جامعة الجوف
Jouf University

سياسة العمل عن بعد

متاح

قائمة المحتويات

قائمة المحتويات 3
الأهداف 4
نطاق العمل وقابلية التطبيق 4
بنود السياسة 5
الأدوار والمسؤوليات 16
الالتزام بالسياسة 16

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة حسابات التواصل الاجتماعي الخاصة بـجامعة الجوف 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 وتمكين الجامعة من أداء إعمالها عن بعد بطريقة أمنة والتكيف مع التغييرات في بيئة الأعمال وأنظمة العمل عن بعد. وكذلك تعزيز قدرات الأمن السيبراني والصمود، عند إتاحة العمل عن بعد ضد التهديدات السيبرانية التي قد ينجم عنها تأثيرات سلبية وخسائر مكلفة. كما تسهم في رفع مستوى الأمن السيبراني على المستوى الوطني .

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأنظمة والإجراءات الخاصة بجامعة الجوف وتنطبق على جميع العاملين في جامعة الجوف.

بنود السياسة

◊ **سياسات وإجراءات الأمن السيبراني**

١-١ ضمان توثيق واعتماد ونشر متطلبات الأمن السيبراني والتزام الجهة بها، وذلك وفقاً لمتطلبات الأعمال التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-١-١ رجوعاً للضابط ١-٣-١ في الضوابط الأساسية للأمن السيبراني، يجب أن تشمل سياسات وإجراءات الأمن السيبراني ما يأتي:

١-١-١-١ تحديد وتوثيق متطلبات وضوابط الأمن السيبراني للعمل عن بعد ضمن سياسات الأمن السيبراني للجهة.

◊ **إدارة مخاطر الأمن السيبراني:**

١-٢ ضمان إدارة مخاطر الأمن السيبراني؛ لحماية الأصول المعلوماتية والتقنية للجهة، على نحو ممنهج؛ وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١-٢-١ بالإضافة للضوابط ضمن المكون الفرعي ١ - ٥ في الضوابط الأساسية للأمن السيبراني، يجب أن تشمل منهجية إدارة مخاطر الأمن السيبراني بحد أدنى ما يأتي:

١-٢-١-١ تقييم مخاطر الأمن السيبراني لأنظمة العمل عن بعد، مرة واحدة سنوياً، على الأقل.

١-٢-١-٢ تقييم مخاطر الأمن السيبراني عند التخطيط وقبل السماح بالعمل عن بعد لأي خدمه أو نظام.

١-٢-١-٣ تضمين مخاطر الأمن السيبراني الخاصة بأنظمة العمل عن بعد والخدمات والأنظمة المسموح لها بالعمل عن بعد في سجل مخاطر الأمن السيبراني الخاص بالجهة، ومتابعته مرة واحدة سنويا، على الأقل.

◊ **برنامج التوعية والتدريب بالأمن السيبراني**

١-٣ ضمان التأكد من أن العاملين بالجامعة لديهم التوعية الأمنية اللازمة وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني. والتأكد من تزويد العاملين بالجامعة بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجامعة والقيام بمسؤولياتهم تجاه الأمن السيبراني.

١-٤-١ بالإضافة للضوابط الفرعية ضمن الضابط ١ - ١٠- ٣ في الضوابط الأساسية للأمن السيبراني، فإنه يجب أن يغطي برنامج التوعية بالأمن السيبراني المخاطر والتهديدات السيبرانية للعمل عن بعد والاستخدام الآمن للحد من هذه المخاطر والتهديدات، بما في ذلك :

١-٣-١-١ الاستخدام الآمن للأجهزة المخصصة للعمل عن بعد والمحافظة عليها وحمايتها.

١-٣-١-٢ التعامل الآمن مع هويات الدخول وكلمات المرور.

١-٣-١-٣ حماية البيانات التي يتم حفظها على الأجهزة المستخدمة للعمل عن بعد والتعامل معها حسب تصنيفها وإجراءات وسياسات الجهة.

١-٣-١-٤ التعامل الآمن مع التطبيقات والحلول المستخدمة للعمل عن بعد كالاجتماعات الافتراضية والتعاون ومشاركة الملفات.

١-٣-١-٥ التعامل الآمن مع الشبكات المنزلية والتأكد من إعدادات الحماية الخاصة بها.

