جامعة حائل
University of Ha'il

سياسة الاستخدام المقبول للأصول

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني؛ لتقليل المخاطر السيبرانية، المتعلقة باستخدام أنظمة جامعة حائل 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 ٢-١-٣ 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 بـجامعة حائل وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

١- البنود العامة

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

١-٢ 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

٢- حماية أجهزة الحاسب الآلي

٢-١ يمنع استخدام وسائط التخزين الخارجية دون الحصول على تصريح مسبق من إدارة الأمن السيبراني

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

٢-٣ يجب تأمين الجهاز قبل مغادرة المكتب وذلك بقفل الشاشة، أو تسجيل الخروج (Sign out or Lock)، سواء كانت المغادرة لفترة قصيرة أو عند انتهاء ساعات العمل.

٢-٤ يُمنع ترك أي معلومات مصنفة في أماكن يسهل الوصول إليها، أو الاطلاع عليها من قبل أشخاص غير مصرح لهم.

٢-٥ يُمنع تثبيت أدوات خارجية على جهاز الحاسب الآلي دون الحصول على إذن مسبق من عمادة تقنية المعلومات والتعليم الالكتروني.

٢-٦ يجب تبليغ إدارة الأمن السيبراني عند الاشتباه بأي نشاط قد يتسبب بضرر على أجهزة الحاسب الآلي الخاصة بـ جامعة حائل أو أصولها.

٣- الاستخدام المقبول للإنترنت والبرمجيات

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

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

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

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

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

٣-٦ يُمنع تنزيل البرمجيات والأدوات أو تثبيتها على أصول جامعة حائل دون الحصول على تصريح مسبق من عمادة تقنية المعلومات والتعليم الالكتروني.

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

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

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

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

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

٤- الاستخدام المقبول للبريد الإلكتروني ونظام الاتصالات

٤-١ يُمنع استخدام البريد الإلكتروني أو الهاتف أو الفاكس أو الفاكس الإلكتروني في غير أغراض العمل، وبما يتوافق مع سياسات الأمن السيبراني ومعاييره.

٤-٢ يُمنع تداول رسائل تتضمن محتوى غير لائق أو غير مقبول، بما في ذلك الرسائل المتداولة مع الأطراف الداخلية والخارجية.

٤-٣ يجب استخدام تقنيات التشفير عند إرسال معلومات حساسة عن طريق البريد الإلكتروني أو أنظمة الاتصالات.

٤-٤ يجب عدم تسجيل عنوان البريد الإلكتروني الخاص بـجامعة حائل في أي موقع ليس له علاقة بالعمل.

٤-٥ يجب تبليغ إدارة الأمن السيبراني عند الاشتباه بوجود رسائل بريد إلكتروني تتضمن محتوى قد يتسبب بأضرار لأنظمة جامعة حائل أو أصولها.

٤-٦ تحتفظ جامعة حائل بحقها في كشف محتويات رسائل البريد الإلكتروني بعد الحصول على التصاريح اللازمة من صاحب الصلاحية وإدارة الأمن السيبراني وفقاً للإجراءات والتنظيمات ذات العلاقة.

٤-٧ يُمنع فتح رسائل البريد الإلكتروني والمرفقات المشبوهة أو غير المتوقعة حتى وإن كانت تبدو من مصادر موثوقة.

٥- الاجتماعات المرئية والاتصالات القائمة على شبكة الإنترنت

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

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

٦- استخدام كلمات المرور

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

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

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

الأدوار والمسؤوليات

١- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.

٢- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.

٣- **تنفيذ السياسة وتطبيقها:** الإدارة العامة للموارد البشرية وجميع العاملين في جامعه حائل.

الالتزام بالسياسة

١- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة بشكل دوري.

٢- يجب على جميع العاملين في جامعة حائل الالتزام بهذه السياسة.

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

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 حائل 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-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأنظمة الخاصة بـجامعة حائل وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

البنود العامة

١-١ يجب تحديد متطلبات الأمن السيبراني المتعلقة بالعاملين.

٢-١ يجب أن يشغل الوظائف ذات العلاقة بالأنظمة الحساسة في جامعة حائل مواطنون ذو الكفاءة اللازمة.

٣-١ يجب تنفيذ ضوابط الأمن السيبراني الخاصة بالموارد البشرية خلال دورة حياة عمل الموظف (Lifecycle) في جامعة حائل والتي تشمل المراحل التالية:

- قبل التوظيف
- خلال فترة العمل
- عند انتهاء فترة العمل أو إنهائها

٤-١ يجب على العاملين في جامعة حائل فهم أدوارهم الوظيفية، والشروط والمسؤوليات ذات العلاقة بالأمن السيبراني، والموافقة عليها.

٥-١ يجب تضمين مسؤوليات الامن السيبراني وبنود المحافظة على سرية المعلومات (Non-Disclosure Agreement) في عقود العاملين في جامعة حائل (لتشمل خلال وبعد انتهاء/إنهاء العلاقة الوظيفية مع جامعة حائل).

٦-١ يجب إدراج المخالفات ذات العلاقة بالأمن السيبراني في لائحة مخالفات الموارد البشرية في جامعة حائل.

٧-١ يُمنع الاطلاع على المعلومات الخاصة بالموظفين دون تصريح مسبق.

٨-١ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لمتطلبات الأمن السيبراني المتعلق بالموارد البشرية.

قبل التوظيف

٢-١ يجب على العاملين التعهد بالالتزام بسياسات الأمن السيبراني قبل منحهم صلاحية الوصول إلى أنظمة جامعة حائل.
٢-٢ يجب تحديد أدوار الموظفين ومسؤولياتهم مع الأخذ في الحسبان تطبيق مبدأ عدم تعارض المصالح.
٢-٣ يجب تحديد أدوار الموظفين ومسؤولياتهم المتعلقة بالأمن السيبراني في الوصف الوظيفي.
٢-٤ يجب أن تشمل الأدوار والمسؤوليات المتعلقة بالأمن السيبراني الآتي:

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

٢-٥ يجب إجراء مسح أمني للعاملين في وظائف الأمن السيبراني، والوظائف التقنية ذات الصلاحيات الهامة والحساسة، والوظائف ذات العلاقة بالأنظمة الحساسة.

أثناء العمل

٣-١ يجب تقديم برنامج توعوي، يختص بزيادة مستوى الوعي بالأمن السيبراني؛ بما في ذلك سياسات الأمن السيبراني ومعاييره، بشكل دوري.
٣-٢ يجب على إدارة الموارد البشرية إبلاغ الإدارات ذات العلاقة عن أي تغيير في أدوار العاملين أو مسؤولياتهم بهدف اتخاذ الإجراءات اللازمة المتعلقة بإلغاء صلاحيات الوصول أو تعديلها.
٣-٣ يجب التأكد من تطبيق متطلبات الأمن السيبراني الخاصة بالموارد البشرية.
٣-٤ يجب إدراج مدى الالتزام بالأمن السيبراني ضمن جوانب تقييم الموظفين.
٣-٥ يجب التأكد من تطبيق مبدأ الحاجة إلى المعرفة (Need-to-know) في تكليف المهمات.

انتهاء الخدمة أو إنهاؤها

٤-١ يجب تحديد إجراءات انتهاء الخدمة المهنية أو إنهائها بشكل يغطي متطلبات الأمن السيبراني.
٤-٢ يجب على إدارة الموارد البشرية إبلاغ الوحدات ذات العلاقة في حال اقتراب موعد انتهاء العلاقة الوظيفية أو إنهائها لاتخاذ الإجراءات اللازمة.
٤-٣ يجب التأكد من إعادة جميع الأصول الخاصة بـجامعة حائل وإلغاء صلاحيات الدخول للعاملين في آخر يوم عمل لهم وقبل حصولهم على المخالصات اللازمة.
٤-٤ يجب تحديد المسؤوليات والواجبات التي ستبقى سارية المفعول بعد انتهاء خدمة العاملين في جامعة حائل، بما في ذلك اتفاقية المحافظة على سرية المعلومات، على أن يتم إدراج تلك المسؤوليات والواجبات في جميع عقود العاملين.

الأدوار والمسؤوليات

١- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.

٢- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.

٣- **تنفيذ السياسة وتطبيقها:** إدارة الموارد البشرية.

الالتزام بالسياسة

١- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة دورياً.
٢- يجب على جميع العاملين في جامعة حائل الالتزام بهذه السياسة.
٣- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة، إلى إجراء تأديبي؛ حسب الإجراءات المتبعة في جامعة حائل.

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 حائل تطبق بفعالية.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١٤-٢-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) 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 حائل وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

١-١ يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية من الوصول المادي غير المصرّح به، على أن تشمل بحد أدنى ما يلي:

١-١ التحكم بالوصول للأماكن الحساسة مثل (مراكز البيانات، مراكز التعافي، أماكن معالجة المعلومات، مراكز المراقبة، غرف اتصالات الشبكة، مناطق الإمداد الخاصة بالأجهزة والمكونات التقنية).

١-٢ مراقبة ومراجعة سجلات الدخول والخروج مثل (الدوائر التلفزيونية المغلقة CCTV).

١-٣ حماية السجلات ومصادر المعلومات من الوصول غير المصرّح به.

١-٤ أمن واتلاف وإعادة استخدام الأصول المادية التي تحتوي على معلومات مصنّفة وتشمل (الوثائق الورقية ووسائط التخزين والحفظ).

١-٥ أمن الأجهزة والمعدات داخل المباني وخارجها.

١-٦ تطوير وتطبيق إجراءات الاستجابة للطوارئ وخطط الإخلاء لمباني ومرافق الجهة في حال الاشتباه أو وقوع أي حوادث مادية أو بيئية.

١-٧ منع دخول السوائل والمواد الخطرة للأماكن الحساسة.

١-٨ التحكم بدرجة حرارة الأماكن الحساسة للحفاظ على كفاءة أداء الأنظمة.

١-٩ 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".

١-١٠ صيانة المعدات والأجهزة داخل المباني وخارجها بشكل دوري.

١-٢ 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:

١-٢-١ حماية كابلات الاتصالات وشبكة البيانات من زراعه أجهزه تنصت (Wiretapping).

٢-٢-١ عدم تمديد كابلات الاتصالات وشبكة البيانات في مناطق تمكن أطراف خارجية من الوصول إليها.

٣-٢-١ حماية وعزل كابلات الاتصالات وشبكة البيانات بكفاءة من الضرر أو الاعتراض غير المصرح به، وضمان تمديدها عبر مناطق آمنة ومحمية.

٤-٢-١ عزل كابلات الكهرباء والطاقة عن كابلات الاتصالات وشبكة البيانات.

٥-٢-١ استخدام مصادر طاقة متعددة وغير منقطعة لدعم التشغيل المستمر للأنظمة والمرافق الحساسة (مثل مراكز البيانات)

١-٣ 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.

١-٤ على إدارة الأمن والسلامة تطوير واعتماد لائحة وإجراءات الأمن المادي والسلامة الخاصة بـجامعة حائل 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.

١-٥ تنفيذ المسح الأمني وتفتيش الحضور للاجتماعات المصنّفة، على أن يتم توفير أجهزة الكشف عن المعادن والمواد الخطيرة.

١-٦ تصنيف جميع مرافق الجهة استناداً على تصنيف المعلومات التي يتم تداولها ومعالجتها فيها.

١-٧ 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.

١-٨ يجب أن تقتصر صلاحية إدارة نظام الوصول المادي على أشخاص بامتيازات محددة يمكن تدقيقها ومراجعتها.

١-٩ مراجعة وتحديث صلاحيات الوصول المادي للمناطق الحساسة بشكل دوري.

١-١٠ توعية منسوبي الجهة حول أفضل الممارسات المتعلقة بالأمن المادي مثل سياسة المكتب النظيف وضمان التزامهم بها.

١-١١ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لمتطلبات الأمن السيبراني المتعلق بالأمن المادي.

الأدوار والمسؤوليات

١- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.
٢- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني بجامعه حائل.
٣- **تنفيذ السياسة وتطبيقها:** مدير إدارة الأمن والسلامة .

الالتزام بالسياسة

١- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة دورياً.
٢- يجب على جميع العاملين في جامعة حائل الالتزام بهذه السياسة.
٣- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة، إلى إجراء تأديبي؛ حسب الإجراءات المتبعة في جامعة حائل .

سياسة أمن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية

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 (Mobile Devices)، والأجهزة الشخصية للعاملين (Bring Your Own Device "BYOD") داخل جامعة حائل، 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-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية للعاملين داخل جامعة حائل وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

١- البنود العامة

١-١ 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.

١-٢ 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 حائل.

١-٣ يجب تطبيق ضوابط الإعدادات والتحصين (Configuration and Hardening) لأجهزة المستخدمين والأجهزة المحمولة وفقاً لمعايير الأمن السيبراني.

١-٤ يجب عدم منح العاملين صلاحيات هامة وحساسة (Privileged Access) على أجهزة المستخدمين والأجهزة المحمولة، ويجب منح الصلاحيات وفقاً لمبدأ الحد الأدنى من الصلاحيات والامتيازات.

١-٥ يجب حذف أو إعادة تسمية حسابات المستخدم الافتراضية في أنظمة التشغيل والتطبيقات.

١-٦ يجب مزامنة التوقيت (Clock Synchronization) مركزياً ومن مصدر دقيق وموثوق لجميع أجهزة المستخدمين والأجهزة المحمولة.

١-٧ يجب تزويد أجهزة المستخدمين والأجهزة المحمولة برسالة نصيّة (Banner) لإتاحة الاستخدام المصرّح به.

١-٨ يجب السماح فقط بقائمة محددة من التطبيقات (Application Whitelisting) ومنع تسرّب البيانات (Data Leakage Prevention) واستخدام أنظمة مراقبة البيانات وغيرها.

١-٩ يجب تشفير وسائط التخزين الخاصة بأجهزة المستخدمين والأجهزة المحمولة الهامة والحساسة والتي لها صلاحيات متقدمة وفقاً لمعيار التشفير المعتمد في جامعة حائل.

١-١٠ يجب منع استخدام وسائط التخزين الخارجية، ويجب الحصول على إذن مسبق من إدارة الأمن السيبراني لامتلاك صلاحية استخدام وسائط التخزين الخارجية.

١-١١ 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 حائل لمنع التهديدات الأمنية الناشئة عن البرمجيات منتهية الصلاحية غير المحمية بحزم التحديثات والإصلاحات.

١-١٢ يجب أن تُمنَع أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD) غير المزوّدة بأحدث برمجيات الحماية من الاتصال بشبكة جامعة حائل 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 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

١-١٣ يجب ضبط إعدادات أجهزة المستخدمين والأجهزة المحمولة غير المستخدمة بحيث تعرض شاشة توقّف محمية بكلمة مرور في حال عدم استخدام الجهاز (Session Timeout) لمدة ٣ دقائق.

١-١٤ يجب إدارة أجهزة المستخدمين والأجهزة المحمولة مركزياً من خلال خادم الدليل النشط (Active Directory) الخاص بنطاق جامعة حائل أو نظام إداري مركزي.

١-١٥ يجب ضبط إعدادات أجهزة المستخدمين والأجهزة المحمولة بإدارة الوحدات التنظيمية المناسبة (Domain Controller) لتطبيق السياسات الملائمة وتثبيت الإعدادات البرمجية اللازمة.

١-١٦ يجب تنفيذ سياسات النطاق المناسبة (Group Policy) في جامعة حائل وتطبيقها في جميع أجهزة المستخدمين والأجهزة المحمولة لضمان التزام جامعة حائل بالضوابط التنظيمية والأمنية.

٢- متطلبات الأمن السيبراني لأمن أجهزة المستخدمين

٢-١ 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.

٢-٢ 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.

٢-٣ يجب تأمين أجهزة المستخدمين مادياً داخل مباني جامعة حائل.

٣- متطلبات الأمن السيبراني لأمن الأجهزة المحمولة

٣-١ يجب منع وصول الأجهزة المحمولة إلى الأنظمة الحساسة إلا لفترة مؤقتة فقط، وذلك بعد إجراء تقييم المخاطر وأخذ الموافقات اللازمة من إدارة الأمن السيبراني. (CSCC-2-5-1-1)

٢-٣ يجب تشفير أقراص الأجهزة المحمولة التي تملك صلاحية الوصول للأنظمة الحساسة تشفيراً كاملاً (Full Disk Encryption). (CSCC-2-5-1-2)

٤- متطلبات الأمن السيبراني لأمن الأجهزة الشخصية (BYOD)

١-٤ يجب إدارة الأجهزة المحمولة مركزياً باستخدام نظام إدارة الأجهزة المحمولة (Mobile Device Management "MDM").

٢-٤ يجب فصل وتشفير البيانات والمعلومات الخاصة بـجامعة حائل المخزنة على الأجهزة الشخصية للعاملين (BYOD).

