانات، البيانات المخزنة (الإلكترونية أو السجلات الورقية) التي تحتفظ بها جامعة الباحة، وكذلك الأشخاص الذين يستخدمونها والطرق التي يتبعونها في التعامل بها والأجهزة المستخدمة للوصول إليها، لضمان سرية البيانات، والحفاظ على معايير الجودة في حماية البيانات.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم 2-7-1 من الضوابط الأساسية للأمن السيبراني ((ECC-2:2024الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع البيانات أو المعلومات التي يتم إنشاؤها أو جمعها أو تخزينها أو معالجتها في جامعة الباحة، سواء كانت في شكل إلكتروني أو غير إلكتروني، وبصرف النظر عن مكان وجود هذه البيانات أو نوع الجهاز المخزنة به، وبالتالي ينبغي أن يستخدمها جميع الموظفين، والأطراف الأخرى التي تتعامل مع البيانات التي تحتفظ بها جامعة الباحة أو تخصها. كما تنطبق على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم من في جامعة الباحة.

بنود السياسة

- المسؤول عن البيانات
  - يجب أن تخضع جميع أصول البيانات الهامة لمسؤول ويجب أن يكون المسؤول أحد الموظفين الذي تتناسب خبرته مع قيمة الأصول التي سيتولى إدارتها وحمايتها.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

- يجب عدم تكليف موظف مسؤول رسمي للبيانات التي ليس لها تصنيف أمني وتكون ذات قيمة عملية محدودة، كما يجب التخلص من البيانات إذا لم يكن هناك حاجة قانونية أو تشغيلية لإبقائها، وينبغي تعيين المسؤولين المؤقتين لهذه البيانات داخل كل إدارة لضمان إتمام عملية التخلص منها.
- يكون منشئ المستندات الجديدة التي لها استخدام داخلي محدد على المدى القصير هو المسؤول عنها، وهذا يشمل الرسائل والخطط والجداول والتقارير، كما يجب إبلاغ جميع الموظفين بمسؤوليتهم عن الوثائق التي ينشئونها.
- يجب تعيين مسؤول موثوق وتحديد مسؤولياته بشكل واضح اتجاه أصول البيانات التي يتم استخدامها في جامعة الباحة على نطاق واسع. وينبغي أن يملك هذا الشخص القدرة على التحكم في هذه البيانات.

- تخزين البيانات:
  - يتم تخزين جميع البيانات الإلكترونية على المنظومات الخاصة بها حتى يسمح بإجراء نسخ احتياطية منتظمة.
  - يجب عدم السماح للموظفين للوصول إلى البيانات إلا بعد أعلامهم وموافقتهم على شروط الاطلاع على البيانات التي سيتعاملون معها.
  - قواعد البيانات التي تحتوي على بيانات شخصية يكون لها إجراءات محددة لإدارتها وتأمين السجلات والوثائق.

- الكشف عن البيانات :
  - في حالة مشاركة البيانات المقيدة مع جامعة الباحة أخرى، يجب الحرص في الكشف عن هذه البيانات وأن يتم بطريقة آمنة.
  - عندما يتم الإفصاح عن البيانات أو مشاركتها، يجب أن يتم ذلك فقط وفقاً لبروتوكول مشاركة البيانات الموثق أو اتفاقية تبادل البيانات.
  - يحظر الإفصاح عن البيانات المقيدة لأي جهة خارجية بدون اتفاق مسبق.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel: 966-17-7257700 Fax: 966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

صلاحيات الوصول للانترنت لمنسوبي الجامعة

نطاق العمل

تغطي هذا المعايير جميع أجهزة المستخدمين المكتبية الخاصة بجامعة الباحة و المتصلة بالشبكة السلكية. بالاضافة للأجهزة المحمولة و الهواتف المتنقلة الخاصة بمنسوبي الجامعة المتصلة بالشبكة اللاسلكية ، وينطبق على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم من في جامعة الباحة.

