قرار مجلس الوزراء رقم (5) لسنة 2021م
بالمصادقة على سياسة أمن المعلومات

مجلس الوزراء،

استناداً لأحكام القانون الأساسي المعدل لسنة 2003م وتعديلاته،
وبعد الاطلاع على قرار مجلس الوزراء رقم (18/12/10/م.و/م.أ) لعام 2019م،
والاطلاع على قرار مجلس الوزراء رقم (13/127/08/م.و/س.ف) لعام 2012م،
وبناءً على تنسيب وزير الاتصالات وتكنولوجيا المعلومات،
وعلى الصلاحيات المخولة لنا،
وتحقيقاً للمصلحة العامة،

قرر مجلس الوزراء في جلسته المنعقدة بتاريخ 2021/08/30م، الآتي:

مادة (1)

المصادقة على سياسة أمن المعلومات المعدلة، المرفقة بهذا القرار.

مادة (2)

يلغى كل ما يتعارض مع أحكام هذا القرار.

مادة (3)

على الجهات المختصة كافة، كل فيما يخصه، تنفيذ أحكام هذا القرار، ويعمل به من تاريخ صدوره، وينشر في الجريدة الرسمية.

صدر في مدينة رام الله بتاريخ: 2021/08/30 ميلادية
الموافق: 22/محرم/1443 هجرية

د. محمد اشتية
رئيس الوزراء

سياسة أمن المعلومات

2021

1

الفهرس

دولة فلسطين رئاسة الوزراء / الأمانة العامة

3

4

دولة فلسطين رئاسة الوزراء / الأمانة العامة Council of Ministers / Cabinet Secretariat State of Palestine

5

المصطلحات	التعريفات
البيانات (Data)	هي مجموعة من الحروف، أو الكلمات، أو الأرقام، أو الرموز، أو الصور (الخام) المتعلقة بموضوع معين لا يكون لها معنى وتحتاج إلى معالجة.
المعلومات (Information)	البيانات التي تم معالجتها ليتم الاستفادة منها.
أنظمة المعلومات (Information systems)	مجموعة متكاملة من المكونات تستخدم لجمع، تخزين، ومعالجة البيانات بهدف توفير المعلومات والمعرفة والمنتجات الرقمية.
البرامج ((Programs	أي تطبيقات او أوامر منسقة حاسوبية تعمل بشكل مترابط لتنفيذ مهام معينه
الأصول (Asset)	أي موارد أو إمكانيات وتشمل أصول مقدم الخدمة وأي شيء يمكن أن يساهم في تقديم هذه الخدمة.
الثغرة (Vulnerability)	ضعف في أحد الأصول أو احدى عناصر التحكم الخاصة بالأصول ويمكن ان سببا لحدوث تهديد ما.
مستخدم النظام (user)	هو الشخص لذي يقوم باستخدام النظام بشكل روتيني لغايات الاستفادة من موارد الأصول.
مدير النظام (administrator)	هو الشخص المسؤول عن ادارة وصيانة الأصول والموارد وأنظمة المعلومات وصيانتها بشكل مستمر.
مالك الأصول (Asset Owner)	هو الشخص المسؤول عن المشتريات الشاملة، والتطوير، والتكامل، والتعديل، والتشغيل، والصيانة، والتقاعد لنظام المعلومات، حيث يعد "مالك الاصول" مساهمًا رئيسيًا في تطوير مواصفات تصميم النظام.
مدير/ مسؤول أمن النظام (System security administrator)	هو الشخص المسؤول عن اعطاء وحجب وتدقيق الصلاحيات للنظام الخاص به، وبما يتوافق مع الاحتياجات المطلوبة.
الشبكة الخاصة الافتراضية (VPN)	قناة اتصال غير مادية مشفرة يتم إنشاؤها عبر الانترنت بالاتفاق بين طرفين لضمان الاتصال ونفاذ البيانات الحساسة بينهما بطريقة آمنة.
دائرة تكنولوجيا المعلومات(IT)	هي الدائرة المختصة في التقنيات و/أو تكنولوجيا المعلومات او ما شابهها في العمل، وهي المسؤولة عن تكنولوجيا المعلومات والتطبيقات في المؤسسة.
الحادث(Incident)	مصطلح خاص بالحالات الاستثنائية أو الحالات التي تستدعي تدخل، والتي تحصل نتيجة محاولة لتغيير، أو