١-٣-١-٦ تجنب العمل عن بعد باستخدام أجهزة أو شبكات عامة غير موثوقة أو أثناء التواجد في أماكن عامة .

١-٣-١-٧ التواصل مباشرة مع إدارة الأمن السيبراني في الجامعة حال الاشتباه بتهديد أمن سيبراني.

١-٣-٢ بالإضافة للضوابط الفرعية ضمن الضابط ١ - ١٠ - ٤ في الضوابط الأساسية للأمن السيبراني، فإنه يجب تدريب العاملين المسؤولين عن إدارة حسابات التواصل الاجتماعي للجهة على المهارات التقنية والخطط والإجراءات اللازمة لضمان تطبيق متطلبات وممارسات الأمن السيبراني عند استخدام حسابات التواصل الاجتماعي.

◊ **إدارة الأصول**

١-٢ التأكد من أن الجامعة لديها قائمة جرد دقيقة، وحديثة للأصول؛ تشمل التفاصيل ذات العلاقة، لجميع الأصول المعلوماتية، والتقنية المتاحة للجامعة؛ وذلك من أجل دعم العمليات التشغيلية للجامعة، ومتطلبات الأمن السيبراني، بهدف تحقيق سرية الأصول المعلوماتية والتقنية للجامعة،

١-٢-١ بالإضافة للضوابط ضمن المكون الفرعي ١-٢ في الضوابط الأساسية للأمن السيبراني، يجب أن تشمل متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية، بحد أدنى، ما يلي:

١-٢-١-١ تحديد وحصر الأصول المعلوماتية والتقنية لأنظمة العمل عن بعد، وتحديثها مرة واحدة، كل سنة؛ على الأقل.

◊ **إدارة هويات الدخول والصلاحيات**

٢-٢ ضمان حماية الأمن السيبراني للوصول المنطقي (Logical Access) إلى الأصول المعلوماتية والتقنية للجامعة؛ من أجل منع الوصول غير المصرح به، وتقييد الوصول إلى ما هو مطلوب؛ لإنجاز الأعمال المتعلقة بالجامعة.

٢-٢-١ بالإضافة للضوابط الفرعية ضمن الضابط ٢-٢-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني المتعلقة بإدارة هويات الدخول، والصلاحيات لحسابات التواصل الاجتماعي للجامعة، بحد أدنى، ما يلي:

٢-٢-١-١ إدارة صلاحيات المستخدمين للعمل عن بعد بناءً على احتياجات العمل، مع مراعاة حساسية الأنظمة ومستوى الصلاحيات، ونوعية الأجهزة المستخدمة من قبل الموظفين للعمل عن بعد .

٢-٢-١-٢ تقييد إمكانية الوصول عن بعد لنفس المستخدم من أجهزة حاسبات متعددة في نفس الوقت (Concurrent Logins) .

٢-٢-١-٣ استخدام معايير آمنه لإدارة الهويات وكلمات المرور المستخدمة في أنظمة العمل عن بعد.

٢-٢-٢ رجوعاً للضابط الفرعي ٢-٢-٣-٥ في الضوابط الأساسية للأمن السيبراني، يجب مراجعة هويات الدخول والصلاحيات المستخدمة للعمل عن بعد، بحد أدنى مرة واحدة كل سنة.

◊ **حماية الأنظمة وأجهزة معالجة المعلومات**

٢-٣ ضمان حماية الأنظمة وأجهزة معالجة المعلومات بما في ذلك أجهزة المستخدمين والبنى التحتية للجهة من المخاطر السيبرانية.

٢-٣-١ بالإضافة للضوابط الفرعية ضمن الضابط ٢-٣-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن

السيبراني لحماية حسابات التواصل الاجتماعي للجامعة، والأصول التقنية الخاصة بها، بحد أدنى، ما يلي :

٢-٣-١-١ تطبيق حزم التحديثات، والإصلاحات الأمنية لأنظمة العمل عن بعد، مرة واحدة شهرياً على الأقل.

٢-٣-١-٢ مراجعة إعدادات الحماية لأنظمة العمل عن بعد والتحصين (Secure Configuration and Hardening)، مرة واحدة كل سنة على الأقل.