٥- متطلبات أخرى

١-٥ إجراء نسخ احتياطي دوري للبيانات المخزّنة على أجهزة المستخدمين والأجهزة المحمولة، وذلك وفقاً لسياسة النسخ الاحتياطية المعتمدة في جامعة حائل.

٢-٥ تُحذَف بيانات جامعة حائل المُخزّنة على الأجهزة المحمولة والأجهزة الشخصية (BYOD) في الحالات التالية:

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

٣-٥ يجب نشر الوعي الأمني للعاملين حول آلية استخدام الأجهزة ومسؤولياتهم تجاهها وفقاً لسياسة الاستخدام المقبول المعتمدة في جامعة حائل وإجراء جلسات توعية خاصة بالمستخدمين ذوي الصلاحيات الهامة والحساسة.

٤-٥ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لحماية أجهزة المستخدمين والأجهزة المحمولة.

٥-٥ يجب مراجعة سياسة أمن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية سنوياً، وتوثيق التغييرات واعتمادها.

الأدوار والمسؤوليات

١- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.
٢- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.
٣- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الالكتروني.

الالتزام بالسياسة

١- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة دورياً.
٢- يجب على عمادة تقنية المعلومات والتعليم الالكتروني و إدارة الأمن السيبراني في جامعة حائل الالتزام بهذه السياسة.
٣- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية

الأهداف

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

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-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تنطبق هذه السياسة على جميع الخدمات المقدمة من الأطراف الخارجية لـجامعة حائل، وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

١- البنود العامة

١-١ يجب توثيق واعتماد إجراءات موحدة لإدارة علاقة جامعة حائل مع الأطراف الخارجية قبل وأثناء وبعد انتهاء العلاقة التعاقدية.

١-٢ يجب تحديد واختيار الأطراف الخارجية المقدمة للخدمات بعناية ووفقاً للسياسات والإجراءات التنظيمية لـجامعة حائل، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٣ يجب إجراء تقييم للمخاطر على الأطراف الخارجية والخدمات المقدمة والـتأكد من سلامتها، وذلك بمراجعة مشاريع الأطراف الخارجية داخل جامعة حائل ومراجعة سجلات الأحداث السيبرانية الخاص بخدمة الطرف الخارجي (إن أمكن) قبل وأثناء العلاقة وبشكل دوري.

١-٤ يجب إعداد العقود والاتفاقيات مع الأطراف الخارجية بشكل يضمن التزام الطرف الخارجي بتطبيق متطلبات وسياسات الأمن السيبراني لـجامعة حائل والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٥ يجب مراجعة العقود والاتفاقيات مع الأطراف الخارجية من قبل الإدارة القانونية للتأكد من أن تكون بنود الاتفاقية ملزمة أثناء فترة العقد وبعد انتهاءها وأن مخالفتها يعرض الطرف الخارجي للمساءلة قانونياً.

١-٦ يجب أن تشمل العقود والاتفاقيات على بنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) والحذف الآمن من قِبَل الطرف الخارجي لبيانات جامعة حائل عند انتهاء الخدمة.

١-٧ يجب مراجعة متطلبات الأمن السيبراني مع الأطراف الخارجية بشكل دوري.

١-٨ يجب مراجعة سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية سنوياً، وتوثيق التغييرات واعتمادها.

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

٢-١ للحصول على خدمات إسناد لتقنية المعلومات أو خدمات مدارة، فإنه يجب اختيار الطرف الخارجي بعناية، ويجب أن يتم التحقق من الآتي:

٢-١-١ إجراء تقييم لمخاطر الأمن السيبراني، والتأكد من وجود ما يضمن السيطرة على تلك المخاطر، قبل توقيع العقود والاتفاقيات أو عند تغيير المتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-١-٢ 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)

٢-١-٣ خدمات الإسناد على الأنظمة الحساسة يجب أن تكون عن طريق شركات وجهات وطنية، وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة. (CSCC-4-1-1-2)

٣- متطلبات الأمن السيبراني المتعلقة بموظفي الأطراف الخارجية

٣-١ 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)

٣-٢ 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 حائل).

٤- التوثيق وضوابط الوصول

٤-١ 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 حائل بما يتماشى مع متطلّبات الأمن السيبراني وأهداف ضوابط الأمن السيبراني الخاصة بـ جامعة حائل.

٤-٢ يجب توفير إمكانية الوصول إلى معلومات جامعة حائل ومعالجتها بطريقة آمنة ومراقبة.

٤-٣ يجب تطبيق الضوابط المتعلّقة بكلمات المرور على جميع المستخدمين الذين يملكون حق الوصول إلى معلومات جامعة حائل بما يتماشى مع متطلّبات الأمن السيبراني وأهداف ضوابط الأمن السيبراني الخاصة بـ جامعة حائل.

٤-٤ يجب تطبيق نظام التحقّق من الهوية متعدّد العناصر على إمكانية الوصول إلى الأنظمة الحسّاسة التي تُعالج المعلومات الخاصة بـ جامعة حائل أو تنقلها أو تُخزّنها.

٤-٥ 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 حائل أو في حال تغيير دوره الوظيفي الذي لا يتطلّب استمرارية وصوله إليها.

٤-٦ يجب أن تقوم الأطراف الخارجية بمراجعة حقوق الوصول بوتيرة دورية وفقًا لسياسات الأمن السيبراني المعتمدة في جامعة حائل.

٤-٧ يجب تخزين كلّ سجلات التدقيق والحفاظ عليها وتوفيرها بناءً على طلب جامعة حائل.

٥- متطلبات الأمن السيبراني المتعلقة بإدارة التغيير

٥-١ يجب أن تتبع الأطراف الخارجية عملية إدارة التغيير الرسمية والمناسبة وفقاً لسياسات وإجراءات جامعة حائل وبما يتوافق مع متطلّبات الأمن السيبراني.

٢-٥ يجب مراجعة واختبار التغيير التي أجريت على الأصول المعلوماتية والتقنية الخاصة بـجامعة حائل قبل تطبيقها على بيئة الإنتاج (Production Environment).

٣-٥ يجب إبلاغ الأطراف المعنية في جامعة حائل بالتغييرات الرئيسية التي مخطط إجراءها وكذلك التي أجريت على الأصول المعلوماتية والتقنية الخاصة بـجامعة حائل.

٦- متطلبات إدارة حوادث الأمن السيبراني واستمرارية الأعمال

١-٦ يجب ان تتضمن بنود العقود والاتفاقيات مع الأطراف الخارجية على متطلبات متعلقة بالإبلاغ عن حوادث الأمن السيبراني وإبلاغ جامعة حائل في حال تعرض الطرف الخارجي إلى حادثة أمن سيبراني.

٢-٦ يجب تحديد وتوثيق إجراءات التواصل بين الطرف الخارجي و جامعة حائل في حال تعرض الطرف الخارجي إلى حادثة أمن سيبراني، ومراجعة وتحديث هذه الإجراءات بشكل دوري.

٣-٦ يجب وضع خطة مناسبة لاستمرارية الأعمال لتفادي عدم توافر الخدمات المقدمة لـجامعة حائل وفقاً لمتطلّبات خطّة استمرارية الأعمال والتعافي من الكوارث الخاصة بـجامعة حائل.

٧- متطلبات حماية البيانات والمعلومات

١-٧ يجب أن تقوم الأطراف الخارجية بمعالجة بيانات ومعلومات جامعة حائل وتخزينها وإتلافها وفقاً لسياسة ومعيار حماية البيانات والمعلومات المعتمدين في جامعة حائل.

٢-٧ يجب تطبيق ضوابط تشفير مناسبة لحماية بيانات ومعلومات جامعة حائل وضمان الحفاظ على سريّتها وسلامتها وتوافرها وفقاً لمعيار التشفير المعتمد في جامعة حائل.

٣-٧ يجب عمل نُسخ احتياطية من بيانات ومعلومات جامعة حائل بشكل دوري ووفقاً لسياسة إدارة النسخ الاحتياطية الخاصة بـجامعة حائل.

٤-٧ يجب عدم معالجة أو تخزين أو استخدام بيانات ومعلومات جامعة حائل 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)

٥-٧ يجب عدم نقل بيانات ومعلومات جامعة حائل الموجودة في الأنظمة الحسّاسة - والتي تُعالجها الأطراف الخارجية - خارج بيئة الإنتاج. (CSCC-2-6-1-5)

٦-٧ يجب تصنيف بيانات ومعلومات جامعة حائل الموجودة في الأنظمة الحسّاسة - والتي تُعالجها الأطراف الخارجية - وفقاً لسياسة تصنيف البيانات والمعلومات المعتمدة في جامعة حائل. (CSCC-2-6-1-2)

٨- التدقيق

١-٨ يجب أن تُجري جامعة حائل تدقيقًا للعمليات والأنظمة ذات الصلة متى كان ذلك ضرورياً أو مناسباً.

٢-٨ يجب أن تتعاون جميع مرافق الطرف الخارجي وموظفيه بصورة كاملة مع أنشطة مراجعة سجل الأحداث والتدقيق التي تقوم بها جامعة حائل بما يشمل المراجعات المُنفّذة.

الأدوار والمسؤوليات

١- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.
٢- **تحديث السياسة ومراجعتها:** إدارة الأمن السيبراني.
٣- **تنفيذ السياسة وتطبيقها:** إدارة الأمن السيبراني وعمادة تقنية المعلومات والتعليم الالكتروني والإدارة العامة للموارد البشرية و الإدارة القانونية و إدارة المشتريات والعقود.

الالتزام بالسياسة

١- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة بشكل دوري.
٢- يجب على جميع الإدارات المعنية بتنفيذ وتطبيق السياسة في جامعة حائل الالتزام بهذه السياسة.
٣- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة لإجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

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 جامعة حائل 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 ٣-١-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) والضابط رقم ٣-١-١ 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 جامعة حائل وتنطبق على جميع العاملين في جامعة حائل .

بنود السياسة

١- يجب التأكد من استمرارية الأنظمة والإجراءات المتعلقة بالأمن السيبراني في جامعة حائل .
٢- يجب إجراء تقييم للمخاطر التي قد تؤثر على استمرارية أعمال جامعة حائل .
٣- يجب معالجة نقاط الضعف لتجنب الحوادث التي قد تؤثر على استمرارية أعمال جامعة حائل .
٤- يجب تحديد المتطلبات التشريعية والتنظيمية الخاصة باستمرارية الأعمال لدى جامعة حائل .
٥- يجب وضع خطط الاستجابة لحوادث الأمن السيبراني التي قد تؤثر على استمرارية أعمال جامعة حائل .
٦- يجب وضع خطط التعافي من الكوارث (Disaster Recovery Plan).
٧- يجب إدراج الأنظمة الحساسة لجامعة حائل ضمن خطط التعافي من الكوارث.
٨- يجب إنشاء مركز للتعافي من الكوارث للأنظمة الحساسة.
٩- يجب إجراء اختبارات دورية للتأكد من فعالية خطط التعافي من الكوارث للأنظمة الحساسة لجامعة حائل مرة واحدة سنويًا على الأقل.
١٠- يجب إجراء اختبار دوري حي للتعافي من الكوارث (Live DR Test) للأنظمة الحساسة.
١١- يجب تضمين حوادث الأمن السيبراني عالية الخطورة ضمن الأسباب الموجبة لتفعيل خطة استمرارية الأعمال في جامعة حائل .

١٢- يجب إجراء تحليل التأثير على الأعمال (Business Impact Analysis) لتحديد الأنظمة الحساسة في جامعة حائل ونسخها إلى موقع التعافي من الكوارث.
١٣- يجب تحديد متطلبات النسخ الدورية الخاصة بالأنظمة الحساسة لـجامعة حائل إلى مركز التعافي.
١٤- يجب تضمين خطط استمرارية سلاسل التوريد والإمداد ضمن خطط استمرارية أعمال جامعة حائل .
١٥- يجب تضمين طرق التواصل الخاصة بفريق الأمن السيبراني في جامعة حائل سواءً الداخلية أو الخارجية وتوثيقها.
١٦- يجب تحديد الأدوار والمسؤوليات للأطراف ذات العلاقة باستمرارية الأعمال في جامعة حائل .
١٧- يجب وضع خطط تنفيذ ومتابعة المسؤوليات والأعمال الخاصة بالأمن السيبراني خلال الكوارث ولحين عودة الأوضاع لطبيعتها.
١٨- يجب إدارة هويات الدخول والصلاحيات على جميع الأنظمة والبيانات المستضافة في موقع التعافي من الكوارث الخاص بـجامعة حائل لضمان عدم الوصول إليها من قبل الأشخاص غير المصرح لهم.
١٩- يجب تضمين متطلبات خطط التعافي من الكوارث في عقود واتفاقيات جامعة حائل مع الأطراف الخارجية ومقدمي الخدمات السحابية.
٢٠- يجب ضمان تطبيق الضوابط الأساسية للأمن السيبراني (ECC-1:2018) في بيئة مركز التعافي من الكوارث التابع لـجامعة حائل مثل: الأمن المادي، أمن الشبكة والبنية التحتية، أمن البيانات والمعلومات، التشفير، إلخ.
٢١- يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لمتطلبات الأمن السيبراني الخاصة باستمرارية أعمال الأمن السيبراني.

الأدوار والمسؤوليات

١- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني بجامعه حائل
٢- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني
٣- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الإلكتروني و إدارة الأمن السيبراني

الالتزام بالسياسة

١- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة بشكل دوري.
٢- يجب على جميع العاملين في جامعة حائل الالتزام بهذه السياسة.
٣- قد يُعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل .

سياسة إدارة الأصول

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة الأصول المعلوماتية والتقنية المملوكة لجامعة حائل. وذلك، لضمان إدارتها ومراقبتها وحمايتها واستخدامها بكفاءة وفعالية، بالإضافة إلى معالجة المخاطر السيبرانية أو تقليلها من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها. يمكن تصنيف الأصول التقنية والمعلوماتية على نطاق واسع على أنها أجهزة وبرامج ومعلومات وأشخاص.

وتهدف هذه السياسة للالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية ذات العلاقة، وهي متطلب تشريعي في الضابط رقم ١-١-٢ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أصول المعلومات المتعلقة بإدارة تقنية المعلومات التي تعود ملكيتها لجامعة حائل، وتنطبق على جميع موظفي جامعة حائل، وعلى كافة الأطراف ذات العلاقة بما في ذلك موظفي وكالات التوظيف المؤقت وشركاء الأعمال وموظفي التعاقد والوحدات الوظيفية بصرف النظر عن المواقع الجغرافية.

بنود السياسة

١- مخزون الأصول المعلوماتية والتقنية

١-١ يجب تحديد وحصر كافة الأصول المعلوماتية والتقنية المتعلقة المملوكة لجامعة حائل، وتحديثها مرة واحدة كل سنه على الأقل.

١-٢ يجب على جامعة حائل ضمان التسجيل الدقيق لكافة الأصول المعلوماتية والتقنية المملوكة للجامعة، مع بيان كافة المعلومات المتعلقة بها بشكل دقيق، بحيث تشمل المعلومات المسجلة بحد أدنى ما يلي:

- معرف الأصل (Asset Identification).
- وصف الأصل.
- موقع الأصل.
- ملكية الأصل.
- الوصي على الأصل.

١-٣ يجب على جامعة حائل تصنيف مخزون الأصول المعلوماتية إلى الفئات الرئيسية التالية:

- أجهزة (Hardware).
- برمجيات (Software).
- معلومات (Information and data).
- خدمات (Services & Utilities).
- أشخاص (People).
- أخري (Others).

١-٤ يجب على جامعة حائل ضمان الالتزام بدقة تسجيل وحيازة وتشغيل وأمن وصيانة وإهلاك كافة الأصول وأنها تنقل بين مواقع الجامعة بدقة تامة.

١-٥ يجب على عمادة تقنية المعلومات والجهات ذات العلاقة التأكد من الالتزام بممارسة السيطرة التامة على جميع الأصول المعلوماتية والتقنية من حيث (أمنها وحفظها واتخاذ التدابير اللازمة لصيانتها وتأمينها) .

١-٦ يجب أن تحتفظ عمادة تقنية المعلومات والجهات ذات العلاقة بمخزون حديث من مواد التهيئة الرئيسية (التطبيقات، البيانات، نظام التشغيل، قواعد البيانات، برامج الإصلاح Patches، الأجهزة وغيرها). ويجب أن يتم عمل مراجعة دورية للمخزون مرة واحدة سنويا على الأقل.

١-٧ يجب على جامعة حائل ضمان المراقبة الدائمة للمخزون، بما يضمن تسجيل الموقع الجديد والوصي الجديد لجميع المعدات الصادرة للآخرين، والأمن المادي على المعدات التي بحوزتهم.

١-٨ يجب على عمادة تقنية المعلومات والجهات ذات العلاقة الالتزام بتزويد إدارة الأمن السيبراني بقوائم المخزون الخاصة بالأصول المعلوماتية والتقنية عند طلبهم ذلك، وذلك لدعم عمليات تقييم المخاطر للأصول المعلوماتية والتقنية، وكذلك لدعم عمليات اتخاذ القرارات الخاصة بالأمن السيبراني.