6

	تعطيل، أو تدمير، أو سرقة، أو وصول غير مصرح به أو استخدام غير مصرح به للأصول فضلاً عن انتهاكات لسياسات وإجراءات المؤسسة.
الحوسبة السحابية (cloud computing)	هي تقديم أو توصيل خدمات وموارد الحاسوب من (خوادم، قواعد بيانات، برامج، شبكات، مساحات تخزينية، تحليلات، ...) وكل ذلك من خلال شبكة الإنترنت، ويتم توفير واجهات لإدارة الخدمات المقدمة من خلال الحوسبة السحابية، وعادة ما تكون من خلال تطبيقات ويب.
السرية (confidentiality)	حماية المعلومات من الوصول إليها من قبل أطراف غير مصرح لها بالوصول سواء من خلال السلوك المتعمد أو عن طريق الصدفة.
التكاملية(Integrity)	التأكد من دقة واكتمال المعلومات وعدم تعديلها من قبل أشخاص غير مصرح لهم.
التوافرية(Availability)	إتاحة الوصول للمعلومات للجهات المخولة عند الحاجة.
المسؤولية (accountability)	تحديد مسؤولية كل شخص يعمل على أنظمة أمن المعلومات لضمان أمن المعلومات.
عدم التنصل ((non repudiation	ضمان عدم تنصل من أي حدث قام به.
الضيف (Guest)	هو كل زائر قد يكون عميل معتمد لدى المؤسسة او عميل متوقع.
نظام كشف التسلل (IDS)	هو نظام يقوم بمسح الشبكة ويراقب حركة مرور الشبكة بحثًا عن أي نشاط مشبوه أو ضار أو انتهاك للسياسة حيث يصدر تنبيهات عند اكتشاف مثل هذا النشاط.
نظام منع التسلل (IPS)	هو نظام يقوم بمسح الشبكة ويراقب حركة مرور الشبكة بحثًا عن أي نشاط مشبوه أو ضار أو انتهاك للسياسة حيث يصدر تنبيهات عند اكتشاف مثل هذا النشاط ويمنعه.
إدارة الوصول ((Access management	العملية المسؤولة عن السماح للمستخدمين بالاستفادة من خدمات تكنولوجيا المعلومات أو البيانات أو الأصول الاخرى.
التدقيق(auditing)	التحقق الرسمي للتأكد من اتباع معيار معين او ارشادات لتدقيق السجلات من اجل تحقيق الكفاءة والفعالية في العمل.
مزود خدمة خارجي(ISP)	طرف خارجي يقوم بتزويد المؤسسة بخدمة معينة.
هوية(Identity)	اسم أو رمز فريد يستخدم لتعريف مستخدم أو شخص أو دور.
سياسة امن المعلومات (Information	السياسة التي تحكم نهج المؤسسة لإدارة أمن المعلومات.

7

(Security Policy	
السياسات(Policies)	مجموعة البنود والتعليمات الموثقة والتي تستخدم لتوجيه القرارات ولضمان التطوير والتنفيذ الملائم للعمليات والمعايير والانشطة والبنية التحتية لتكنولوجيا المعلومات.
الاستعانة بمصدر خارجي(Third party)	استخدام مزود خارجي لإدارة خدمات تكنولوجيا المعلومات.
المخاطرة(Risk)	حدث محتمل يمكن أن يتسبب في ضرر أو خسارة قد يؤثر على القدرة على تحقيق الأهداف.
مستوى الخدمة (Service level)	قياس الانجاز والابلاغ عنه مقابل هدف واحد او أكثر من أهداف مستوى الخدمة.
مركز الحاسوب الحكومي (GCC)	النواة الأساسية للخدمات الإلكترونية المقدمة للمؤسسات والهيئات الحكومية، يقوم المركز باستضافة الخوادم التي تقدم الخدمات الإلكترونية لجهات مختلفة من مؤسسات وهيئات حكومية، وتشمل الخوادم الفعلية والخوادم الافتراضية القادرة على احتواء المعلومات والبيانات اللازمة، كما يقوم المركز بحفظ البيانات بأنواعها المختلفة للرجوع لها في حالة الطوارئ، وذلك من خلال التخزين الاحتياطي بتقنيات متقدمة تُمكن من التأكد من سلامة البيانات المخزنة وسهولة وسرعة استرجاعها عند الحاجة.