٢-٣-١-٣ مراجعة وتحصين الإعدادات المصنعية (default Configuration) للأصول التقنية لأنظمة العمل عن بعد، ومنها وجود كلمات مرور ثابتة وخلفية افتراضية،

٢-٣-١-٤ الإدارة الآمنة للجلسات (Secure Session Management)، ويشمل موثوقية الجلسات (Authenticity)، وأقفالها (Lockout)، وإنهاء مهلتها (Timeout)

٢-٣-١-٥ تقييد تفعيل الخصائص والخدمات في أنظمة العمل عن بعد حسب الحاجة، على أن يتم تحليل المخاطر السيبرانية المحتملة في حال الحاجة لتفعيلها.

◊ **إدارة أمن الشبكات**

٢-٤ ضمان حماية شبكات الجهة من المخاطر السيبرانية .

٢-٤-١ بالإضافة للضوابط الفرعية ضمن الضابط ٢-٥-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة أمن شبكات الجامعة للعمل عن بعد، بحد أدنى، ما يلي:

٢-٤-١-١ تقييد منافذ وبروتوكولات وخدمات الشبكة المستخدمة لعمليات الدخول عن بعد، وخصوصاً على الأنظمة الداخلية، وفتحها حسب الحاجة .

٢-٤-١-٢ مراجعة إعدادات وقوائم جدار الحماية (Firewall Rules) ذات العلاقة بأنظمة العمل عن بعد؛ مرة واحدة كل سنة على الأقل .

٢-٤-١-٤ الحماية من هجمات تعطيل الشبكات على أنظمة العمل عن بعد للحد من المخاطر الناتجة عن هجمات تعطيل الشبكات .

٢-٤-١-٤ الحماية من التهديدات المتقدمة المستمرة على مستوى الشبكة لأنظمة العمل عن بعد (Network APT)

◊ أمن الأجهزة المحمولة (Mobile Devices Security)

٢-٥ ضمان حماية أجهزة الجامعة المحمولة (بما في ذلك أجهزة الحاسب المحمول والهواتف الذكية والأجهزة الذكية اللوحية) من المخاطر السيبرانية. وضمان التعامل بشكل آمن مع المعلومات الحساسة والمعلومات الخاصة بأعمال الجهة وحمايتها أثناء النقل والتخزين عند استخدام الأجهزة الشخصية للعاملين في الجهة (مبدأ BYOD).

٢-٥-١ بالإضافة للضوابط الفرعية ضمن الضابط ٢- ٦ -٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة للعمل عن بعد في الجامعة، بحد أدنى، ما يلي:

٢-٥-١-١ إدارة الأجهزة المحمولة وأجهزة (BYOD) مركزياً باستخدام نظام إدارة الأجهزة المحمولة ((Mobile Device Management (MDM)).

٢-٥-١-٢ تطبيق حزم التحديثات، والإصلاحات الأمنية للأجهزة المحمولة، مرة واحدة شهريا، على الأقل.

◊ حماية البيانات والمعلومات (Data and Information Protection)

٢-٦ ضمان حماية السرية، وسلامة بيانات ومعلومات الجهة، ودقتها، وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٦-١ بالإضافة للضوابط الفرعية ضمن الضابط ٢-٧-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لحماية البيانات والمعلومات للعمل عن بعد في الجهة، بحد أدنى، ما يلي:

٢-٦-١-١ تحديد البيانات المصنفة، حسب التشريعات ذات العلاقة، التي يمكن استخدامها أو الوصول إليها أو التعامل معها من خلال أنظمة العمل عن بعد.

٢-٦-١-٢ حماية البيانات المصنفة، التي تم تحديدها في الضابط ٢-٦-١-١، باستخدام ضوابط مثل منع استخدام نوع من البيانات المصنفة أو تقنيات مثل منع تسريب البيانات (Data Leakage Prevention). ويمكن تحديد هذه الضوابط والتقنيات عن طريق تحليل المخاطر السيبرانية للجامعة.

◊ التشفير (Cryptography)

٢-٧ ضمان الاستخدام السليم والفعال للتشفير؛ لحماية الأصول المعلوماتية الإلكترونية للجهة، وذلك وفقاً للسياسات، والإجراءات التنظيمية للجامعة، والمتطلبات التشريعية والتنظيمية، ذات العلاقة.

٢-٧-١ بالإضافة للضوابط الفرعية ضمن الضابط ٢-٨-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بالتشفير لدى المشتركين، بحد أدنى ما يلي:

٢-٧-١-١ استخدام طرق وخوارزميات محدثة وآمنة للتشفير على كامل الاتصال الشبكي المستخدم للعمل عن بعد وفقاً للمستوى المتقدم (Advanced) ضمن المعايير الوطنية للتشفير (NCS – 1:2020).