١-٩ يجب أن تحتفظ إدارة الأمن السيبراني بقائمة المخزون لجميع أجهزة الكمبيوتر والشبكات بجامعة حائل التي تم إيقاف تشغيلها.

١-١٠ يجب على عمادة تقنية المعلومات والجهات ذات العلاقة تطوير وتوثيق واعتماد إجراءات جرد الأصول المادية، والتأكد من احتواء جميع أجهزة الكمبيوتر والاتصالات بجامعة حائل على معرف فريد يمكن قراءته بواسطة الكمبيوتر بحيث يمكن إجراء عمليات الجرد المادي بكفاءة.

٢ - ملكية الأصول

٢-١ يجب على الجامعة ضمان تخصيص وتوثيق "مالك الأصول المعلوماتية والتقنية" والذي يتولى المسؤولية النهائية عن الأصل المعلوماتي والتقني وعن القرارات الهامة التي تتعلق بالأصل، وأن يكون ذلك وفقًا للسياسات والإجراءات التنظيمية الخاصة بجامعة حائل والمتطلبات التشريعية والتنظيمية ذات العلاقة. وعلى مالكي الأصول المعلوماتية التعاون فيما بينهم لضمان تحديد الضوابط الكافية للأصول المعلوماتية التي بحوزتهم بهدف الوصول إلى مستوى منظم ومتسق من الحماية.

٢-٢ يجب الالتزام بسياسات وإجراءات ملكية البيانات والمعلومات المعتمدة من قبل إدارة البيانات بجامعة حائل والمتطلبات التشريعية والتنظيمية الوطنية ذات العلاقة والصادرة من مكتب إدارة البيانات الوطنية، عند تخصيص وتوثيق ملاك أصول البيانات والمعلومات.

٢-٣ يجب تحديد ما يلي بخصوص كل أصل من الأصول:

٢-٣-١ المالك: مدراء القطاعات- الإدارات- المكلفين الذين لهم مسؤوليات رئيسية عن الأصول المعلوماتية المرتبطة بالمهام الوظيفية الخاصة بسلطاتهم. وعندما لا يتم ذكر المالكين بوضوح ضمن التصميم التنظيمي، تقوم عمادة تقنية المعلومات بعملية تعيينه، ويكون المالكون مسؤولين عن:

- تحديد الأصول المعلوماتية.
- تخصيص التصنيفات الأمنية المناسبة للمعلومات.
- ضمان القيام بعملية عنونة ملائمة للمعلومات الحساسية.
- تعيين "الوصي" الذي تكون المعلومات بحوزته.
- ضمان التعريف بتصنيف حماية للمعلومات كما ينبغي، واستيعاب هذا التصنيف من قبل "الأوصياء" على المعلومات.
- مراجعة الأصول المعلوماتية بصورة دورية لتحديد ما إذا كانت هناك حاجة لتغيير تصنيفها.

٢-٣-٢ الوصي: المدراء، الإداريون، مزودو الخدمة، وأولئك الذين تم تعيينهم من قبل المالك لإدارة، ومعالجة، أو تخزين الأصول المعلوماتية. ويكون الأوصياء مسؤولين عن فهم التصنيفات الأمنية للمعلومات، وتطبيق الضوابط اللازمة لإدامة وحفظ تصنيفات المعلومات والعناوين التي وضعها المالكون.

٢-٣-٣ المستخدمون: الأفراد، أو المجموعات أو الهيئات، المخولة من قبل المالك بالدخول إلى الأصول المعلوماتية. ويكون المستخدمون مسؤولين عن:

- استيعاب وفهم تصنيفات الحماية، والتقيد بالضوابط التي حددها المالك وطبقها الوصي.
- إدامة وحفظ تصنيفات المعلومات وطرق عنونتها التي وضعها المالك.
- الاتصال بالمالك عندما تكون المعلومات غير معنونة، أو عند عدم معرفة التصنيف.

٣ - الاستخدام المقبول للأصول

٣-١ يجب على جامعة حائل تحديد "سياسة الاستخدام المقبول للأصول" التي تحدد إرشادات إدارة الأصول، وضمان تطبيقها بما يتوافق مع السياسات والإجراءات التنظيمية الخاصة بجامعة حائل والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٣ يجب على جميع العاملين في جامعة حائل الالتزام بكافة البنود الواردة بسياسة الاستخدام المقبول للأصول المعتمدة، كما ينبغي عليهم استخدام كافة الأصول لأغراض العمل فقط، وبما يخدم مصالح الجامعة في سياق العمليات الاعتيادية.

٣-٣ يجب ان يلتزم كافة الموظفين والمقاولين ومستخدمي الطرف الثالث بالالتزام بقواعد الاستخدام المقبول للمعلومات والأصول الخاصة بجامعة حائل التي ترتبط بتسهيلات معالجة المعلومات بما في ذلك:

- قواعد استخدام البريد الالكتروني والانترنت.
- إرشادات استخدام الأجهزة المتنقلة، وخصوصًا فيما يتعلق باستخدامها خارج مباني الجامعة.
- على كافة المستخدمين عدم الاشتراك في أية أنشطة غير قانونية كالدخول إلى الأصول غير المصرح بالدخول إليها، أو الاختراق، أو التسبب بإدخال ما يضر بالحواسيب أو إدخال الفيروسات، أو القيام بتصرفات من شأنها التسبب في تعطيل استخدام الأصول.

٤ - إعادة الأصول

٤-١ يجب على جميع الموظفين والمستخدمين الخارجيين إعادة جميع الأصول المعلوماتية والتقنية التي في حيازتهم عند إنهاء عملهم أو عقدهم أو اتفاقهم.

٤-٢ يجب أن تضمن عمادة شؤون أعضاء هيئة التدريس والموظفين بجامعة حائل بالتعاون مع الإدارات ذات الصلة ان جميع المستخدمين يعيدون جميع أصول جامعة حائل التي بحوزتهم عند إنهاء عملهم أو عقدهم او اتفاقهم. قد يشمل ذلك على سبيل المثل لا الحصر:

- عملية رسمية لإعادة الأصول المعلوماتية لجامعة حائل (مثل إخلاء طرف من الجهة المختصة بإدارة المخزون)
- عملية رسمية لإعادة أو إتلاف معلومات جامعة حائل من أي نوع.
- يجب التأكد من المسح الآمن لكافة البرامج والمعلومات الخاصة بجامعة حائل من الأجهزة والمعدات الخاصة بالمستخدم وذلك في حالة استخدام أجهزة ومعدات شخصية.
- يجب ألا يتلقى الموظفون والمؤقتون والمتعاقدون والاستشاريون رواتبهم النهائية إلا إذا أعادوا جميع الأجهزة والبرامج ومواد العمل والمعلومات السرية والممتلكات الأخرى التابعة لجامعة حائل. حيث تضمن هذه السياسة إعادة المعلومات السرية وأجهزة الكمبيوتر الشخصية والممتلكات الأخرى لجامعة حائل.
- فور مغادرة الموظفين لمنشآت جامعة حائل، يجب إزالة بطاقة التعريف الخاصة بهم وتخزينها في مكان آمن ومناسب بعيدًا عن الأنظار العامة. تمنع السياسة الموظفين من مغادرة موقع العمل وبطاقاتهم عليهم، وإخطار الجميع بشكل غير مباشر بأنهم يعملون بجامعة حائل.
- يجب على الإدارة أو الإدارات المسؤولة التأكد من سحب جميع المعلومات الموجودة في حيازة الموظف الذي تم إنهاء خدمته، ويجب التأكد من إلغاء صلاحية الوصول إليها مباشرة بعد إنهاء الخدمة.

- يجب على الموظف المنتهية خدماته نقل كافة المعلومات قبل اخر يوم عمل وتسليم جميع مهامه إلى موظف آخر والتأكد من تسليم كل شي بشكل تام.

٥ - تصنيف أصول المعلومات

٥-١ يجب تحديد مستوى تصنيف المعلومات لجميع المعلومات التي يتم الاحتفاظ بها أو تخزينها او إنتاجها من قبل جامعة حائل وفقًا لمتطلبات الحساسية، والأهمية، والسرية، والخصوصية وقيمة المعلومات وأية متطلبات تتعلق بالمعلومات.

٥-٢ يجب على إدارة البيانات بجامعة حائل تحديد سياسات وإجراءات تصنيف البيانات وفقا للمتطلبات التشريعية والتنظيمية الوطنية ذات العلاقة والصادرة من مكتب إدارة البيانات الوطنية، والالتزام بها.

٥-٣ يجب على كل الجهات ذات العلاقة الالتزام بسياسات وإجراءات تصنيف البيانات المعتمدة من قبل إدارة البيانات بجامعة حائل، عند تصنيف المعلومات.

٥-٤ يجب تصنيف كافة الأصول المعلوماتية، التي تم إنتاجها داخليًا أو خارجيًا، وفقًا لأحد التصنيفات الأربع التالية بناء على متطلبات الحساسية والخصوصية، والقيمة التي تمثلها للجامعة: سري للغاية – سري – داخلي – عام.

٥-٥ عند التعامل مع معلومات تتضمن تصنيفات مختلفة، فإنه يتم تصنيف المجموعة أو المعلومات الجديدة وفقا لأعلى تصنيف يحمله أي من هذه المعلومات.

٥-٦ ينبغي مراجعة تصنيف كل أصل من الأصول المعلوماتية من قبل مالك الأصل على فترات زمنية منتظمة أو عند حدوث تغيير على أهميتها.

٦ - التعامل مع الوسائط

٦-١ يجب على عمادة تقنية المعلومات تحديد الإجراءات الخاصة "بإدارة الوسائط القابلة للإزالة والتخلص منها", وفقًا للسياسات والإجراءات التنظيمية الخاصة بجامعة حائل والمتطلبات التشريعية والتنظيمية ذات العلاقة، ويجب على كافة الجهات والعاملين الالتزام بهذه الإجراءات.

٦-٢ يجب التخلص من وسائط التخزين التي تحتوي على معلومات بشكل آمن عندما لا تكون هناك حاجة إليها، وذلك باستخدام الإجراءات الرسمية المحددة.

٦-٣ يجب حماية الوسائط التي تحتوي على معلومات ضد الوصول غير المصرح به أو سوء الاستخدام أو الفساد أثناء نقلها.

٧ - متطلبات أخرى

٧-١ عند اتخاذ القرار بخصوص مستوى حماية المعلومات، يتوجب على الجامعة اخذ المتطلبات القانونية والتنظيمية والتشريعية ذات الصلة بعين الاعتبار.

٢-٧ يراعى في ضوابط حماية المعلومات التصنيف واحتياجات العمل إلى تبادل أو تقييد المعلومات، والآثار المترتبة على العمل نتيجة لهذه الاحتياجات.

٣-٧ يجب ان يتم عنونة كافة الأصول المعلوماتية وفقا للحساسية وسياسة إدارة الأصول الخاصة بالجامعة. وينبغي أن تعمل عمادة تقنية المعلومات على تبني مخططًا ملائما للعنونة.

٤-٧ يجب أن تتضمن العنونة المادية للوثائق، والأجهزة والوسائط غير الثابتة، تصنيفا أمنيا مناسبا يلبي متطلبات سياسة إدارة الأصول الخاصة بالجامعة.

٥-٧ ينبغي على الجهات ذات العلاقة وضع إجراءات لتداول وتخزين المعلومات، وذلك لحماية المعلومات من الإفشاء غير المصرح به أو إساءة الاستخدام.

٦-٧ على كافة المستخدمين إتباع الإجراءات الرسمية والصادرة من الجهات التشريعية في الجامعة قبل الكشف عن أية معلومات تخص الجامعة للعموم. وينبغي العمل على حماية سلامة ودقة هذه المعلومات بعد الكشف عنها.

٧-٧ يجب مراجعة متطلبات الأمن السيبراني الخاصة بإدارة الأصول موائمتها مع متطلبات إدارة البيانات دوريًا.

٨-٧ يجب مراجعة هذه السياسة مرة واحدة في السنة على الأقل.

الأدوار والمسؤوليات

٩- **راعي ومالك وثيقة السياسة:** إدارة الأمن السيبراني
١٠-**مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني
١١-**تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات وإدارة الأمن السيبراني.

الالتزام بالسياسة

١- يجب على مكتب إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة بشكل دوري.
٢- يجب على جميع العاملين في جامعة حائل الالتزام بهذه السياسة.
٣- قد يُعرّض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي؛ حسب الإجراءات المُتبعة في جامعة حائل.

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 بـجامعة حائل 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-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بـجامعة حائل، وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

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

١-١ إدارة الصلاحيات

١-١-١ توثيق واعتماد إجراء لإدارة الوصول يوضح آلية منح صلاحيات الوصول للأصول المعلوماتية والتقنية وتعديلها وإلغائها في جامعة حائل، ومراقبة هذه الآلية والتأكد من تطبيقها.

١-١-٢ إنشاء هويات المستخدمين (User Identities) وفقاً للمتطلبات التشريعية والتنظيمية الخاصة بـجامعة حائل.

١-١-٣ التحقق من هوية المستخدم (Authentication) والتحقق من صحتها قبل منح المستخدم صلاحية الوصول إلى الأصول المعلوماتية والتقنية.

١-١-٤ توثيق واعتماد مصفوفة (Matrix) لإدارة تصاريح وصلاحيات المستخدمين (Authorization) بناءً على مبادئ التحكم بالدخول والصلاحيات التالية:

١-١-٤-١ مبدأ الحاجة إلى المعرفة والاستخدام (Need-to-Know and Need-to-Use).

١-١-٤-٢ مبدأ فصل المهام (Segregation of Duties).

١-١-٤-٣ مبدأ الحد الأدنى من الصلاحيات والامتيازات (Least Privilege).

١-١-٥ تطبيق ضوابط التحقّق والصلاحيات على جميع الأصول التقنية والمعلوماتية في جامعة حائل من خلال نظام مركزي آلي للتحكّم في الوصول، مثل بروتوكول النفاذ إلى الدليل البسيط (Lightweight Directory Access Protocol "LDAP").

١-١-٦ منع استخدام الحسابات المشتركة (Generic User) للوصول إلى الأصول المعلوماتية والتقنية الخاصة بـجامعة حائل.

١-١-٧ ضبط إعدادات الأنظمة ليتم إغلاقها تلقائياً بعد فترة زمنية محدّدة (Session Timeout)، (يوصى ألا تتجاوز الفترة ١٥ دقيقة).

١-١-٨ تعطيل حسابات المستخدمين غير المستخدمة خلال فترة زمنية محدّدة (يوصى ألا تتجاوز الفترة ٩٠ يوماً).

١-١-٩ ضبط إعدادات جميع أنظمة إدارة الهويات والوصول لإرسال السجلات إلى نظام تسجيل ومراقبة مركزي وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني.

١-١-١٠ 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]

١-١-١١ 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)

١-٢ منح حق الدخول

١-٢-١ متطلبات حق الدخول لحسابات المستخدمين

١-٢-١-١ 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).

١-٢-١-٢ منح المستخدم حق الوصول إلى الأصول المعلوماتية والتقنية الخاصة بـجامعة حائل بما يتوافق مع الأدوار والمسؤوليات الخاصة به.

١-٢-١-٣ 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.

١-٢-١-٤ تعطيل إمكانية تسجيل دخول المستخدم من أجهزة حاسبات متعدّدة في نفس الوقت (Concurrent Logins).

١-٢-٢ 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:

١-٢-٢-١ 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.

١-٢-٢-٢ يجب تفعيل سجل كلمة المرور (Password History) لتتبع عدد كلمات المرور التي تم تغييرها.

١-٢-٢-٣ 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).

١-٢-٢-٤ منع استخدام الحسابات ذات الصلاحيات الهامة والحسّاسة في العمليات التشغيلية اليومية.

١-٢-٢-٥ التحقّق من حسابات المستخدمين ذات الصلاحيات الهامة والحسّاسة على الأصول التقنية والمعلوماتية من خلال آلية التحقّق من الهوية متعدد العناصر (Multi-Factor Authentication "MFA") 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 بصمة الإصبع").

١-٢-٢-٦ يجب أن يتطلب الوصول إلى الأنظمة الحساسة والأنظمة المستخدمة لإدارة الأنظمة الحساسة ومتابعتها استخدام التحقق من الهوية متعدد العناصر (MFA) لجميع المستخدمين.

١-٢-٣ الدخول عن بُعد إلى شبكات جامعة حائل

١-٢-٣-١ منح صلاحية الدخول عن بعد للأصول المعلوماتية والتقنية بعد الحصول على إذن مسبق من إدارة الأمن السيبراني وتقييد الدخول باستخدام التحقق من الهوية متعدد العناصر (MFA).