دولة فلسطين رئاسة الوزراء / الأمانة العامة Council of Ministers / Cabinet Secretariat State of Palestine

1 المقدمة

تعتمد مؤسسات الدولة على أنظمة المعلومات والتقنيات الحديثة والمعلومات في عملها؛ ان تسريب معلومات من هذه المؤسسات عن طبيعة عملها أو معلومات تتعلق بالمواطنين يؤدي إلى إلحاق خسائر مادية ومعنوية بالمؤسسة، لذلك يجب حمايتها والتأكد من سريتها وتكاملها وتوافرها، وللحفاظ على أمن المعلومات يجب وضع السياسات والإجراءات الكفيلة بحماية المعلومات.

إن الحفاظ على أمن هذه الأنظمة والمعلومات يعتبر من الاهتمامات الرئيسية للإدارة العليا في المؤسسة التي تعمل جنباً إلى جنب مع مجلس الوزراء لإطلاق ودعم الجهود المبذولة لتعزيز أمن المعلومات، وتعتبر هذه السياسة من العناصر الرئيسية في نظام إدارة أمن المعلومات.

إن العمل في أمن المعلومات يحتاج إلى العمل بروح الفريق ويحتاج إلى المشاركة والدعم من كافة الموظفين الذين يستخدمون أنظمة المعلومات؛ وإدراكاً منا لأهمية العمل بروح الفريق فإن هذه السياسة توضح مسؤوليات المستخدمين والخطوات الواجب إتباعها للمساعدة في حماية المعلومات وأنظمتها، كما تتضمن هذه السياسة الطرق الواجب إتباعها في مواجهة التهديدات المختلفة مثل الاستخدام غير المسموح به والاختراق ونشر ونسخ وتغيير وتدمير وفقد المعلومات وسوء الاستخدام ومنع الاستخدام وغيرها من التهديدات. كما ويجب تحديد المخالفات، العقوبات، والإجراءات التأديبية المترتبة على عدم الالتزام وانتهاك سياسات وإجراءات أمن المعلومات المعتمدة في المؤسسة وكذلك يجب تحديد الجهة المخولة والمسؤولة عن تنفيذ العقوبات، وتحديد آلية التبليغ عن المخالفات بما لا يتعارض مع القوانين المعمول بها.

8

لقد تم إعداد وتعميم هذه السياسة لتحديد الاتجاه المناسب للتعامل مع أمن المعلومات في المؤسسة وبما يتناسب مع المعايير العالمية بهذا الشأن وخاصة معايير .ISO27001

إن الأهداف المطلوب تحقيقها من هذه السياسة تتحقق بتطبيق بنود هذه السياسة بالطريقة الأنسب لطبيعة عمل وبيئة المؤسسة، ويتمثل في تطوير وتطبيق إجراءات العمل بما يتماشى مع هذه السياسة أو من خلال فرز سياسة متخصصة لتناول كل بند بشمولية وتخصص أو من خلال الطريقتين معا: الإجراءات وفرز السياسات المتخصصة.

وعلى كل مؤسسة إصدار التعليمات بما يتماشى مع هذه السياسات والتوجيهات العامة في هذه الوثيقة كل فيما يخصه بما ينسجم مع طبيعة عمل وهيكلية المؤسسة.

1.1 الهدف

تهدف وثيقة سياسة أمن المعلومات هذه إلى تحديد متطلبات الأمن للاستخدام السليم والآمن لخدمات تكنولوجيا المعلومات في المؤسسة. وهدفها هو حماية المؤسسة وجميع مستخدمي الانظمة من التهديدات الأمنية التي قد تعرض نزاهتهم وخصوصيتهم وسمعتهم ونتائج أعمالهم للخطر.