◊ إدارة النسخ الاحتياطية (Backup and Recovery Management)

٢-٨ ضمان حماية بيانات ومعلومات الجهة، والإعدادات التقنية للأنظمة، والتطبيقات الخاصة بالجهة، من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقاً للسياسات، والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية، ذات العلاقة.

٢-٨-١ بالإضافة للضوابط الفرعية ضمن الضابط ٢-٩-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية لأنظمة العمل عن بعد في الجهة، بحد أدنى، مايلي:

٢-٨-١-١ عمل النسخ الاحتياطي على فترات زمنية مخطط لها؛ بناء على تقييم المخاطر للجامعة، لأنظمة العمل عن بعد. على أن يتم عمل النسخ الاحتياطية، لأنظمة العمل عن بعد مرة واحدة كل أسبوع.

٢-٨-٢ رجوعا للضابط٢-٩-٣-٣ في الضوابط الأساسية للأمن السيبراني، يجب إجراء فحص دوري؛ كل ستة أشهر على الأقل، لتحديد مدى فعالية استعادة النسخ الاحتياطية، الخاصة بأنظمة العمل عن بعد.

◊ **إدارة الثغرات(Vulnerabilities Management)**

٢-٩ ضمان اكتشاف الثغرات التقنية في الوقت المناسب، ومعالجتها بشكل فعال؛ وذلك لمنع احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية أو تقليلها، وكذلك التقليل من الآثار المترتبة على أعمال للجامعة.

٢-٩-١ بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٠-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة الثغرات للأصول التقنية وأنظمة العمل عن بعد، بحد أدنى، ما يلي:

٢-٩-١-١ فحص الثغرات واكتشافها على أنظمة العمل عن بعد وتصنيفها حسب خطورتها، مرة واحدة كل ثلاثة أشهر على الأقل.

٢-٩-١-٢ معالجة الثغرات على أنظمة العمل عن بعد، مرة واحدة كل ثلاثة أشهر على الأقل.

◊ **اختبار الاختراق (Penetration Testing)**

٢-١٠ تقييم مدى فعالية قدرات تعزيز الأمن السيبراني واختباره في الجهة؛ وذلك من خلال عمل محاكاة لتقنيات الهجوم السيبراني الفعلية وأساليبه، وكذلك اكتشاف نقاط الضعف الأمنية غير المعروفة التي قد تؤدي إلى الاختراق السيبراني للجامعة؛ وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-١٠-١ بالإضافة للضوابط الفرعية ضمن الضابط ٢-١١-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لاختبار الاختراق لأنظمة العمل عن بعد، بحد أدنى، ما يلي:

٢-١٠-١-١ نطاق عمل اختبار الاختراق، ليشمل جميع المكونات التقنية لأنظمة العمل عن بعد.

٢-١٠-٢ رجوعاً للضابط ٢-١١-٣-٢ في الضوابط الأساسية للأمن السيبراني، يجب عمل اختبار الاختراق على أنظمة العمل عن بعد مرة واحدة كل سنة على الأقل.

◊ **إدارة سجلات الأحداث ومراقبة الأمن السيبراني**

٢-١١ ضمان تجميع سجلات الأمن السيبراني وتحليلها ومراقبتها في الوقت المناسب؛ من أجل الاكتشاف الاستباقي للهجمات السيبرانية، وإدارة مخاطرها بفعالية؛ لمنع الآثار المترتبة على أعمال الجهة أو تقليلها.

٢-١١-١ بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٢-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات إدارة سجلات الأحداث، ومراقبة الأمن السيبراني للأصول التقنية وأنظمة العمل عن بعد للجامعة والأصول التقنية التابعة لها، بحد أدنى، ما يلي:

٢-١١-١-١ تفعيل سجلات الأحداث (Event Logs) الخاصة بالأمن السيبراني على الأصول التقنية وأنظمة العمل عن بعد.

٢-١١-١-٢ مراقبة سلوك مستخدمي أنظمة العمل عن بعد ((User Behavior Analytics (UBA) وتحليله.

٢-١١-١-٣ مراقبة سجلات الأحداث، الخاصة بالأصول التقنية وأنظمة العمل عن بعد على مدار الساعة.