١-٢-٣-٢ حفظ سجلات الأحداث المتعلقة بجميع جلسات الدخول عن بُعد الخاصة ومراقبتها حسب حساسية الأصول المعلوماتية والتقنية.

١-٣ إلغاء وتغيير حق الوصول

١-٣-١ يجب على الإدارة العامة للموارد البشرية تبليغ عمادة تقنية المعلومات والتعليم الالكتروني لاتخاذ الإجراء اللازم عند انتقال المستخدم أو تغيير مهامه أو إنهاء/انتهاء العلاقة الوظيفية بين المستخدم وجامعة حائل. وتقوم عمادة تقنية المعلومات والتعليم الالكتروني بإيقاف أو تعديل صلاحيات الدخول الخاصة بالمستخدم بناءً على مهامه الوظيفية الجديدة.

١-٣-٢ في حال تم إيقاف صلاحيات المستخدم، يمنع حذف سجلات الأحداث الخاصة بالمستخدم ويتم حفظها وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني.

٢- مراجعة هويات الدخول والصلاحيات

٢-١ 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.

٢-٢ 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.

٢-٣ يجب تسجيل وتوثيق جميع محاولات الوصول الفاشلة والناجحة ومراجعتها دورياً.

٣- إدارة كلمات المرور

٣-١ تطبيق سياسة آمنة لكلمة المرور ذات معايير عالية لجميع الحسابات داخل جامعة حائل، ويتضمّن الجدول أدناه أمثلة على ضوابط كلمات المرور لكل مستخدم:

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	٨ أحرف أو أرقام أو رموز	١٢ حرفاً أو رقماً أو رمزاً	٨ أحرف أو أرقام أو رموز
سجل كلمة المرور	تذكّر ٥ كلمات مرور	تذكّر ٥ كلمات مرور	تذكّر ٥ كلمات مرور
الحد الأعلى لعمر كلمة المرور	٤٥ يوماً	٤٥ يوماً	٤٥ 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	٣٠ دقيقة أو حتى يقوم النظام بفك الإغلاق	٣٠ دقيقة أو حتى يقوم النظام بفك الإغلاق	٣٠ دقيقة أو حتى يقوم النظام بفك الإغلاق
حد إغلاق الحساب	٥ محاولات غير صحيحة لتسجيل الدخول	٥ محاولات غير صحيحة لتسجيل الدخول	لا توجد محاولات
إعادة ضبط عداد إغلاق الحساب بعد مرور فترة معينة	٣٠ دقيقة (يقوم المدير بفك إغلاق الحساب المغلق يدوياً)	٣٠ دقيقة (يقوم المدير بفك إغلاق الحساب المغلق يدوياً)	لا يوجد
استخدام التحقق متعدد العناصر	مُفعل على الدخول عن بعد فقط	مُفعل	غير مُفعل

٢-٣ معايير كلمات المرور

١-٢-٣ يجب أن تتضمّن كلمة المرور (٨) أحرف على الأقل.

٢-٢-٣ يجب أن تكون كلمة المرور معقّدة (Complex Password) وتتضمّن ثلاثة رموز من الرموز التالية على الأقل:

١-٢-٢-٣ أحرف كبيرة (Upper Case Letters).

٢-٢-٢-٣ أحرف صغيرة (Lower Case Letters).

٣-٢-٢-٣ أرقام (١٢٣٥).

٤-٢-٢-٣ رموز خاصّة (@#%*#).

٣-٢-٣ يجب إشعار المستخدمين قبل انتهاء صلاحية كلمة المرور لتذكيرهم بتغيير كلمة المرور قبل انتهاء الصلاحية.

٤-٢-٣ يجب ضبط إعدادات كافة الأصول المعلوماتية والتقنية لطلب تغيير كلمة المرور المؤقتة عند تسجيل المستخدم الدخول لأول مرة.

٥-٢-٣ يجب تغيير جميع كلمات المرور الافتراضية لجميع الأصول المعلوماتية والتقنية قبل تثبيتها في بيئة الإنتاج.

٦-٢-٣ 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.

٣-٣ حماية كلمات المرور

١-٣-٣ يجب تشفير جميع كلمات المرور للأصول المعلوماتية والتقنية الخاصة بـجامعة حائل بصيغة غير قابلة للقراءة أثناء إدخالها ونقلها وتخزينها وذلك وفقاً لسياسة التشفير.

٣-٣-٢ يجب إخفاء (Mask) كلمة المرور عند إدخالها على الشاشة.
٣-٣-٣ يجب تعطيل خاصية "تذكّر كلمة المرور" (Remember Password) على الأنظمة والتطبيقات الخاصة بـجامعة حائل.
٣-٣-٤ منع استخدام الكلمات المعروفة (Dictionary) في كلمة المرور كما هي.
٣-٣-٥ يجب تسليم كلمة المرور الخاصة بالمستخدم بطريقة آمنة وموثوقة.
٣-٣-٦ 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.
٣-٣-٧ 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).

٤- متطلبات أخرى

٤-١ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لإدارة هويات الدخول والصلاحيات.

٤-٢ يجب مراجعة تطبيق متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات دورياً.

٤-٣ يجب مراجعة هذه السياسة سنوياً على الأقل، أو في حال حدوث تغييرات في المتطلبات التشريعية أو التنظيمية أو المعايير ذات العلاقة.

الأدوار والمسؤوليات

١- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.
٢- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.
٣- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الالكتروني والإدارة العامة للموارد البشرية وإدارة الأمن السيبراني.

الالتزام بالسياسة

١- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة دورياً.
٢- يجب على كافة العاملين في جامعة حائل الالتزام بهذه السياسة.
٣- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

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 بـجامعة حائل 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-1:2018) 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 بـجامعة حائل، وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

١- يجب إدارة حزم التحديثات والإصلاحات (Patch Management) بشكل يضمن حماية الأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة وأجهزة معالجة المعلومات.
٢- يجب تنزيل حزم التحديثات والإصلاحات من مصادر مرخصة وموثوقة وفقاً للإجراءات المتبعة داخل جامعة حائل.
٣- يجب استخدام أنظمة تقنية موثوقة وآمنة لإجراء مسح دوري للكشف عن الثغرات وحزم التحديثات ومتابعة تطبيقها.
٤- يجب على عمادة تقنية المعلومات والتعليم الالكتروني 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.
٥- يجب وضع خطة للاسترجاع (Rollback Plan) وتطبيقها في حال تأثير حزم التحديثات والإصلاحات سلباً على أداء الأنظمة أو التطبيقات أو الخدمات.
٦- يجب على اللجنة الإشرافية للأمن السيبراني التأكد من تطبيق حزم التحديثات والإصلاحات دورياً.
٧- يجب منح الأولوية لحزم التحديثات والإصلاحات التي تعالج الثغرات الأمنية حسب مستوى المخاطر المرتبطة بها.
٨- يجب جدولة التحديثات والإصلاحات بما يتماشى مع مراحل الإصدارات البرمجية التي يطرحها المورد.
٩- 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)
١٠- 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

١١- يجب أن تتبع عملية إدارة التحديثات والإصلاحات متطلّبات عملية إدارة التغيير.
١٢- في حال وجود ثغرات أمنية ذات مخاطر عالية، يجب تنصيب حزم التحديثات والإصلاحات الطارئة وفقاً لعملية إدارة التغيير الطارئة (Emergency Change Management).
١٣- يجب تنزيل التحديثات والإصلاحات على خادم مركزي (Centralized Patch Management Server) 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.
١٤- بعد تنصيب حزم التحديثات والإصلاحات، يجب استخدام أدوات مستقلة وموثوقة للتأكد من أن الثغرات تمت معالجتها بشكل فعال.
١٥- يجب استخدام مؤشر قياس الأداء (Key Performance Indicator "KPI") لضمان التطوير المستمر لإدارة حزم التحديثات والإصلاحات.
١٦- يجب مراجعة سياسة إدارة حزم التحديثات والإصلاحات وإجراءاتها سنوياً، وتوثيق التغييرات واعتمادها.

الأدوار والمسؤوليات

١- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.
٢- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.
٣- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الالكتروني.

الالتزام بالسياسة

١- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة بشكل مستمر.
٢- يجب على إدارة الأمن السيبراني وعمادة تقنية المعلومات والتعليم الالكتروني في جامعة حائل الالتزام بهذه السياسة.
٣- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة، إلى إجراء تأديبي؛ حسب الإجراءات المتبعة في جامعة حائل.

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 بـجامعة حائل 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-1:2018) الصادرة عن الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية والتطبيقات الخاصة بـجامعة حائل، وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

١- يجب تحديد جميع الأصول المعلوماتية والتقنية المستخدمة داخل جامعة حائل وكذلك التطبيقات والبرمجيات المعتمدة والتأكد من توفير معايير تقنية أمنية (Technical Security Standards) لها.
٢- يجب تطوير وتوثيق واعتماد المعايير التقنية الأمنية الخاصة بجميع الأصول المعلوماتية والتقنية والتطبيقات والبرمجيات المصرح بها داخل جامعة حائل.
٣- يجب تحصين وضبط إعدادات أجهزة الحاسب الآلي، والأنظمة، والتطبيقات، وأجهزة الشبكات، والأجهزة الأمنية الخاصة بـجامعة حائل بما يتوافق مع المعايير التقنية الأمنية المعتمدة لمقاومة الهجمات السيبرانية.
٤- يجب استخدام إحدى الطرق التالية لتطوير المعايير الأمنية التقنية:
٤-١ دليل الإعدادات والتحصين (Security Configuration Guidance) الخاص بالمُورد وذلك وفقاً للسياسات والإجراءات التنظيمية الخاصة بـجامعة حائل، والمتطلبات التشريعية والتنظيمية ذات العلاقة وأفضل الممارسات الدولية.
٤-٢ 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.
٤-٣ تطوير معايير أمنية تقنية خاصة بـجامعة حائل بما يتناسب مع طبيعة الأعمال وبما يتوافق مع دليل الإعدادات والتحصين الخاص بالمورد والمعايير المصنعية.
٥- يجب أن تغطي الضوابط الخاصة بالمعايير التقنية الأمنية بحد أدنى ما يلي:
٥-١ إيقاف أو تغيير الحسابات المصنعية والافتراضية.
٥-٢ منع تثبيت البرمجيات غير المرغوب بها.
٥-٣ تعطيل منافذ الشبكة غير المستخدمة.

٥-٤ تعطيل الخدمات غير المستخدمة.
٥-٥ تقييد استخدام وسائط الحفظ والتخزين الخارجي.
٥-٦ تغيير الإعدادات الافتراضية التي قد تُستغل في الهجمات السيبرانية.
٦- يجب مراجعة الإعدادات والتحصين والتأكد من تطبيقها في الحالات التالية:
٦-١ مراجعة الإعدادات والتحصين للأصول المعلوماتية والتقنية والتطبيقات دورياً والتأكد من تطبيقها وفقاً للمعايير التقنية الأمنية المعتمدة.
٦-٢ مراجعة الإعدادات والتحصين قبل إطلاق وتدشين المشاريع والتغييرات المتعلقة بالأصول المعلوماتية والتقنية.
٦-٣ مراجعة الإعدادات والتحصين قبل إطلاق وتدشين التطبيقات.
٦-٤ مراجعة الإعدادات والتحصين لأنظمة التحكم الصناعي دورياً والتأكد من تطبيقها وفقاً للمعايير التقنية الأمنية المعتمدة.
٧- يجب اعتماد صورة (Image) لإعدادات وتحصين الأصول المعلوماتية والتقنية الخاصة بـجامعة حائل وفقاً للمعايير التقنية الأمنية، وحفظها في مكان آمن.
٨- يجب استخدام صورة (Image) معتمدة في تثبيت أو تحديث الأصول المعلوماتية والتقنية.
٩- 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.
١٠- 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.
١١- يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لإدارة الإعدادات والتحصين.
١٢- يجب مراجعة متطلبات الأمن السيبراني المتعلقة بالإعدادات والتحصين للأصول المعلوماتية والتقنية والتطبيقات الخاصة بـجامعة حائل سنوياً، أو في حالة حدوث تغييرات في المتطلبات التشريعية أو التنظيمية أو المعايير ذات العلاقة.

الأدوار والمسؤوليات

١- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.
٢- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.
٣- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الالكتروني.

الالتزام بالسياسة

١- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة دورياً.
٢- يجب على كافة العاملين في جامعة حائل الالتزام بهذه السياسة.
٣- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

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 بـجامعة حائل 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 ١-٨-٢ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية الإلكترونية الخاصة بـجامعة حائل، وتنطبق على جميع العاملين في جامعة حائل، بما في ذلك الجهات التي تتعامل معها والأطراف الخارجية.

بنود السياسة

٤- البنود العامة

١-٤ يجب على جامعة حائل تطوير وتوثيق واعتماد إجراءات ومعايير خاصة بالتشفير بناءً على حاجة العمل وعلى تحليل المخاطر في جامعة حائل 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 وتنظيمياً)، وطرق استخدامها وآلية إصدار المفاتيح ونشرها واستعادتها، بالإضافة إلى إدارة النسخ الاحتياطية للمفاتيح وإجراءات إتلاف مفاتيح التشفير. (ECC-2-8-3-1)

٢-٤ يجب تشفير البيانات أثناء النقل والتخزين بناءً على تصنيفها وحسب السياسات والإجراءات التنظيمية لـجامعة حائل، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٣-٤ يجب استخدام طرق وخوارزميات ومفاتيح وأجهزة تشفير محدثة وفقاً لما تصدره الهيئة بهذا الشأن. (CSCC-2-7-1-3)

٤-٤ يجب تشفير جميع بيانات الأنظمة الحساسة، أثناء النقل (Data-In-Transit). (CSCC-2-7-1-1)

٥-٤ 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)

٦-٤ يجب تحديد وتوثيق الأدوار والمسؤوليات المتعلقة بإدارة البنية التحتية لمفاتيح التشفير (Key Management Infrastructure "KMI")، للأدوار التالية على الأقل:

٤-٦-١ مسؤول مفاتيح وأنظمة التشفير (Keying Material Manager) باعتباره مدير إدارة الأمن السيبراني.
٤-٦-٢ مشرفو التشفير المسؤولون عن حماية مفاتيح التشفير (Key Custodians).
٤-٦-٣ الجهات المعنية بإصدار الشهادات (Certification Authorities "CAs")، بحيث تكون موثوقة وآمنة.
٤-٦-٤ الجهات المعنية بتسجيل الشهادات (Registration Authorities "RAs")، بحيث تكون موثوقة وآمنة.

٥- الاستخدام الآمن للتشفير

٥-١ يجب تحديد وتوثيق كافة حلول التشفير المستخدمة (بما في ذلك الخوارزميات والبرامج والوحدات (Modules) والمكتبات (Libraries) ومكونات التشفير الأخرى) وتقييمها واعتمادها من قبل إدارة الأمن السيبراني قبل تطبيقها في جامعة حائل.

٥-٢ يجب التأكد من تطبيق التشفير وفقاً لحلول التشفير المعتمدة لدى جامعة حائل.

٥-٣ يُمنع استخدام خوارزميات التشفير المطورة داخلياً وفقاً لدليل التشفير الخاص بمشروع أمان تطبيق الويب المفتوح (OWASP).

٥-٤ يجب استخدام طرق التحقق الآمن (مثل استخدام مفاتيح التشفير العامة والتواقيع الرقمية والشهادات الرقمية) للحد من المخاطر السيبرانية ووفقاً لحلول التشفير المعتمدة في جامعة حائل.

٥-٥ 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 حائل.

٥-٦ 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 حائل.

٦- إدارة مفاتيح التشفير

٦-١ يجب إدارة مفاتيح التشفير بطريقة آمنة خلال عمليات دورة حياتها (Key Lifecycle Management) والتأكد من استخدامها بشكل سليم وفعّال. (ECC-2-8-3-2)

٦-٢ يجب أن يتم إصدار شهادات التشفير عن طريق جهة إصدار الشهادات الداخلية في جامعة حائل للخدمات المحلية أو عن طريق جهة خارجية موثوقة.

٦-٣ 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.

٦-٤ يجب توفير التقنيات اللازمة لحماية مفاتيح التشفير عند تخزينها (Tamper Resistant Safe).

٦-٥ يجب حماية المفاتيح الخاصة (Private Key) من خلال تأمينها بكلمة مرور و/أو من خلال تخزينها على وسيط آمن، ووفقاً لإجراءات التشفير المعتمدة.

٦-٦ يجب تصنيف مفاتيح التشفير الخاصة باعتبارها معلومات "سرية للغاية" وفقاً لسياسة تصنيف البيانات المعتمدة في جامعة حائل.

٦-٧ يجب تفعيل سجلات الأحداث لحلول إدارة مفاتيح التشفير ومراقبتها دورياً.

٦-٨ يجب تحديد مدة لاستخدام مفاتيح التشفير وتاريخ الإنشاء وتاريخ الانتهاء لكل مفتاح.