1.2 النطاق

تنطبق هذه السياسة على كافة مؤسسات الدولة وموظفيها الدائمين او المؤقتين، كما وتشمل كل من الشركاء الذين لديهم وقت وصول محدد أو غير محدد لخدمات المؤسسة والزوار الذين لديهم وصول مؤقت. وتعتبر جميع عناصر هذه السياسة الزامية وعلى الجميع تطبيقها والالتزام بها.

1.3 تاريخ المستند

	نسخة الإصدار	الوصف	التاريخ	الفريق	التعديلات
1	0.5	مسودة	كانون أول /2019	ابراهيم أبو بكر، ناديه صوان، آية فاخوري، بركات عبوه، يعرب عواد.	النسخة الأولى من مسودة سياسة أمن المعلومات.
2	0.8	مسودة	كانون الأول / 2020	ابراهيم أبو بكر، ناديه صوان، آية فاخوري، بركات عبوه، يعرب عواد، محمد علوي.	جمع وتدوين الملاحظات الواردة من كافة المؤسسات والوزارات الحكومية
3	1	مسودة	نيسان/ 2021	ابراهيم أبو بكر، ناديه صوان، آية فاخوري، بركات عبوه، يعرب عواد.	عرضها للقراءة الثالثة من سياسة أمن المعلومات
4	1.1	نهائية	تموز /2021	ابراهيم أبو بكر، آية فاخوري، بركات عبوه، يعرب عواد.	بعد دراسة الملاحظات في القراءة الثالثة

9

1.4 المسؤوليات

المسؤوليات المترتبة على موظفي أمن المعلومات في الدوائر الحكومية تبعا للمسمى الوظيفي:

المسمى الوظيفي	المهام
مسؤول أمن المعلومات	• مراقبة تطوير السياسات والإجراءات الأمنية حيث إن هذه السياسات بمثابة القواعد الأمنية التي سيلتزم بها كافة موظفي المؤسسة لتحقيق أقصى درجات الأمان المعلوماتي. • مراقبة حماية شبكة المؤسسة باستخدام أجهزة الجدر النارية. • مراقبة حماية خوادم وحواسيب المؤسسة من خلال التحميل والتحديث المستمر للبرامج المضادة الفيروسات. • مراقبة حماية أنظمة البريد الإلكتروني للمؤسسة ضد الرسائل الإلكترونية المضرة والبريد التطفلي من خلال تحديث ومراقبة نظام حماية البريد الإلكتروني. • مراقبة الشبكة والانظمة من منظور أمني وكشف حوادث ومحاولات الاختراق، والتعامل السريع معها لمنع حدوثها أو الحد من آثارها. • تطبيق المعايير الدولية لأمن المعلومات مثل ISO27001، والذي يهتم بتطوير وتنفيذ وتشغيل ومراقبة نظام أمن معلومات موثوق، ويهدف الى إدارة فعالة ومستمرة للمخاطر وتوفر حماية مناسبة للمعلومات حسب أهميتها. • تنفيذ برامج توعوية لأمن المعلومات من خلال طرق ووسائل مختلفة، ومنها برامج توعوية تفاعلية لموظفي المؤسسة من خلال الشبكة الداخلية. • مراجعة صلاحيات المستخدمين لأنظمة المؤسسة بشكل مستمر والتأكد من أحقية المستخدم للصلاحيات المعطاة واقتصارها على حاجة العمل. • تقييم للمخاطر والتأكد من أمن كافة الأنظمة بشكل مستمر وذلك بالقيام بالمسح الأمني Vulnerability Assessment وتطبيق حلول عاجلة ومضادة للثغرات الموجودة على كافة المستويات: الشبكة الخارجية، الشبكة الداخلية، الانظمة قواعد المعلومات والتطبيقات. • متابعة أحدث إصدارات التطبيقات والبرامج ذات العلاقة بأمن المعلومات، والتحديث المستمر لها بما يضمن بيئة معلوماتية آمنة.
إدارة الأمن وملكية النظام	مالكي الأنظمة والمعلومات هم مدراء الإدارات والدوائر وأعضاء الإدارة العليا أو من ينوب عنهم في المؤسسة ممن يتحملون مسؤولية تنفيذ وتطوير ومتابعة الأنظمة والبرامج والتطبيقات المختلفة التي تتعامل مع البيانات والمعلومات بما يخدم مصلحة العمل، ويجب أن يتم اعتماد مدير أمن/مالك لكل نظام، وهو مسؤول عن تصنيف المعلومات من حيث السرية ويملك قرار السماح باستخدام النظام.
مسؤوليات تقنية أمن المعلومات	يجب أن يتم تعيين فني واحد أو أكثر لكل نظام من أنظمة المعلومات أو مصادر المعلومات، وفني الأمن يمتلك الصلاحيات الكاملة لتطبيق السياسات الأمنية على النظام