٢-١١-١-٤ تحديث إجراءات مراقبة الأمن السيبراني على مدار الساعة وتطبيقها، بحيث تشمل مراقبة عمليات الدخول عن بعد، ولاسيما عمليات الدخول عن بعد من خارج المملكة والتحقق من صحتها.

٢-١١-٢ رجوعا للضابط ٢-١٢-٣-٥ في الضوابط الأساسية للأمن السيبراني، يجب ألا تقل مدة الاحتفاظ بسجلاتً الأحداث الخاصة بالأمن السيبراني لأنظمة العمل عن بعد عن ١٢ شهراً، حسب المتطلبات التشريعية والتنظيمية ذات العلاقة.

◊ إدارة حوادث وتهديدات الأمن السيبراني

٢-١٢ ضمان تحديد واكتشاف حوادث الأمن السيبراني في الوقت المناسب وإدارتها بشكل فعال والتعامل مع تهديدات الأمن السيبراني استباقياً من أجل منع أو تقليل الآثار المترتبة على أعمال الجهة، مع مراعاة ما ورد في الأمر السامي الكريم رقم (٣٧١٤٠) وتاريخ ١٤٣٨/٨/١٤ هـ

٢-١٢-١ بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٣-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات إدارة حوادث وتهديدات الأمن السيبراني في للجامعة، بحد أدنى، ما يلي:

٢-١٢-١-١ تحديث خطط الاستجابة لحوادث الأمن السيبراني ومعلومات التواصل داخل الجهة بما يتوافق مع حالة العمل عن بعد، وبما يضمن القدرة على التواصل وجاهزية فرق الاستجابة للحوادث.

٢-١٢-١-٢ الحصول على المعلومات الاستباقية (Threat Intelligence) ذات العلاقة بأنظمة العمل عن بعد بشكل دوري والتعامل معها.

٢-١٢-١-٣ تنفيذ وتطبيق التوصيات والتنبيهات الخاصة بحوادث وتهديدات الأمن السيبراني الصادرة من مشرف القطاع أو الهيئة الوطنية للأمن السيبراني.

◊ الأمن السيبراني المتعلق بالأطراف الخارجية

٣-١ ضمان حماية أصول الجهة من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية (بما في ذلك خدمات الإسناد لتقنية المعلومات والخدمات المدارة). وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٣-١-١ يجب تقييم مدى الحاجة لاستخدام خدمات إدارة حسابات التواصل الاجتماعي (social media management) والمراقبة

الآلية لحسابات التواصل الاجتماعي أو لحماية هوية الجهة من الانتحال (brand protection) ومخاطر الأمن السيبراني المتعلقة بها.

٣-١-٢ بالإضافة للضوابط الفرعية ضمن الضابط ٤ - ١ - ٢ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة باستخدام خدمات إدارة حسابات التواصل الاجتماعي (social media management) والمراقبة الآلية لحسابات التواصل الاجتماعي أو لحماية هوية الجهة من الانتحال (brand protection)، بحد أدنى، ما يلي:

٣-١-٢-١ بنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) والحذف الآمن من قبل الطرف الخارجي لبيانات الجهة عند انتهاء الخدمة .

٣-١-٢-٢ إجراءات التواصل للإبلاغ عن الثغرات وفي حال اكتشاف حادثة أمن سيبراني.

٣-١-٢-٣ إلزام الطرف الخارجي بتطبيق متطلبات وسياسات الأمن السيبراني لحماية حسابات التواصل الاجتماعي للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.

◊ الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة (Cloud Computing and Hosting Cybersecurity)

٣-١ ضمان معالجة المخاطر السيبرانية، وتنفيذ متطلبات الأمن السيبراني للحوسبة السحابية، والاستضافة بشكل ملائم وفعّال؛ وذلك وفقا للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية، والتنظيمية، والأوامر، والقراراتً ذات العلاقة. وضمان حماية الأصول المعلوماتية والتقنية للجهة، على خدمات الحوسبة السحابية؛ التي تتم استضافتها، أو معالجتها، أو إدارتها بواسطة أطراف خارجية.

١-٣-١ بالإضافة للضوابط الفرعية ضمن الضابط ٤-٢-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة باستخدام خدمات الحوسبة السحابية والاستضافة، بحد أدنى، ما يلي:

٣-١-١-١ موقع استضافة أنظمة العمل عن بعد يجب أن يكون داخل المملكة.