٦-٩ يجب تجديد مفاتيح التشفير قبل انتهاء صلاحيتها.

٦-١٠ 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.

٦-١١ في حال تعرض مفتاح التشفير الخاص (Private Key) المُستخدم من قبل جامعة حائل 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).

٦-١٢ يجب إلزام الجهة المعنية بإصدار الشهادات، في حال تعرضت مفاتيح التشفير الخاصة بها (Private Keys) إلى انتهاك أمني، بإبلاغ جامعة حائل وإلغاء جميع الشهادات فوراً واستبدال المفتاح الخاص بالجهة المعنية بإصدار الشهادات.

٦-١٣ 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).

٦-١٤ 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.

٦-١٥ مشرفو التشفير هم المسؤولون عن حماية مفاتيح التشفير (Key Custodians) وهم المصرح لهم فقط باستبدال مفاتيح التشفير عند الحاجة.

٦-١٦ 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.

٧- متطلبات أخرى

٧-١ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر للاستخدام السليم والفعال للتشفير.

٧-٢ يجب مراجعة كافة متطلبات الأمن السيبراني الخاصة بالتشفير دورياً. (ECC-2-8-4)

٧-٣ تتم مراجعة هذه السياسة مرة واحدة في السنة؛ على الأقل.

الأدوار والمسؤوليات

١- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.
٢- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.
٣- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الالكتروني وإدارة الأمن السيبراني.

الالتزام بالسياسة

١- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة دورياً.

٢- يجب على كافة العاملين في جامعة حائل الالتزام بهذه السياسة.
٣- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

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 بـجامعة حائل 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-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أجهزة المستخدمين والخوادم الخاصة بـجامعة حائل، وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

١- البنود العامة

a. يجب على جامعة حائل تحديد تقنيات وآليات الحماية الحديثة والمتقدمة وتوفيرها والتأكد من موثوقيتها.

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

c. 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).

d. قبل اختيار تقنيات وآليات الحماية، يجب التأكد من ملاءمتها لأنظمة التشغيل الخاصة بـجامعة حائل مثل أنظمة ويندوز (Windows)، وأنظمة يونكس (UNIX)، وأنظمة لينكس (Linux)، ونظام ماك (Mac)، وغيرها.

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

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

٢-إعدادات تقنيات وآليات الحماية من البرمجيات الضارة

a. يجب ضبط إعدادات تقنيات الحماية وآلياتها وفقاً للمعايير التقنية الأمنية المعتمدة لدى جامعة حائل، مع الأخذ بالاعتبار إرشادات المورد وتوصياته.

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

c. لا يُسمح للأشخاص التابعين لأطراف خارجية بالاتصال بالشبكة أو الشبكة اللاسلكية لـجامعة حائل دون تحديث برنامج مكافحة الفيروسات وضبط الإعدادات المناسبة.

d. 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.

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

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

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

h. يجب القيام بعمليات مسح دورية لأجهزة المستخدمين والخوادم والتأكد من سلامتها من البرمجيات الضارة.

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

j. 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.

k. 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)

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

m. بجب 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 المشرف على إدارة الأمن السيبراني.

n. يجب إدارة تقنيات الحماية من البرمجيات الضارة مركزياً ومراقبتها باستمرار.

٣- متطلبات أخرى

a. يجب على إدارة الأمن السيبراني التأكد من توافر الوعي الأمني اللازم لدى جميع العاملين للتعامل مع البرمجيات الضارة والتقليل من مخاطرها.

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

c. يجب مراجعة متطلبات الأمن السيبراني لحماية أجهزة المستخدمين والخوادم الخاصة بـجامعة حائل دورياً.

الأدوار والمسؤوليات

١- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.
٢- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.
٣- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الالكتروني وإدارة الأمن السيبراني.

الالتزام بالسياسة

١- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة دورياً.
٢- يجب على كافة العاملين في جامعة حائل الالتزام بهذه السياسة.
٣- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

سياسة أمن البريد الإلكتروني

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية البريد الإلكتروني لـجامعة حائل 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 ٢-٤-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أنظمة البريد الإلكتروني الخاصة بـجامعة حائل وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

a. يجب توفير تقنيات حديثة لحماية البريد الإلكتروني وتحليل وتصفية (Filtering) رسائل البريد الإلكتروني وحظر الرسائل المشبوهة، مثل الرسائل الإقتحامية (Spam Emails) ورسائل التصيّد الإلكتروني (Phishing Emails).
b. يجب أن تستخدم أنظمة البريد الإلكتروني أرقام تعريف المستخدم وكلمات المرور مرتبطة، لضمان عزل اتصالات المستخدمين المختلفين.
c. يجب توفير التقنيات اللازمة لتشفير البريد الإلكتروني الذي يحتوي على معلومات مصنفة.
d. يجب تطبيق خاصية التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) للدخول عن بعد والدخول عن طريق صفحة موقع البريد الإلكتروني (Webmail).
e. يجب أرشفة رسائل البريد الإلكتروني والقيام بالنسخ الاحتياطي دورياً.
f. يجب تحديد مسؤولية البريد الإلكتروني للحسابات العامة والمشتركة (Generic Account)
g. 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.
h. يجب توثيق مجال البريد الإلكتروني لـجامعة حائل 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).
i. يجب أن يقتصر الوصول إلى رسائل البريد الإلكتروني على العاملين لدى جامعة حائل.
j. يجب اتخاذ الإجراءات اللازمة؛ لمنع استخدام البريد الإلكتروني لـجامعة حائل في غير أغراض العمل.

k. يمنع وصول مسؤول النظام (System Administrator) إلى معلومات البريد الإلكتروني الخاصة بأي موظف دون الحصول على تصريح مسبق.
l. 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.
m. يجب تذييل رسائل البريد الإلكتروني المرسلة إلى خارج جامعة حائل بإشعار إخلاء المسؤولية.
n. يجب تطبيق التقنيات اللازمة؛ لحماية سرية رسائل البريد الإلكتروني وسلامتها، وتوافرها أثناء نقلها وحفظها؛ وتشمل هذه الإجراءات استخدام تقنيات التشفير وتقنيات منع تسريب البيانات.
o. يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لنظام البريد الإلكتروني.
p. يجب تعطيل خدمة تحويل البريد الإلكتروني من الخادم (Open Mail Relay).

الأدوار والمسؤوليات

١- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.
٢- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.
٣- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الالكتروني وإدارة الأمن السيبراني.

الالتزام بالسياسة

١- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة بشكل دوري.
٢- يجب على جميع العاملين في جامعة حائل الالتزام بهذه السياسة.
٣- قد يُعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي؛ حسب الإجراءات المتبعة في جامعة حائل.

سياسة أمن الخوادم

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بالخوادم (Servers) الخاصة بـجامعة حائل 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-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الخوادم الخاصة بـجامعة حائل، وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

١- البنود العامة

a. يجب تحديد جميع الخوادم الخاصة بـجامعة حائل وتوثيقها، والتأكد من أن برمجيات الخوادم محدثة ومعتمدة.

b. يجب تطوير وتطبيق معايير تقنية أمنية (Technical Security Standards) للخوادم المستخدمة داخل جامعة حائل باستخدام أفضل المعايير الدولية.

c. يجب ضبط إعدادات الخوادم وفقاً للمعايير التقنية الأمنية المعتمدة قبل تشغيل الخوادم في بيئة الإنتاج.

d. يجب توفير الحماية اللازمة لجميع الخوادم للسيطرة على مخاطر الأمن السيبراني ذات العلاقة.

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

f. 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 حائل.

٢-إعدادات الخوادم

g. يجب اعتماد صورة (Image) لإعدادات وتحصين أنظمة تشغيل الخوادم الخاصة بـجامعة حائل وحفظها في مكان آمن وفقاً للمعايير التقنية الأمنية المعتمدة.

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

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

٣-الوصول والإدارة

j. يجب تقييد الوصول إلى الخوادم الخاصة بـجامعة حائل بحيث يكون الوصول متاحاً للمستخدمين المصرح لهم وعند الحاجة فقط.

k. يجب تقييد الدخول إلى الخوادم وحصره على حسابات مشرفي الأنظمة ومراجعة الحسابات والصلاحيات الممنوحة للمشرفين بشكل دوري.

l. 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).

m. يجب استخدام التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) للدخول إلى الخوادم الخاصة بالأنظمة الحساسة (CSCC-3-1-2-2).

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

o. 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).

٤- حماية الخوادم

a. يجب أن تُمنَع الخوادم غير المحدّثة أو غير الموثوقة من الاتصال بشبكة جامعة حائل 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.

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

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

d. يجب تقييد استخدام وسائط التخزين الخارجية على الخوادم، ويجب الحصول على إذن مسبق من إدارة الأمن السيبراني قبل استخدامها، والتأكد من استخدامها بشكل آمن.

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

٥- المتطلبات التشغيلية لإدارة الخوادم

a. يجب إدارة الخوادم مركزياً في جامعة حائل لكشف المخاطر بصورة أسرع، وتسهيل إدارة ومراقبة الخوادم مثل تقييد الوصول وتثبيت حزم التحديثات وغيرها.

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

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

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

e. 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.

f. يجب على عمادة تقنية المعلومات والتعليم الالكتروني مراقبة مكونات الخوادم التشغيلية والتأكد من فعالية أدائها، وتوافرها، وتوفير سعة تخزينية مناسبة، ونحو ذلك.

٦- إدارة الثغرات واختبار الاختراق

a. 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).

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

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

٧- الحماية المادية والبيئية للخوادم

a. يجب رصد ومراقبة الدخول والخروج من مرافق جامعة حائل، على سبيل المثال الأبواب والأقفال.

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

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

٨- متطلبات أخرى

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

b. 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

١- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.
٢- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.
٣- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الالكتروني وإدارة الأمن السيبراني.

الالتزام بالسياسة

١- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة دورياً.
٢- يجب على كافة العاملين في جامعة حائل الالتزام بهذه السياسة.
٣- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

سياسة أمن الشبكات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بأمن الشبكات الخاصة بـجامعة حائل 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-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الشبكات التقنية الخاصة بـجامعة حائل وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

٤- البنود العامة

a. تحديد وتوثيق جميع أجهزة الشبكة داخل جامعة حائل والتأكد من أن جميع الأجهزة محدثة ومعتمدة.

b. توثيق واعتماد معايير تقنية أمنية (Technical Security Standards) لجميع أجهزة الشبكة المستخدمة داخل جامعة حائل.

c. إدارة صلاحيات الدخول إلى الشبكات الخاصة بـجامعة حائل وفقاً لسياسة إدارة هويات الدخول والصلاحيات، بحيث يكون الاتصال بالشبكة متوفراً عند الحاجة ومتاحاً للمستخدمين المصرح لهم فقط.

٥- متطلبات الوصول إلى الشبكة

a. تطوير واعتماد إجراءات خاصة بمنح وإلغاء صلاحيات الدخول إلى الشبكة وذلك وفقاً لسياسة إدارة هويات الدخول والصلاحيات الخاصة بـجامعة حائل.

b. للحصول على صلاحية الدخول إلى الشبكة، يجب على المستخدم تقديم طلب إلى عمادة تقنية المعلومات والتعليم الالكتروني يوضح فيه نوع الطلب وفترة صلاحيته ومبرراته.

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

d. يجب استخدام اسم المستخدم وكلمة المرور للدخول إلى الشبكة الخاصة بـجامعة حائل وذلك وفقاً لسياسة إدارة هويات الدخول والصلاحيات.

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

f. توفير الحماية اللازمة عند تصفح الإنترنت والاتصال به، وتقييد الدخول إلى المواقع الإلكترونية المشبوهة، ومواقع مشاركة تخزين الملفات، ومواقع الدخول عن بعد.
g. عدم ربط الشبكة اللاسلكية بالشبكة الداخلية لـجامعة حائل، إلا بناءً على دراسة متكاملة للمخاطر المترتبة على ذلك، والتعامل معها بما يضمن حماية الأصول التقنية الخاصة وسرية البيانات وسلامتها، وحماية النظم والتطبيقات المتصلة بـجامعة حائل.
h. يُمنع ربط الأنظمة الحساسة بالشبكة اللاسلكية لـجامعة حائل.
i. يجب توفير التقنيات اللازمة لوضع القيود وإدارة منافذ وبروتوكولات وخدمات الشبكة.
j. 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).

٦- متطلبات وصول الأطراف الخارجية إلى الشبكة

a. يخضع منح صلاحية وصول الأطراف الخارجية إلى شبكة جامعة حائل لمتطلبات الأمن السيبراني المشار إليها في سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية.
b. استخدام تقنيات تشفير ومصادقة آمنة لنقل البيانات من الأطراف الخارجية وإليها.
c. تحديد مدة زمنية معينة للأطراف الخارجية للدخول إلى شبكة جامعة حائل.
d. مراجعة صلاحيات المستخدمين والأطراف الخارجية دورياً وذلك وفقًا لسياسات الأمن السيبراني المعتمدة في جامعة حائل.

٧- حماية الشبكات

a. يجب عزل وتقسيم الشبكات مادياً ومنطقياً باستخدام جدار الحماية (Firewall) ومبدأ الدفاع الأمني متعدد المراحل (Defense-in-Depth). (ECC-2-5-3-1)
b. تطبيق العزل المنطقي لشبكة الأنظمة الحساسة (VLAN).
c. تطبيق العزل المنطقي بين شبكة بيئة الإنتاج وشبكة بيئة الاختبار والشبكات الأخرى.
d. يمنع ربط الأنظمة الحساسة بالإنترنت في حال كانت هذه الأنظمة تقدم خدمة داخلية لـجامعة حائل ولا توجد هناك حاجة ضرورية جداً للدخول على الخدمة من خارج جامعة حائل. (CSCC-2-4-1-6)
e. تطبيق العزل المنطقي بين شبكة الاتصالات الهاتفية عبر الإنترنت (Voice Over IP "VOIP") وشبكة البيانات.
f. تقييد استخدام منافذ الشبكة المادية في جميع مرافق جامعة حائل 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.
g. 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.
h. يمنع اتصال الشبكة الداخلية بالإنترنت مباشرةً، ويكون الاتصال عن طريق استخدام موزع اتصالات الإنترنت (Proxy) لتحليل وتصفية البيانات المنتقلة من وإلى جامعة حائل.
i. 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.
j. يجب توفير التقنيات اللازمة لأمن نظام أسماء النطاقات (DNS).
k. يجب توفير أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات (Intrusion Prevention Systems) على جميع أجزاء الشبكة وتحديثها دورياً.
l. يجب توفير أنظمة الحماية من التهديدات المتقدمة المستمرة على مستوى الشبكة (Network APT) على شبكة الأنظمة الحساسة.

m. 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)

n. يجب توفير أنظمة الحماية من هجمات تعطيل الشبكات (Distributed Denial of Service Attack "DDoS") على الأنظمة الخارجية الحساسة. (CSCC-2-4-1-8)

٨- الأمن المادي والبيئي

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

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

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

٩- متطلبات أخرى

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

b. 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

١- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.

٢- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.

٣- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الالكتروني وإدارة الأمن السيبراني.

الالتزام بالسياسة

١- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة دورياً.

٢- يجب على كافة العاملين في جامعة حائل الالتزام بهذه السياسة.

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

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 بـجامعة حائل 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-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أنظمة قواعد البيانات الخاصة بـجامعة حائل، وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

١- البنود العامة

١-١يجب تحديد وتوثيق جميع أنظمة قواعد البيانات المستخدمة داخل جامعة حائل والعمل على توفير البيئة المناسبة لحمايتها من المخاطر البيئية والتشغيلية.

١-٢يجب تطوير واعتماد معايير التقنية الأمنية لأنظمة قواعد البيانات داخل جامعة حائل وتطبيقها من قبل مشرفي قواعد البيانات.

١-٣فيما 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)

١-٤يتم منح حق الوصول إلى قواعد البيانات وفقاً لسياسة إدارة هويات الدخول والصلاحيات.

١-٥يمنع نسخ أو نقل قواعد البيانات الخاصة بالأنظمة الحساسة من بيئة الإنتاج إلى أي بيئة اخرى. (CSCC-2-6-1-5)

٢- الإجراءات الأمنية المطلوبة لاستضافة قواعد البيانات

a. 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.

b. توفير العزل المنطقي بين قواعد البيانات الخاصة بـجامعة حائل وقواعد البيانات المستضافة الأخرى.

c. يجب أن يكون موقع الاستضافة الخاص بالخدمات السحابية موجوداً ضمن النطاق الجغرافي للمملكة العربية السعودية. (ECC-3-3-2-4)

d. 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 حائل.

٣- المتطلبات المتعلّقة بإدارة التغييرات على أنظمة قواعد البيانات

٣-١ يجب أن تتم التغييرات على قواعد البيانات (مثل ترحيل قواعد البيانات، والنقل إلى بيئة الإنتاج) وفقاً لعملية إدارة التغيير المعتمدة في جامعة حائل.