	أو مصدر المعلومات المسؤول عنه بشريطة اعلام المسؤول المباشر بشكل رسمي لكي يتم اعلام اصحاب العلاقة ان لزم الامر. يكون فني الأمن وبالتعاون مع الموظفين الأخرين من دائرة تقنية المعلومات مسؤول عن حماية المعلومات من المخاطر المختلفة، بالإضافة الى تنفيذ وتطبيق السياسات والإجراءات الأمنية المعتمدة، ويعتبر أي موظف فني في إدارة تقنية المعلومات فني أمن وكذلك يعتبر المستخدم فني أمن على المعلومات المحفوظة على جهاز الحاسوب الذي يستخدمه.
مسؤوليات إدارة الشبكة	1. مسؤول عن تجهيز وتركيب أجهزة الشبكات داخل المؤسسة وضبط اعدادات الشبكة الخارجية والداخلية التابعة لها، وتوصيل كافة أجهزة الحواسيب بها مع تحديد الصلاحيات، وضبط اعدادات أجهزة الخوادم وتوفير الصيانة الدورية لها، وعرض التوصيات الخاصة بشراء أجهزة ومعدات حديثة لتطوير الشبكة الخاصة بالمؤسسة وتوفير كافة وسائل الحماية والأمان لتجنب مشاكل الاختراقات وسرقة البيانات لشبكة وخوادم وحواسيب المؤسسة، بالإضافة إلى كل ما يتعلق بالنسخ الاحتياطي. 2. تنفيذ سياسات امن المعلومات والتعليمات والاجراءات فنيا واداريا المتعلقة في امن المعلومات على كافة الاجهزة التي تتعلق بالشبكة.
إدارة النظام	لدى مدير الانظمة الكثير من المسؤوليات المتعلقة بحفظ وتشغيل أنظمة الحواسيب، و تنزيل كافة البرامج الحاسوبية المتعلقة بالمؤسسة، وصيانة الخوادم وأجهزة الحواسيب أو أي أنظمة حاسوبية تابعة لها، وأيضاً التخطيط والتجاوب مع انقطاع الخدمة، وكل ما يتعلق بالدعم الفني والمشاكل الأخرى، وإدارة مشروعات تابعة للأنظمة المختلفة بالإضافة إلى إدارة كلمات المرور المتعلقة بحسابات المستخدمين و المحولات (راوتر) والموجهات الافتراضية، لذا يجب على مدراء النظام تغيير أسماء حسابات المدراء وتعطيل أي حساب موجود مسبقاً وعدم استخدامه لاحقاً مهما كان عدد هذه الحسابات، كإجراء أولي في هذا الصدد، حيث إن ترك هذه الحسابات وكلمات المرور كما هي يجعل من السهل على المخترقين التسلل إلى الشبكة.
مسؤوليات المستخدم	المستخدم مسؤول عن الالتزام بسياسات ومعايير وإجراءات أمن المعلومات المعتمدة وتعلمها.

11

1.5 عناصر السياسة العامة

1.5.1 التقيد بتعليمات هذه الوثيقة مطلوب من جميع موظفي المؤسسة، المستشارين، والأطراف الأخرى الذين يتم التعاقد معهم من قبل المؤسسة أو من قبل أي طرف آخر للعمل بالمؤسسة وتحدده المؤسسة.