معايير الفتح و الاغلاق

تتبع جامعة الباحة المعايير التالية لفتح و اغلاق المواقع و التطبيقات لمنسوبيها بناء على:

1-أن تكون ضمن المجال التعليمي و الاخلاقي

2-نسبة استهلاك سرعة الانترنت خلال أوقات العمل و خارجها

3-السماح لمواقع و تطبيقات الجهات الحكومية

4-وسائل التواصل الاجتماعي مع الاخذ بالاعتبار النقطة الثانية

5-امان و موثوقية الموقع و التطبيق

6-ضمان مصلحة العمل

الية التطبيق

يتم فتح و اغلاق المواقع و التطبيقات لمنسوبي الجامعة على عدة مراحل حسب تدفق البيانات في كل من الأجهزة أدناه:

- Forcepoint Web Gateway

- Forcepoint NGFW

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

Huawei Internal FW -

و ذلك باختيار التصنيف المناسب أو تحديد المواقع و التطبيقات لكل من الموظفين و أعضاء هيئة التدريس و الطلاب كل على حدة.

الية المراجعة والتحديث

- تتم مراجعة السياسات بصورة دورية على ان تكون شهريا أو عند تحديث جذري للانظمة
- تتم المراجعة عند تأثير أي تصنيف مغلق على موقع رسمي اخر لا يمكن الوصول له
- يتم تحديث المواقع و التطبيقات في حالة الشكوى أو الطلب من قبل منسوبي الجامعة اذ لم يكن هنالك تعارض مع معايير الوصول للانترنت.
- يمكن استخدام خدمات Quota, QoS & Scheduling عند الحاجة

صلاحية الموظفين و أعضاء هيئة التدريس

المواقع المسموحة:

Business and Economy, Collaboration - Office, Education, Entertainment, Government, Health,Information Technology, Internet Communication,Miscellaneous, News and Media,Parked Domain,Productivity, Shopping, Social Organizations, Social Web - Facebook ,LinkedIn ,Twitter,Various ,YouTube ,Religion ,Society and Lifestyles,Special Events, Sports, Whats app, Telegram

المواقع الممنوعة:

Abortion , Adult Material, Drugs, Extended Protection, Gambling, Illegal or Questionable, Militancy and Extremist, Security, Violence & Weapons

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa

صلاحية الطلاب

المواقع المسموحة:

Government, Education, YouTube, Google, Twitter, Microsoft-Windows-Update, Bing, Digicert-Online-Certificate-Status-Service, Microsoft-NCSI, Apple, WhatsApp, Social Web, Avast-Update, Avira-Update, Microsoft-Office-365, TLS-1.2, TLS-1.0, Trend-Micro-Active Update, Microsoft-Online-Certificate-Status-Service, Telegram, TLS

المواقع الممنوعة:

Abortion , Adult Material, Drugs, Extended Protection, Gambling, Illegal or Questionable, Militancy and Extremist, Security, Violence & Weapons

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** وحدة الامن السيبراني .

2- **مراجعة السياسة وتحديثها:** وحدة الامن السيبراني

3- **تنفيذ السياسة وتطبيقها:** عمادة التعلم الالكتروني وتقنية المعلومات و وحدة الامن السيبراني

الالتزام بالسياسة

1- يجب على وحدة الامن السيبراني و عمادة التعلم الالكتروني وتقنية المعلومات ضمان التزام جامعة الباحة بهذه السياسة بشكل دوري.

2- يجب على جميع منسوبي جامعة الباحة من موظفين وطلاب وطالبات وأعضاء هيئة تدريس ومن في حكمهم في الإلتزام بهذه السياسة

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة الباحة.

المملكة العربية السعودية , الباحة - ص . ب (1988)
هاتف: 966-17-7257700 فاكس: 966-17-7257777
KINGDOM OF SAUDI ARABIA, Al-Baha P.O.Box(1988)
Tel:966-17-7257700 Fax:966-17-7257777
contact@bu.edu.sa @BahaUniversity bu.edu.sa