٣-٢ يتم تثبيت التحديثات والإصلاحات على نظام قواعد البيانات وفقاً لسياسة إدارة حزم التحديثات والإصلاحات المعتمدة في جامعة حائل.

٣-٣ التأكد من استخدام أنظمة قواعد بيانات موثوقة ومعتمدة ومرخصة.

٣-٤ التأكد من وجود خطة واضحة للتعافي من الكوارث خاصة بأنظمة قواعد البيانات.

٣-٥ يجب على جامعة حائل توقيع اتفاقية مستوى الخدمة للدعم مع المورّدين فيما يتعلّق بنظام إدارة قواعد البيانات في بيئة الإنتاج.

٣-٦ تطبيق التجزئة والتشفير على قواعد البيانات المخزنة وفقاً لسياسة التصنيف وسياسة التشفير المعتمدة في جامعة حائل.

٤- مراقبة سجلات الأحداث المتعلقة بنظام قواعد البيانات

٤-١ تفعيل وحفظ سجلات الأحداث الخاصة بنظام قواعد البيانات وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني المعتمدة في جامعة حائل.

٤-١ يجب على إدارة الأمن السيبراني مراقبة سجلات الأحداث المتعلقة بقواعد البيانات الخاصة بالأنظمة الحساسة، ومراقبة سلوك المستخدمين.

٤-٣ يجب على أدارة الامن السيبراني مراقبة سجلات الأحداث الخاصة بمشرفي قواعد البيانات ومراقبة سلوكهم ومراجعتها دورياً.

٥- المتطلبات التشغيلية

٥-٣ 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.

٥-٤ يجب على عمادة تقنية المعلومات والتعليم الإلكتروني مراقبة أنظمة قواعد البيانات التشغيلية والتأكد من جودة أدائها، وتوافرها، وتوفير سعة تخزينية مناسبة، ونحوه.

٥-٥ مزامنة التوقيت (Clock Synchronization) مركزياً ومن مصدر دقيق وموثوق لجميع أنظمة قواعد البيانات. (ECC-2-3-3-4)

٦- متطلبات أخرى

٦-١ استخدام مؤشر قياس الأداء (Key Performance Indicator "KPI") لضمان التطوير المستمر لنظام إدارة قواعد البيانات.

٦-٢ 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

١- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.
٢- **مراجعة السياسة وتحديثها:** مدير إدارة لأمن السيبراني.
٣- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الإلكتروني وإدارة الأمن السيبراني.

الالتزام بالسياسة

١- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة دورياً.
٢- يجب على كافة العاملين في جامعة حائل الالتزام بهذه السياسة.
٣- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

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 بـجامعة حائل، 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-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع تطبيقات الويب الخارجية الخاصة بـجامعة حائل، وتنطبق هذه السياسة على جميع العاملين في جامعة حائل.

بنود السياسة

١- المتطلبات العامة

e. يجب أن تتبع تطبيقات الويب الخارجية التي يتم شراؤها أو تطويرها داخلياً مبدأ المعمارية متعددة المستويات (Multi-tier Architecture). (ECC-2-15-3-2)

f. يجب استخدام مبدأ المعمارية متعددة المستويات لتطبيقات الويب الخارجية للأنظمة الحساسة على ألا يقل عدد المستويات عن ٣ مستويات (3-tier Architecture). (CSCC-2-12-2-2)

g. 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)

h. يجب استخدام نظام جدار الحماية لتطبيقات الويب (Web Application Firewall "WAF") لحماية تطبيقات الويب الخارجية من الهجمات الخارجية. (ECC-2-15-3-1)

i. يجب تطبيق العزل المنطقي لبيئة التطوير (Development Environment) وبيئة الاختبار (Testing Environment) عن بيئة الإنتاج (Production Environment).

j. يجب استخدام تقنيات حماية البيانات والمعلومات في تطبيقات الويب الخارجية ووفقاً لسياسة حماية البيانات والمعلومات وسياسة التصنيف.

k. في حال شراء تطبيقات ويب من طرف خارجي، يجب التأكد من التزام المورد بسياسات ومعايير الأمن السيبراني في جامعة حائل.

l. يجب تطبيق الحد الأدنى على الأقل لمعايير أمن التطبيقات وحمايتها (Ten OWASP Top) لتطبيقات الويب الخارجية للأنظمة الحساسة. (CSCC-2-12-1-2-2)

٢-متطلبات حق الوصول (Access Right)

m. يجب استخدام التحقّق من الهوية متعدّد العناصر (Multi-Factor Authentication) لعمليات دخول المستخدمين على تطبيقات الويب الخارجية. (ECC-2-15-3-5)
n. 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)
o. ينبغي أن يقتصر حق الوصول إلى منظومات الإنتاج، وأن يتم التحكم به وفقاً للمسؤوليات الوظيفية.
p. يجب نشر سياسة الاستخدام الآمن لجميع مستخدمي تطبيقات الويب الخارجية. (ECC-2-15-3-4)

٣-متطلبات تطوير أو شراء تطبيقات الويب

q. 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 حائل.
r. قبل استخدام المعلومات المحمية في بيئة الاختبار، يجب الحصول على إذن مسبق من إدارة الأمن السيبراني واستخدام ضوابط مشددة لحماية تلك البيانات، مثل: تقنيات مزج البيانات (Data Scrambling) وتقنيات تعتيم البيانات (Data Masking)، وحذفها مباشرة بعد الانتهاء من استخدامها.
s. يجب حفظ شفرة المصدر (Source Code) بشكل آمن وتقييد الوصول إليها للمصرح لهم فقط.
t. يجب إجراء اختبار الاختراق لتطبيق الويب الخارجي في بيئة الاختبار وتوثيق النتائج والتأكد من معالجة جميع الثغرات قبل إطلاق التطبيق على بيئة الإنتاج.
u. يجب إجراء فحص الثغرات للمكونات التقنية لتطبيقات الويب والتأكد من معالجتها بتثبيت حزم التحديثات والإصلاحات المعتمدة لدى جامعة حائل.
v. يجب اعتماد تطبيقات الويب من قبل اللجنة التقنية الاستشارية للتغيير (CAB) قبل إطلاقها في بيئة الإنتاج.

٤- متطلبات أخرى

a. يجب مراجعة متطلبات الأمن السيبراني الخاصة بحماية تطبيقات الويب الخارجية دورياً. (ECC-2-15-4)
b. يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لحماية تطبيقات الويب الخارجية.
c. تتم مراجعة هذه السياسة مرة واحدة في السنة؛ على الأقل.

الأدوار والمسؤوليات

١- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.
٢- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.
٣- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الإلكتروني وإدارة الأمن السيبراني.

الالتزام بالسياسة

١- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة بشكل مستمر.
٢- يجب على كافة العاملين في جامعة حائل الالتزام بهذه السياسة.

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

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 حائل 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 حائل على خدمات الحوسبة السحابية التي تتم استضافتها أو معالجتها أو إدارتها بواسطة أطراف خارجية، وتنطبق هذه السياسة على جميع العاملين في جامعه حائل

بنود السياسة

١- البنود العامة

a. تُطبَق جميع متطلبات الأمن السيبراني الخاصة بالأطراف الخارجية في سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية على جميع مقدمي خدمات الحوسبة السحابية والاستضافة.

b. يجب على إدارة الأمن السيبراني التحقق من كفاءة وموثوقية مقدم خدمات الحوسبة السحابية والاستضافة بالإضافة إلى حصوله على ترخيص ووجود سجل رسمي له داخل المملكة العربية السعودية.

c. يجب تطبيق متطلبات الأمن السيبراني الخاصة بخدمات الحوسبة السحابية والاستضافة وفقاً للسياسات والإجراءات التنظيمية الخاصة بجامعة حائل والمتطلبات التشريعية والتنظيمية ذات العلاقة.

d. يجب على جامعة حائل إجراء تقييم لمخاطر الأمن السيبراني المترتبة على استضافة التطبيقات أو الخدمات في الحوسبة السحابية قبل اختيار مقدم خدمات الحوسبة السحابية والاستضافة.

e. يجب أن يكون موقع استضافة الأنظمة الحساسة، أو أي جزء من مكوناتها التقنية، داخل جامعه حائل 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)

f. يجب على إدارة الأمن السيبراني تطوير وتوثيق واعتماد إجراءات خاصة باستخدام الخدمات السحابية.

g. يجب أن تتضمن عقود مقدمي خدمات الحوسبة السحابية والاستضافة بحد أدنى ما يلي:

i. متطلبات الأمن السيبراني وبنود اتفاقية مستوى الخدمة (Service Level Agreement "SLA").
ii. بنود المحافظة على سرية المعلومات (Non-disclosure Clauses) بما في ذلك حذف البيانات وإتلافها بالاتفاق بين مقدم الخدمة وجامعة حائل بناء على تصنيف تلك البيانات ومع مراعاة سياسة تصنيف البيانات.
iii. متطلبات استمرارية الأعمال والتعافي من الكوارث.
iv. يجب أن تتضمن عقود مقدمي خدمات الحوسبة السحابية والاستضافة إمكانية جامعة حائل إنهاء الخدمة دون مبرر أو اشتراطات .

h. يجب مراجعة تطبيق متطلبات الأمن السيبراني مع مقدمي خدمات الحوسبة السحابية والاستضافة دورياً، مرة واحدة في السنة، على الأقل.

٢- متطلبات الأمن السيبراني المتعلقة باستضافة/تخزين البيانات

a. يجب تصنيف البيانات قبل استضافتها/تخزينها لدى مقدمي خدمات الحوسبة السحابية والاستضافة. (ECC-4-2-3-1)

b. 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)

c. يجب أن يكون موقع واستضافة وتخزين معلومات جامعة حائل داخل المملكة العربية السعودية (ECC-4-2-3-3) مع مراعاة التنظيمات والجوانب التشريعية بعدم خضوع تلك البيانات لأي قوانين دول أخرى.

d. يجب على إدارة الأمن السيبراني التأكد من فصل البيئة الخاصة بجامعة حائل(ويشمل ذلك الخوادم الافتراضية، والشبكات وقواعد البيانات) عن غيرها من البيئات التابعة لجهات أخرى في خدمات الحوسبة السحابية. (ECC-4-2-3-2)

e. يجب الحصول على موافقة إدارة الأمن السيبراني لاستضافة الأنظمة الحساسة أو أي جزء من مكوناتها التقنية.

f. يجب على جامعة حائل التأكد من تطبيق متطلبات خصوصية البيانات على البيانات المستضافة في الحوسبة السحابية.

g. يجب تشفير البيانات والمعلومات المنقولة إلى الخدمات السحابية، أو المخزنة فيها، أو المنقولة منها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة في جامعه حائل

h. يجب على جامعة حائل التأكد من أن مقدم خدمات الحوسبة السحابية والاستضافة يقوم بعمل النسخ الاحتياطي دورياً وحماية النسخ الاحتياطية وفقاً لسياسة النسخ الاحتياطية المعتمدة في جامعه حائل

i. يجب على جامعة حائل 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.

j. يجب على مقدم خدمات الحوسبة السحابية والاستضافة تقييد الدخول إلى الخدمات السحابية الخاصة بجامعة حائل على المستخدمين المصرح لهم فقط وباستخدام وسائل التحقق من هوية المستخدم وفقاً لسياسة إدارة هويات الدخول والصلاحيات المعتمدة في جامعه حائل

k. يجب على مقدم خدمات الحوسبة السحابية والاستضافة توفير التقنيات والأدوات اللازمة لجامعة حائل لإدارة ومراقبة خدماتها السحابية.

l. يجب على إدارة الأمن السيبراني وإدارة الشؤون القانونية تضمين بنود متطلبات الأمن السيبراني المتعلقة باستضافة البيانات في العقد مع مقدم خدمة الحوسبة السحابية.

٣- متطلبات أخرى

a. يجب على جامعة حائل التأكد من تفعيل سجلات الأحداث على الأصول المعلوماتية المستضافة.

b. يجب على جامعة حائل مراقبة سجلات الأحداث الخاصة بالأمن السيبراني دورياً.

c. يجب على جامعة حائل التأكد من مزامنة التوقيت (Clock Synchronization) الخاص بالبنية التحتية للخدمة السحابية مع التوقيت الخاص بـجامعه حائل

d. يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لحماية الأصول المعلوماتية والتقنية على خدمات الحوسبة السحابية.

e. يجب مراجعة متطلبات الأمن السيبراني الخاصة بخدمات الحوسبة السحابية والاستضافة دورياً.

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

الأدوار والمسؤوليات

١- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الامن السيبراني
٢- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني
٣- **تنفيذ وتطبيق السياسة:** عمادة تقنية المعلومات والتعليم الإلكتروني و إدارة الأمن السيبراني

الالتزام بالسياسة

١- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة بشكل دوري.
٢- يجب على كافة العاملين في جامعة حائل الالتزام بهذه السياسة.
٣- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعه حائل

سياسة الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية

الأهداف

الغرض من هذه السياسة هو تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير ضمن إدارة المشاريع المعلوماتية والتقنية لضمان استمرارية أعمال جامعة حائل وحمايتها من المخاطر السيبرانية والتهديدات الداخلية والخارجية, ويتم ذلك من خلال التأكد من أن متطلبات الأمن السيبراني مضمنة في منهجية إدارة مشاريع جامعة حائل وإجراءاتها لحماية السرية, وسلامة الأصول المعلوماتية والتقنية لجامعة حائل وضمان دقتها وتوافرها, وكذلك التأكد من تطبيق معايير الأمن السيبراني في أنشطة تطوير التطبيقات والبرامج, وفقًا للسياسات والإجراءات التنظيمية لجامعة حائل والمتطلبات التشريعية والتنظيمية ذات العلاقة.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٦ 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 حائل وتنطبق على جميع المشاريع التقنية بالجامعة

بنود السياسة

١- يجب التأكد من أن متطلبات الأمن السيبراني مضمنة من منهجية وإجراءات إدارة مشاريع الجامعة لحماية السرية وسلامة الأصول المعلوماتية والتقنية للجهة ودقتها وتوافرها، وأن تكون متطلبات الأمن السيبراني جزء أساسي من متطلبات المشاريع التقنية، وذلك وفقًا للسياسات والإجراءات التنظيمية للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢- يجب على الجهات ذات العلاقة التأكد من تضمين متطلبات الأمن السيبراني في منهجية وإجراءات إدارة المشاريع.

٣- يجب على الجهات ذات العلاقة التأكد من تضمين متطلبات الأمن السيبراني في إدارة التغيير على الأصول المعلومات والتقنية في الجهة لضمان تحديد مخاطر الأمن السيبراني ومعالجتها كجزء من دورة حياة المشروع التقني.

٤- تشمل متطلبات الأمن السيبراني لإدارة المشاريع والتغييرات على الأصول المعلوماتية والتقنية للجهة ما يلي:

- إجراء فحص الثغرات (Assessment Vulnerabilities)، لاكتشاف وتقييم الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعال، وذلك وفق سياسة ومعيار إدارة الثغرات المعتمدة بالجامعة

- اجراء مراجعة للإعدادات والتحصين (Secure Configuration and Hardening) وحزم التحديثات قبل إطلاق وتدشين التطبيقات وفقًا للسياسات والمعايير المعتمدة بالجامعة.

٥- تشمل متطلبات الأمن السيبراني لمشاريع تطوير التطبيقات والبرمجيات الخاصة للجامعة ما يلي:

- استخدام معايير التطوير الآمن للتطبيقات (Secure Coding Standards) المعتمدة.
- استخدام مصادر مرخصة وموثوقة لأدوات تطوير التطبيقات والمكتبات الخاصة بها (Libraries).
- اجراء اختبار للتحقق من مدى استيفاء التطبيقات للمتطلبات الأمنية السيبرانية للجهة.
- أمن التكامل (Integration) بين التطبيقات.

٦- يجب تحديد الأدوار والمسؤوليات للأطراف ذات العلاقة بإدارة المشاريع التقنية في جامعة حائل.

٧- يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر للأمن السيبراني الخاصة بإدارة المشاريع المعلوماتية والتقنية.

٨- يجب مراجعة متطلبات الأمن السيبراني وتطبيقها مع العاملين المسؤولين عن إدارة المشاريع التقنية دوريًا، مرة واحدة في السنة على الأقل.

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

الأدوار والمسؤوليات

١- **راعي ومالك وثيقة السياسة:** إدارة الأمن السيبراني
٢- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.
٣- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات وإدارة الأمن السيبراني.