1.5.2 يوقع كل موظف يستخدم أنظمة المعلومات و/أو التقنيات المعمول بها في المؤسسة على إقرار وتعهد بأن الموظف قد قرأ وفهم ووافق على الالتزام بسياسات ومعايير وإجراءات أمن المعلومات المعتمدة في المؤسسة.

1.5.3 الالتزام بالتعليمات والمسؤوليات والسياسات ضمن هذه الوثيقة لضمان السرية، والسلامة، وعدم ضياع المعلومات المتعلقة بعمل المؤسسة.

1.5.4 لا يجوز السماح باستثناءات للسياسات المحددة في أي جزء من هذه الوثيقة إلا من قبل الادارة العليا للمؤسسة وبالتنسيق مع مسؤول أمن المعلومات.

1.5.5 في حالة الحصول على أي استثناء يتم تسجيله في سجل الحوادث مع تحديد التاريخ والوقت والوصف وسبب الاستثناء وكيفية إدارة المخاطر.

1.5.6 في حالة مواجهة الموظف لأي أمر طارئ، أو خلل تقني، أو غير تقني، أو مشكلة في خدمات المؤسسة، يقوم الموظف بالتبليغ عن المشكلة حسب التسلل الإداري.

1.5.7 يجب استخدام جميع الخدمات التي تقدمها المؤسسة وفقًا للمتطلبات الفنية والأمنية المحددة في تصميم الخدمات.

1.5.8 قد تؤدي مخالفة السياسات الواردة في هذه الوثيقة إلى اتخاذ إجراءات تأديبية. في بعض الحالات الخطيرة يمكن أن تؤدي إلى المحاكمة.

2 السياسة العامة ومعايير أمن المعلومات

2.1 الهدف

تحديد مجموعة القواعد التي تهدف الى توعية الموظفين بأفضل الممارسات لضمان سرية وحماية المعلومات والموارد.

2.2 النطاق

تنطبق هذه السياسة على جميع موظفي المؤسسة والزوار او اي شخص يمنح صلاحية وصول بشكل دائم او مؤقت لموارد المؤسسة.

2.3 عناصر السياسة

2.3.1 سياسة التوعية بأمن المعلومات

2.3.1.1 الهدف

ضمان توفير التوعية اللازمة لجميع موظفي الوزارات والمؤسسات الحكومية لغايات إتباع أفضل الممارسات لضمان سلامة أمن المعلومات.

2.3.1.2 النطاق

تنطبق هذه السياسة على كافة المؤسسات والعاملين فيها بصفة دائمة او مؤقتة

2.3.1.3 عناصر السياسة

2.3.1.3.1 تنظم دائرة تكنولوجيا المعلومات ورشة واحدة على الأقل سنويا تكرر في موعد لاحق من نفس العام، بحيث يكون الحضور الزامي لجميع الموظفين لغاية توضيح أساسيات أمن المعلومات للموظفين.

2.3.1.3.2 نشر مادة الورشة من خلال البوابة الالكترونية والبريد الالكتروني لجميع الموظفين وأي وسيلة اخرى تراها المؤسسة مناسبة.

2.3.1.3.3 يقدم قسم الموارد البشرية لكل موظف جديد كراسة أو كتيب للتوعية بأمن المعلومات على أن تتضمن الصفحة الأخيرة "الإقرارات" التي يتوجب أن يوقع عليها الموظف.

2.3.1.3.4 يقع على عاتق كل موظف مواكبة التحديثات عبر مشاركته بالدورات التدريبية الخاصة بأمن المعلومات والتي تنفذ من قبل الادارة المختصة.

2.3.1.3.5 يجب تعميم نشرات توعوية والتنبيهات المتعلقة بامن المعلومات على كافة الموفين من خلال الوسائط المعمول بها ف بالمؤسسة كالبريد الالكتروني، وبوابة الموظف، ولوحة الاعلانات، وغيرها.

2.3.2 سياسة معايير أمن المعلومات

2.3.2.1 الهدف

تحديد المعايير التي تهدف هذه السياسة الى الحفاظ عليها

2.3.2.2 النطاق

تنطبق هذه السياسة على جميع الوثائق المتعلقة بسياسات ومعايير أمن المعلومات والاشخاص القائمين على تطبيقها وموظفي المؤسسة الدائمين او المؤقتين

2.3.2.3 عناصر السياسة

2.3.2.3.1 تعتبر سياسات وإجراءات ومعايير ومقاييس أمن المعلومات المستخدمة في المؤسسة وكل ما يتعلق بها معلومات سرية لا يسمح نشرها أو إطلاع أطراف خارجية عليها.

2.3.2.3.2 يجب الامتثال لمعايير امن المعلومات المعتمدة لكل من الانظمة والشبكات ومراجعة تطبيقها.

2.3.3 سياسة سرية المعلومات

2.3.3.1 الهدف

تحديد القواعد الواجب اتباعها لضمان خصوصية وسرية البيانات الخاصة بالمؤسسة والافراد العاملين فيها

2.3.3.2 النطاق

جميع موظفي المؤسسة والعاملين المؤقتين او ما يطلق عليهم بالطرف الثالث

2.3.3.3 عناصر السياسة

2.3.3.3.1 يلتزم الموظف التزاما تاما بسياسات أمن المعلومات الصادرة عن المؤسسة او السياسات العامة الصادرة عن الحكومة.

2.3.3.3.2 يلتزم الموظف التزاما تاما باتفاقية عدم الافصاح في التعامل مع المعلومات السرية المتعلقة بالمؤسسة او عمل المؤسسة.

2.3.3.3.3 لا يجوز للموظف الافصاح عن اي معلومات سرية تتعلق بالمؤسسة أو عملها لاي شخص داخل/خارج المؤسسة الا بموافقة الادارة المعنية.

2.3.3.3.4 يقع على الموظف مسؤولية منع الوصول غير المصرح به الى المصادر التي تقع تحت مسؤوليته الخاصة مثل الحاسب الالي او المعلومات التي يعمل عليها او يعالجها.

13

2.3.3.3.5 يمنع على الموظف طباعة او نقل اي معلومات سرية وفي حالة الحاجة الى ذلك يتم بموافقة الادارة المعنية وعلى طابعات او وسائل نقل توفر عناصر التحكم بالوصول.

2.3.3.3.6 على الموظف التأكد من تأمين الموارد السرية التي يعمل عليها عند ترك الحاسب او الملفات وذلك لضمان عدم وصول أحد اليها.

2.3.3.3.7 يقع على عاتق الموظف رفع كامل المعلومات التي يعمل عليها على السيرفر المركزي حسب الملف المخصص له من قبل إدارة الحاسوب ولا تتحمل الادارة أي فقدان للبيانات على جهاز الموظف.

2.4 سياسة التعاقد مع الأطراف الخارجية

2.4.1 الهدف

ضمان سرية وأمن البيانات المعروضة على الأطراف الخارجية.

2.4.2 النطاق

جميع موظفي المؤسسة والعاملين المؤقتين او ما يطلق عليهم بالطرف الثالث.

2.4.3 عناصر السياسة

2.4.3.1 على اي طرف ثالث يتم التعاقد معه الالتزام بسياسة أمن المعلومات واي سياسات داخلية معتمدة.

2.4.3.2 تعتبر جميع المعلومات في المؤسسة خاصة ما لم يتم نشرها ضمن وسائل الإعلام العامة ويمنع إطلاع أطراف خارجية عليها، وأي طرف خارجي يحتاج الاطلاع على معلومات خاصة بالمؤسسة يجب أن يتبع الإجراءات الداخلية المتبعة لذلك بالإضافة إلى الحصول على الموافقة الخطية من الموظف الذي تم تعيينه مدير أمن النظام وتوقيع اتفاقية عدم نشر المعلومات المعتمدة في المؤسسة. وفي حال تم فقد أو تسريب معلومات خاصة بالمؤسسة لطرف خارجي غير مسموح له الاطلاع عليها أو لمجرد الشك في حدوث ذلك يجب على الموظف إبلاغ دائرة تقنية المعلومات أو الموظف المسؤول عن إدارة أمن المعلومات مباشرة وبشكل خطي.