الالتزام بالسياسة

١- يجب على مدير الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة بشكل دوري.
٢- يجب على كافة العاملين في جامعة حائل الالتزام بهذه السياسة.
٣- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

سياسة حماية البيانات

الأهداف

الغرض من هذه السياسة هو حماية البيانات، البيانات المخزنة (الإلكترونية أو السجلات الورقية) التي تحتفظ بها جامعة حائل، وكذلك الأشخاص الذين يستخدمونها والطرق التي يتبعونها في التعامل بها والأجهزة المستخدمة للوصول إليها، لضمان حماية السرية وسلامة بيانات ومعلومات الجامعة ودقتها وتوافرها, وذلك وفقًا للسياسات والإجراءات التنظيمية للجامعة, والمتطلبات التشريعية والتنظيمية ذات العلاقة. كما تقوم هذه السياسة بتحديد المتطلبات والمسؤوليات الأساسية للإدارة السليمة لأصول البيانات وتحديد وسائل التعامل مع البيانات ونقلها داخل الجامعة.

كما تصف السياسة 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 بالجامعة. بالإضافة إلى تحديد متطلبات التعامل مع بيانات الجامعة من أجل توفير أساسيات لحمايتها.

نطاق العمل وقابلية التطبيق

تسري هذه السياسة على جميع من يقوم بالأعمال من النظم والأشخاص وطرق العمل، ويشمل ذلك جميع المدراء التنفيذيين واللجان والإدارات والشركاء والموظفين والأطراف الأخرى الذين لديهم إمكانية الوصول إلى نظم المعلومات أو البيانات التي يتم إنشاؤها أو جمعها أو تخزينها أو معالجتها في جامعة حائل، 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 الجامعة أو تخصها.

بنود السياسة

١- تصنيف المعلومات

١-٢ يجب وضع جميع البيانات في جامعة حائل في أحد التصنيفات التالية:

١-٢-١ سرية (مقيدة): تعرف البيانات السرية على أنها عالية الحساسية، ويسبب الكشف عنها أو فقدانها أو تدميرها أضرار كبيرة لشخص أو أكثر أو لجامعة حائل. ويمكن أن تشمل ما يلي:

- البيانات الشخصية للموظفين أو العملاء في جامعة حائل مثل هوية المستخدم (User ID) والضمان الاجتماعي أو أرقام الهوية أرقام 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.

١-٢-٢ حساسية (داخلية): وهي البيانات ذات المخاطر المنخفضة ونشرها أو فقدها أو تدميرها لن يكون له تأثير كبير على الأشخاص أو جامعة حائل، ولكن لا يجوز نشرها خارج جامعة حائل، وغالبًا تشتمل على ما يلي:

- البريد الإلكتروني، معظم الرسائل يمكن حذفها أو نشرها دون أن تتسبب في أضرار (باستثناء البريد الإلكتروني المستلم 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 يوميًا يمكن تصنيفها على انها حساسة. ومن أمثلة هذه البيانات محاضر الاجتماعات وخطط العمل والتقارير الداخلية للمشاريع.

١-٢-٣ عامة (غير مقيدة): وهي البيانات التي يمكن الكشف عنها للعامة وتشمل البيانات والملفات التي لا تعتبر حرجة بالنسبة لاحتياجات وعمليات العمل، يتم نشرها عمدًا لاستخدامها حيث يكون تأثيرها محايدًا أو ايجابيًا على جامعة حائل، مثل المواد التسويقية والإعلانات.

١-٢-٤ الالتزام: يجب أن يلتزم الشركاء أو من يعمل مع جامعة حائل من جهات خارجية بهذا التصنيف الأمني للبيانات.

٢- المسؤول عن البيانات

a. يجب أن تخضع جميع أصول البيانات الهامة لمسؤول ويجب أن يكون المسؤول أحد الموظفين الذي تتناسب خبرته مع قيمة الأصول التي سيتولى إدارتها وحمايتها.

b. 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.

c. 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.

d. يجب تعيين مسؤول موثوق وتحديد مسؤولياته بشكل واضح اتجاه أصول البيانات التي يتم استخدامها في جامعة على نطاق واسع وينبغي أن يملك هذا الشخص على القدرة التحكم في هذه بيانات.

٣- تخزين البيانات

a. يتم تخزين جميع البيانات الإلكترونية على المنظومات الخاصة بها حتى يسمح بإجراء نسخ احتياطية منتظمة .

b. يجب عدم السماح للموظفين للوصول إلى البيانات إلا بعد اعلامهم وموافقتهم على شروط الاطلاع على البيانات التي سيتعاملون معها

c. قواعد البيانات التي تحتوي على بيانات شخصية يكون لها إجراءات محددة لإداراتها وتأمين السجلات والوثائق.

d. يجب تخزين الملفات التي يتم تصنيفها كمخاطر أمنية محتملة في أكثر المناطق أمنًا على الشبكة.

٤- الكشف عن البيانات

a. في حالة مشاركة البيانات المقيدة مع جامعة حائل أخرى، يجب الحرص في الكشف عن هذه البيانات وأن يتم بطريقة آمنة.

b. عندما يتم الإفصاح عن البيانات أو مشاركتها، يجب أن يتم ذلك فقط وفقًا لبروتوكول مشاركة البيانات الموثق أو اتفاقية تبادل البيانات.

c. يحظر الإفصاح عن البيانات المقيدة لأي جهة خارجية.

٥- الاحتفاظ بالسجلات واتلافها

a. سجلات المحاسبة المالية، وتشمل على:

- الوثائق المتعلقة بكشوف المرتبات وإجراءات المحاسبة ودفاتر الحسابات الدائنة والجداول الزمنية، ودفاتر الحسابات والفواتير وتقارير نفقات الموظفين. ويجب الاحتفاظ بها خمس سنوات على الأقل.
- ينبغي الاحتفاظ بصفة دائمة بتقارير المراجعة السنوية والبيانات المالية، والاحتفاظ بالخطط السنوية والميزانيات للمدة اللازمة لتنفيذها والرجوع إليها عند الحاجة.

b. يجب الاحتفاظ بالعقود والمراسلات ذات الصلة بالعقود (بما في ذلك أي تعديلات على بنود العقد وجميع الوثائق الداعمة الاخرى).

c. سجلات جامعة حائل (محاضر الاجتماعات، التكاليف الموقعة من الإدارة، أختام جامعة حائل، التأسيس واللوائح، سجلات المساهمة والتقارير السنوية) والتراخيص والتصاريح ووثائق التأمين يجب أن تحتفظ بشكل دائم.

d. يجوز إتلاف المستندات المعتبرة في حكم المستندات ذات القيمة بعد اتخاذ الإجراءات اللازمة لتسجيل بياناتها أو ملخصها إذا مضى على استعمالها أو على إجراء آخر قيد فيها خمس سنوات إلا إذا كانت هذه المستندات محل فحص أو مراجعة أو كانت مطلوبة في دعوة قائمة أو كانت القوانين واللوائح أو تعليمات وزارة المالية تقرر الاحتفاظ بها لمدة أطول.

e. الوثائق الالكترونية

- المستندات الالكترونية: وتشمل مكتبة برامج مايكروسوفت (Microsoft Office Suite) , ملفات (PDF), والاحتفاظ يعتمد أيضًا على موضوع السجلات وتصنيف بياناتها.
- البريد الإلكتروني: يعتمد الاحتفاظ برسائل البريد الإلكتروني على محتواها فلا ينبغي الاحتفاظ بجميعها، والبريد الالكتروني الذي يتم حفظه يجب أن يكون مطبوعًا في نسخة ورقية أن يحتفظ به في الملف المناسب ويتم تنزيله الى ملف كمبيوتر ويتم الاحتفاظ به إلكترونيًا أو على القرص كملف منفصل.
- ملفات صفحة ويب: في جميع الاجهزة في محيط العمل، يجب أن يتم جدولة متصفحات الانترنت لحذف ملفات جمع البيانات مرة واحدة في الشهر.

f. الملفات والمستندات القانونية

يتم الاحتفاظ بالأرشيف القانوني الخاص بجامعة حائل بدون تحديد مدة على النحو التالي:

- ملفات الدعاوي القضائية وما يصدر فيها من أحكام ابتدائية ونهائية، وقرارات وأوامر المحاكم بما في ذلك جميع الملفات ذات الصلة.
- المذكرات والآراء القانونية الصادرة عن المكاتب القانونية.

g. السجلات الشخصية

- ملفات منسوبي الجامعة وما تتضمنه من مستندات تخص مهامهم الوظيفية, ويجب أن تحتفظ بشكل دائم حتى بعد إنهاء علاقة الموظف بالجامعة.
- سجلات الإدارية الوظيفية (وتشمل الحضور والانصراف، استمارة الطلبات، سجل تغيرات العمل، أوراق إنهاء الخدمة، نتائج الاختبارات، سجلات التدريب) يتم الاحتفاظ بها وفق الحاجة إليها وللمدة اللازمة وفق تقديرات جامعة حائل.
- سجلات وأوراق امتحانات شغل الوظائف: تحتفظ جامعة حائل بأوراق إجابة الامتحانات التحريرية والسجلات والقوائم وسائر الوثائق المتعلقة بالامتحانات التي تجريها لمدة سنتين تبدأ من تاريخ اعتماد نتيجة الامتحان.

h. سجلات ومستندات تتمتع جامعة حائل بسلطة تقديرية في تحديد لمدة اللازمة للاحتفاظ بها وترتبط السلطة التقديرية باستمرار حاجة جامعة حائل لها أو استخدامها والرجوع إليها ومنها:

- التقارير الاستشارية
- دليل السياسات والإجراءات (الأصلي / النسخ)
- التقارير السنوية.

i. إجراءات إتلاف الوثائق

- يجب عدم إزالة أو إتلاف السجلات الا ان كانت مصنفة بذلك وعند انتهاء مدة الاحتفاظ بها.
- عند الاحتفاظ بالسجلات خلال الفترة المحددة لها في جداول الاحتفاظ، يتم إعدادها للإتلاف.
- الوثائق المالية يتم إتلافها والتخلص منها وفق الإجراءات المحددة بلائحة الميزانية والحسابات والمخازن.
- الوثائق المالية والسجلات المتعلقة بالموظفين يتم اتلافها بوسيلة تضمن إتلاف المستندات إتلافا كليا.
- يتم التخلص من البيانات الالكترونية المحتفظ بها في الوسائط الاخرى عن طريق الإتلاف المادي لتلك الوسائط.
- يجب ان تتم عملية إتلاف السجلات بشكل آمن وكامل
- يجب تسجيل عملية الإتلاف في وثيقة رسمية لإتلاف البيانات داخل جامعة حائل

٦- نشر البيانات

a. البيانات المصنفة على أنها غير مقيدة يمكن أن تكون متاحة للعامة وجميع الموظفين وكذلك الأطراف الأخرى.

b. البيانات التي تحتاج إلى الحماية يمكن الوصول إليها عن طريق الوصول المصرح به، مثل الموظفين أو الشركاء وفق مبدأ " الحاجة إلى المعرفة" لأغراض ذات صلة بالأعمال. وينبغي منح هذا التصريح لفترة محددة وتحددها الأعلى مستوى.

c. تقتصر البيانات السرية على مجموعة من الأشخاص في وظيفة معينة تتطلب طبيعة عملهم ضرورة الوصول إلى البيانات السرية التي تحتفظ بها جامعة حائل.

d. البيانات المقيدة يتم الوصول إليها بموجب إجراءات رسمية ولأفراد متخصصين ومحددين على أساس الوظيفة.

٧- الوصول إلى البيانات

a. الأفراد المصرح لهم فقط يمكنهم الوصول إلى البيانات المتوفرة بشكل كامل

b. المستخدمين يصرح لهم الوصول للبيانات واستخدامها عند الطلب.

c. المصرح لهم فقط من الموظفين أو المجموعات أو المنظمات يمكنهم الوصول للبيانات اللازمة لإجراء العمل فقط، كما أن قيمة الملكية الفكرية محمية عند استخدام هذه البيانات.

الأدوار والمسؤوليات

١- **راعي ومالك وثيقة السياسة:** إدارة الأمن السيبراني
٢- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.
٣- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات و إدارة الأمن السيبراني.

الالتزام بالسياسة

١- يجب على مدير الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة بشكل دوري.
٢- يجب على كافة العاملين في جامعة حائل الالتزام بهذه السياسة.
٣- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

سياسة النسخ الاحتياطي

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بضمان حماية البيانات والمعلومات والإعدادات التقنية للأنظمة والتطبيقات الخاصة بجامعة حائل من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقا للسياسات والإجراءات التنظيمية لجامعة حائل والمتطلبات التشريعية والتنظيمية ذات العلاقة .بالإضافة إلى توفير إطار متسق لتطبيقه على عملية النسخ الاحتياطي للمساعدة في منع حدوث فقد في بيانات جامعة حائل من خلال ضمان توفر نسخ احتياطية من البيانات تعمل بشكل صحيح عند الحاجة إليها، سواء كان ذلك لمجرد استرداد ملف معين أو عند الحاجة إلى الاسترداد الكامل لأنظمة التشغيل وأنظمة التطبيقات الخاصة بالجامعة

نطاق العمل وقابلية التطبيق

تنطبق هذه السياسة على جميع البيانات المخزنة على أنظمة جامعة حائل، وعلى جميع أجهزة الكمبيوتر، سواء أجهزة الكمبيوتر المحمولة وأجهزة سطح المكتب، وعلى جميع الخوادم التي تملكها جامعة حائل وأي أجهزة إلكترونية أخرى تخزن البيانات.

بنود السياسة

١- تحديد البيانات الهامة

a. يجب أن تحدد **جامعة حائل** 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.

b. البيانات التي يتم نسخها احتياطيًا

سيتم الاحتفاظ بنسخة احتياطية من:

- جميع البيانات التي تقرر أنها هامة وحساسة لأعمال **جامعة حائل**.
- جميع المعلومات المخزنة على خادم الملفات التابعة لـجامعة حائل. وتقع على عاتق المستخدم ضمان نقل أي بيانات ذات أهمية إلى خادم الملفات.
- جميع البيانات المخزنة على خوادم الشبكة، والتي قد تتضمن خوادم الويب وخوادم قواعد البيانات ووحدات التحكم في النطاق والجدران النارية وخوادم الوصول عن بعد.

٢- تخزين النسخ الاحتياطي

a. يجب ان تخزن وسائط النسخ الاحتياطي في حاوية مقاومة للحريق وفي منطقة مؤمنة بأنظمة التحكم بالدخول.

b. يجب الحفاظ على الفصل الجغرافي بين أماكن حفظ النسخ الاحتياطية وموقع جامعة حائل، 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.

c. 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.

d. يسمح بالنسخ الاحتياطي عبر الإنترنت إذا كانت الخدمة تلبي المعايير المحددة هنا.

٣- تكرار النسخ الاحتياطي

a. يجب إجراء عملية النسخ الاحتياطي على فترات منتظمة.

b. الآلية التي يتم بها تكرار عملية النسخ الاحتياطي هي ما يضمن استعادة البيانات بنجاح، يتعين على جامعة حائل جدولة مواعيد مناسبة لعملية النسخ الاحتياطي متسقة مع طبيعة عمل جامعة حائل؛ 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.

c. 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 حائل.

d. يجب تحديد المستوى الذي تكون عنده المعلومات ضرورية ويتعين تخزين نسخ احتياطية لها.

e. 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.

٤- الاحتفاظ بالنسخ الاحتياطي

a. يجب أن تحدد جامعة حائل الوقت اللازم للاحتفاظ بالنسخ الاحتياطي، وما عدد النسخ المخزنة من البيانات المنسوخة احتياطياً الكافية للحد من المخاطر بكفاءة مع الحفاظ على البيانات المطلوبة.

b. 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.

٥- النسخ المخزنة

a. النسخ المخزنة يجب أن تخزن مع وصف قصير يتضمن المعلومات التالية:

تاريخ النسخ الاحتياطي / اسم النظام / نوع طريقة النسخ الاحتياطي (كامل / تزايدي).

b. 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.

c. 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.
- تقديم إيصال تسليم كدليل على أن النسخة الاحتياطية قد تم إرجاعها.

d. 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.

٦- اختبار عملية استعادة البيانات

a. 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.

b. يجب اختبار وسائط النسخ الاحتياطي بانتظام لضمان الاعتماد عليها للاستخدام الطارئ عند الضرورة.

c. يجب اختبار استعادة النسخ الاحتياطي عند إجراء أي تغيير قد يؤثر على نظام النسخ الاحتياطي.

d. 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 ذلك.

٧- وسائط النسخ الاحتياطي

a. 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

b. عند الحاجة إلى ضوابط خاصة لحماية المعلومات السرية أو الحساسة، ينبغي مراعاة ما يلي:

- استخدام أماكن تخزين (حاويات) آمنة.
- التسليم باليد.

c. يجب التخلص من جميع وسائط النسخ الاحتياطية بشكل مناسب، وذلك كما يلي:

- يجب تجهيز وسائط النسخ الاحتياطي للتخلص منها.
- يجب ألا 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.

d. 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

١- **راعي ومالك وثيقة السياسة:** إدارة الأمن السيبراني
٢- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.
٣- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات و إدارة الأمن السيبراني.

الالتزام بالسياسة

١- يجب على مدير الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة بشكل دوري.
٢- يجب على كافة العاملين في جامعة حائل الالتزام بهذه السياسة.
٣- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

سياسة إدارة مخاطر الأمن السيبراني

الأهداف

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لإدارة مخاطر الأمن السيبراني في جامعه حائل، 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-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية وأنظمة وأجهزة التحكم الصناعي الخاصة بـجامعه حائل وإجراءات عمل جامعه حائل، وتنطبق على جميع العاملين في جامعه حائل.

بنود السياسة

١- البنود العامة

١-١ يجب تطوير وتوثيق واعتماد منهجية إدارة مخاطر الأمن السيبراني (Cybersecurity Risk Management Methodology) وإجراءات إدارة مخاطر الأمن السيبراني في جامعه حائل، 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.

١-٢ يجب أن تغطي منهجية إدارة مخاطر الأمن السيبراني بحد أدنى ما يلي:

١-٢-١ تحديد الأصول ومعرفة أهميتها.

١-٢-٢ تحديد وتقييم المخاطر التي تمس أعمال أو أصول أو العاملين في جامعه حائل (مثل: الآثار المترتبة على جامعه حائل الناتجة عن المخاطر السيبرانية).

١-٢-٣ تحديد التهديدات والثغرات المتعلقة بالأمن السيبراني التي قد تؤثر على الأصول المعلوماتية والتقنية وتقييمها.

١-٢-٤ تحديد أساليب التعامل مع المخاطر السيبرانية.

١-٢-٥ ترتيب تدابير الحدّ من المخاطر السيبرانية حسب الأولية ووفق إجراءات محدّدة.

١-٢-٦ تصنيف مستويات المخاطر السيبرانية وتعريفها بناءً على مستوى التأثير واحتمالية حدوث التهديد لـجامعه حائل.

١-٢-٧ إنشاء سجل مخاطر الأمن السيبراني لتوثيق المخاطر ومتابعتها.

١-٢-٨ تحديد الأدوار والمسؤوليات لإدارة مخاطر الأمن السيبراني والتعامل معها.

١-٣ يجب تنفيذ تقييم المخاطر دورياً لضمان حماية الأصول المعلوماتية والتقنية والتعامل مع المخاطر حسب الأولوية.

١-٤ يجب أن تكون إدارة مخاطر الأمن السيبراني متوافقة مع إدارة المخاطر المؤسسية (Enterprise Risk Management "ERM") في جامعه حائل.

٢- المراحل الرئيسية لإدارة المخاطر السيبرانية

٢-١ تحديد المخاطر (Risk Identification): يجب أن تُحدّد إدارة الأمن 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.

٢-٢ تقييم المخاطر (Risk Assessment):

٢-٢-١ يجب على إدارة الأمن السيبراني تنفيذ إجراءات تقييم مخاطر الأمن السيبراني بحد أدنى في الحالات التالية:

٢-٢-١-١ في المراحل الأولى من المشاريع التقنية.

٢-٢-١-٢ قبل إجراء تغيير جوهري في البنية التقنية.

٢-٢-١-٣ عند التخطيط للحصول على خدمات طرف خارجي.

٢-٢-١-٤ عند التخطيط وقبل إطلاق منتجات وخدمات تقنية جديدة.

٢-٢-٢ يجب إعادة تقييم المخاطر وتحديثها على النحو التالي:

٢-٢-٢-١ دورياً لجميع الأصول المعلوماتية والتقنية، وسنوياً على الأقل للأنظمة الحسّاسة. (CSCC-1-2-1-1)

٢-٢-٢-٢ بعد وقوع حادث متعلّق بالأمن السيبراني ينتهك سلامة الأصول المعلوماتية والتقنية وتوافرها وسريّتها.

٢-٢-٢-٣ بعد الحصول على نتائج تدقيق مهمّة أو معلومات استباقية.

٢-٢-٢-٤ في حال التغيير على الأصول المعلوماتية والتقنية.

٢-٢-٣ يجب أن تغطي عملية تقييم المخاطر ما يلي:

٢-٢-٣-١ تحليل المخاطر (Risk Analysis): يجب أن تُقيّم إدارة الأمن السيبراني احتمالية وقوع التهديدات والآثار الناتجة عنها، وأن تستخدم نتائج هذا التقييم لتحديد المستوى العام لهذه المخاطر. ويجب أن تعتمد إدارة الأمن السيبراني منهجية كميّة (Quantitative) أو نوعيّة (Qualitative) لإجراء تحليل المخاطر.

٢-٢-٣-٢ تقدير المخاطر (Risk Evaluation): يجب أن تُقدِّر إدارة الأمن السيبراني حجم المخاطر السيبرانية بالتوافق مع معايير تقدير المخاطر المؤسسية المعتمدة في جامعه حائل، وتحديد أساليب التعامل معها حسب الأولوية.

٢-٣ معالجة المخاطر (Risk Treatment):

٢-٣-١ يجب أن تحدد إدارة الأمن السيبراني خيارات معالجة المخاطر حسب القائمة التالية:

٢-٣-١-١ 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.

٢-٣-١-٢ تجنّب المخاطر (Risk Avoidance): التخلص من الخطر بتجنب الاستمرار بمصدر الخطر.

٢-٣-١-٢-١ 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.

٢-٣-١-٢-٢ تقبّل المخاطر وتحمّلها (Risk Acceptance): مستوى الخطر مقبول ولكن يجب المراقبة باستمرار في حال حدوث تغيير.

٢-٣-٢ يجب تحديد خيارات معالجة المخاطر وتوثيقها بناءً على نتائج تقييم المخاطر وتكلفة التنفيذ والمنافع المتوقّعة.

٢-٤ متابعة المخاطر (Risk Oversight):

٢-٤-١ لمتابعة المخاطر يجب أن تُعِدّ إدارة الأمن السيبراني سجلاً للمخاطر وأن تحافظ عليه لتوثيق مخرجات عملية إدارة المخاطر. على أن يشمل بحد أدنى على المعلومات التالية:

٢-٤-١-١ عملية تحديد المخاطر.

٢-٤-١-٢ نطاق المخاطر.

٢-٤-١-٣ المسؤول أو صاحب المخاطر.

٢-٤-١-٤ وصف للمخاطر بما في ذلك أسبابها وآثارها.

٢-٤-١-٥ تحليل للمخاطر يُوضّح التأثيرات الناتجة عن المخاطر ونطاقها الزمني.

٢-٤-١-٦ تقييم وتصنيف للمخاطر يشتمل على احتمالية المخاطر وحجمها وتصنيفها الإجمالي في حال حدوثها.

٢-٤-١-٧ خطّة التعامل مع المخاطر تتضمّن إجراء التعامل معها والشخص المسؤول عنها وجدولها الزمني.

٢-٤-١-٨ وصف الخطر المتبقي.

٢-٤-٢ يجب استخدام مؤشر قياس الأداء (Key Performance Indicator "KPI") لضمان فعالية إدارة مخاطر الأمن السيبراني.

٢-٤-٣ يجب على إدارة الأمن السيبراني جمع الأدلة المتعلقة بحالة المخاطر السيبرانية ومراجعتها بشكل دوري.

٣- مستوى المخاطر المقبول (Risk Appetite)

٣-١ يجب تحديد معايير تقبّل المخاطر وتوثيقها، وفقاً لمستوى المخاطر وتكلفة معالجة الخطر مقابل تأثيره.

٣-٢ يجب تطبيق ضوابط إضافية من أجل تقليل المخاطر إلى مستوى مقبول في حال عدم استيفاء الخطر المتبقي لمعايير تقبّل المخاطر.

٣-٣ في حال تجاوز معايير تقبّل المخاطر، يتم التصعيد لصاحب الصلاحية لاتخاذ الإجراءات أو القرارات اللازمة.

٤- متطلبات أخرى

٤-١ 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.

٤-٢ يجب مراجعة سياسة إدارة مخاطر الأمن السيبراني سنوياً، وتوثيق التغييرات واعتمادها.

الأدوار والمسؤوليات

٤- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني بجامعه حائل
٥- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني بجامعه حائل
٦- **تنفيذ السياسة وتطبيقها:** إدارة الأمن السيبراني بجامعه حائل

الالتزام بالسياسة

٤- يجب على المشرف على إدارة الأمن السيبراني بجامعه حائل ضمان التزام جامعه حائل بهذه السياسة دورياً.

٥- يجب على جميع العاملين في جامعه حائل الالتزام بهذه السياسة.

٦- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعه حائل.

قائمة المحتويات

المقدمة

تتمثل رؤية البوابة الإلكترونية لجامعة حائل في سعي الجامعة لأن تصبح بوابتها الإلكترونية نافذة عملية للتعرف على أنشطة وخدمات الجامعة, كونها بيئة مناسبة لنشر المعرفة وحقلًا لتبادل الخبرات على المستووين الإقليمي والدولي الأمر الذي من شأنه أن يثري العملية التعليمية قدمًا إلى الامام. ولأن إدارة البوابة معنية ببذل قصارى جهدها لتقديم خدمة ذات جودة عالية لكل المستفيدين, فهي تضع سرية معلوماتهم على رأس قائمة الأولويات. وبالتالي حددت الإدارة عددًا من المبادئ الواجب مراعاتها من قبل مستخدم البوابة من أجل الحفاظ على خصوصية وسرية معلوماته, علمًا بأن تلك المبادئ تشكل فيما بينها سياسة للخصوصية وسرية المعلومات. وعلى زوار البوابة الاطلاع المستمر على سياسة الخصوصية وماتحويه من شروط ومبادئ لضمان سرية المعلومات من أجل التعرف على أي تحديثات تتم عليها, علمًا بأن إدارة البوابة غير مطالبة بالإعلان عن أية تحديثات تتم على تلك الشروط والمبادئ. ويعني استخدامك للبوابة أنك اطلعت ووافقت على تلك الشروط والمبادئ ومايتم عليها من تعديلات مستمرة.

النطاق

تم إعداد سياسة الخصوصية لمساعدة الزوار والمستخدمين على تفهم طبيعة البيانات التي يتم جمعها منهم عند زيارة البوابة وكيفية التعامل معها.

تتخذ البوابة الإلكترونية للجامعة الإجراءات والتدابير المناسبة والملائمة للحفاظ على المعلومات الشخصية التي لديها وحفظها بشكل آمن بما يضمن حمايتها من الفقدان أو الدخول غير المصرح به أو إساءة الإستخدام، أو التعديل والإفصاح غير المصرح بهما، ومن أهم التدابيرالمعمول بها في إدارة البوابة لحماية معلومات الزائر الشخصية ما يلي:

- الإجراءات والتدابيرالمشددة لحماية أمن المعلومات والتقنيات المستخدمة للوقاية من عمليات الاحتيال والدخول غيرالمصرح به إلى أنظمتنا.
- التحديث المستمر لإجراءات وضوابط الحماية التي تفي أو تزيد عن المعايير القياسية.
- تأهيل الموظفين المسؤولين عن إدارة البوابة وتدريبهم على احترام سرية المعلومات الشخصية لزوار البوابة وزائراتها.

البنود العامة

1- أمن المعلومات الشخصية

- تم إعداد هذه المعلومات المتعلقة بالخصوصية وسرية المعلومات لمساعدة الزوار والمستخدمين على تفهم طبيعة البيانات التي يتم جمعها منهم عند زيارة البوابة وكيفية التعامل معها.

- تقوم إدارة البوابة باتخاذ الإجراءات والتدابير المناسبة والملائمة للحفاظ على المعلومات الشخصية التي لديها بشكل آمن يضمن حمايتها من الفقدان أو الدخول غير المصرح به أو إساءة الاستخدام، أو التعديل والإفصاح غير المصرح بهما.

2- جمع المعلومات الشخصية

- عزيزي الزائر... اعلم أنه بمجرد زيارتك لبوابة جامعة حائل، فإن الخادم الخاص بالجامعة يقوم بتسجيل عنوان بروتوكول شبكة الإنترنت IP الخاص بالمستخدم وتاريخ ووقت الزيارة والعنوان URL الخاص بأي موقع إلكتروني تتم منه إحالتك إلى بوابة جامعة حائل.
- وكما هو الحال في معظم المواقع الإلكترونية؛ فبمجرد أن تتم زيارة البوابة يتم وضع ملف صغير على القرص الصلب الخاص بجهاز الزائر (المتصفح)، وهو ما يسمى بـ "كوكيز" (Cookies)، وملفات الكوكيز عبارة عن ملفات نصية، تقوم بعض المواقع التي تزورها بإيداعها على القرص الصلب في جهازك وهو ما يسهل من عملية دخولك إلى البوابة مستقبلاً والاستفادة مما يعرض عليها من خدمات، وتحتوي هذه الملفات النصية على معلومات تتيح للموقع الذي أودعها أن يسترجعها عند الحاجة لها خلال زيارة المستخدم المقبلة للموقع ومن هذه المعلومات المحفوظة:
  - حفظ رمز أمني لتعريف المستخدم في النظام.
  - حفظ إعدادات الصفحة في حال كان ذلك متاح على البوابة.
  - حفظ نوع المستخدم.
  - عدم إتاحة إمكانية التصويت أكثر من مرة لنفس المستخدم.
  - حفظ التطبيقات التي قام باستخدامها.
- وعلى هذا الأساس فإنَّ بوابة جامعة حائل ستستخدم المعلومات الموجودة في ملفات الكوكيز لأغراض فنية خاصة بها وذلك عند زيارتها أكثر من مرة، كما أن البوابة بإمكانها تغيير المعلومات الموجودة ضمن ملفات الكوكيز أو إضافة معلومات جديدة كلما قمت بزيارتها.
- إذا أرسلت لنا بريداً إلكترونياً عبر البوابة الإلكترونية لجامعة حائل تزودنا فيه ببيانات شخصية، فإننا قد نتقاسم البيانات الضرورية مع جهات أو إدارات أخرى، وذلك لخدمتك بصورة أكثر فعالية، ولن نتقاسم بياناتك الشخصية مع الجهات غير الحكومية إلا إذا كانت من الجهات المصرح لها من الجهات المختصة بالقيام بأداء خدمات حكومية محددة، وبتقديمك لبياناتك ومعلوماتك الشخصية من خلال البوابة الإلكترونية لجامعة حائل، فإنك توافق تمامًا على تخزين ومعالجة واستخدام تلك البيانات من قبل السلطات السعودية، ونحن نحتفظ بالحق في كل الأوقات في كشف أي معلومات للجهات المختصة، عندما يكون ذلك ضروريا للالتزام بأي قانون أو نظام أو طلب حكومي.
- أنت موافق إنك مسؤول بمفردك عن تمام وصحة وصدق البيانات التي ترسلها من خلال هذه البوابة.

3- حماية خصوصيتك

- لكي نتمكن من مساعدتك في حماية معلوماتك الشخصية فإننا نوصي بما يلي:

1- الاتصال بنا بشكل فوري عندما تظن أن شخصاً ما استطاع الحصول على كلمة السر الخاصة بك، أو رمز الاستخدام، أو الرقم السري، أو أي معلومات سرية أخرى.
2- لا تعط معلومات سرية عبر الهاتف أو شبكة الإنترنت ما لم تعرف هوية الشخص أو الطرف المستقبل للمعلومة.
3- استخدم متصفحاً آمناً عند قيامك بإنجاز المعاملات عبر الإنترنت مع إغلاق التطبيقات غير المستخدمة على الشبكة، وتأكد من أن برنامج الحماية من الفيروسات محدث على الدوام.
4- في حالة وجود أية استفسارات أو آراء حول مبادئ الخصوصية، يمكن التواصل مع إدارة البوابة عبر البريد الإلكتروني التالي: info@uoh.edu.sa

- للحفاظ على بياناتك الشخصية، يتم تأمين التخزين الإلكتروني والبيانات الشخصية المرسلة باستخدام التقنيات الأمنية المناسبة.
- هذه البوابة قد تحتوي على روابط إلكترونية لمواقع أو بوابات قد تستخدم طرقًا لحماية المعلومات وخصوصياتها تختلف عن الطرق المستخدمة لدينا. ونحن غير مسؤولين عن محتويات وطرق وخصوصيات هذه المواقع الأخرى، وننصحك بالرجوع إلى إشعارات الخصوصية الخاصة بتلك المواقع.

4- إرسال الرسائل الإلكترونية إلى الجامعة

عندما تقوم بالاستفسار أو طلب معلومات حول منتج ما أو خدمة محددة أو في حالة قيامك بإعطاء معلومات إضافية مستخدما أياً من وسائل الاتصال مع الجامعة سواء كانت إلكترونية أو غير إلكترونية، مثل طلب الاستفسار على موقعنا، فإننا سنستخدم عنوان بريدك الإلكتروني للرد على استفساراتك، كما أنه من الممكن حفظ عنوان بريدك ورسالتك وإجابتنا عليها لأغراض مراقبة الجودة، كما أننا قد نقوم بذلك للغايات القانونية والرقابية.