2.4.3.3 توقيع الطرف الخارجي على اتفاقية سرية البيانات واتفاقيات اخرى معتمدة من قبل الجهة الحكومية.

2.5 سياسة تصنيف المعلومات

2.5.1 الهدف

تحديد سياسة المؤسسة فيما يتعلق بتصنيف البيانات حسب حساسيتها وسريتها لتحديد مستوى الحماية المناسب لهذه المعلومات.

2.5.2 النطاق

جميع موظفي المؤسسة والعاملين المؤقتين.

2.5.3 عناصر السياسة

2.5.3.1 يجب تصنيف المعلومات حسب مدى حاجتها للحماية وأولويتها والدرجة المطلوبة من الحماية عند التعامل معها.

2.5.3.2 يجب استخدام خطة لتصنيف المعلومات لتحديد مجموعة مناسبة من مستويات الحماية وتوضيح الحاجة إلى إجراءات خاصة للتعامل مع المعلومات.

14

2.5.3.3 تقع على عاتق مالك الأصل مسؤولية تحديد وتصنيف حساسية المعلومات بشكل دوري والتأكد من تحديثها بالمستوى المناسب.

2.5.3.4 ضبط اعدادات أنظمة الأرشفة الإلكترونية وإدارة الوثائق بما يشمل ضبط درجة التصنيف.

2.6 سياسة تشفير البيانات

2.6.1 الهدف

تحديد سياسة المؤسسة فيما يتعلق باستخدام ضوابط التشفير وإدارتها.

2.6.2 النطاق

جميع موظفي المؤسسة والعاملين المؤقتين

2.6.3 عناصر السياسة

2.6.3.1 يتم تحديد الحاجة للتشفير بناء على حساسية وتصنيف البيانات من ناحية السرية

2.6.3.2 يتم تحديد تقنية التشفير المستخدمة بناء على تصنيف البيانات والاشخاص المخول لهم الوصول اليها، حيث ان زيادة عدد الاشخاص المخول لهم بالوصول للبيانات يمكن ان يكون سببا في زيادة خطر تسريب البيانات وبالتالي يمكن استخدام تقنيات تشفير وبطرق مختلفة لضمان عدم تسريب البيانات او تحديد الشخص الذي سرب البيانات.

2.6.3.3 يجب النظر بأي قيود قانونية سواء على مستوى المؤسسة او الدولة قد تجبر على ضمان حد أدنى من قوة عمليات التشفير او تمنع تقنيات تشفير معينة.

2.6.3.4 عند تطبيق تقنية التشفير يجب ضمان سلامة البيانات وانه يمكن استرجاعها دون تلف او ضياع، حيث يفضل عند تشفير البيانات ان يتم فك التشفير لحظيا للتأكد من ان البيانات تم تشفيرها بشكل صحيح ولم يكن هناك اي اخطاء في العملية أدت الى تلف او ضياع البيانات.

2.6.3.5 يجب مراجعة تقنيات التشفير بشكل دوري لفحص جودة التقنية المستخدمة او امكانية ظهور هجمة قد تؤدي الى كسر التشفير وبالتالي كشف او تسريب بيانات ذات حساسية عالية.

3 سياسة الاستخدام المقبول

3.1 الهدف

تحديد مجموعة القواعد التي تحكم طرق استخدام موارد المؤسسة من قبل المستخدمين. بالإضافة الى تقليل المخاطر المحتملة مثل البرمجيات الخبيثة والمشاكل القانونية.

3.2 النطاق

تنطبق هذه السياسة على جميع موظفي المؤسسة والزوار او اي شخص يمنح صلاحية وصول بشكل دائم او مؤقت لموارد المؤسسة.

3.3 عناصر السياسة

3.3.1 الاستخدام الشخصي

3.3.1.1 يجب ان يكون الاستخدام الأساسي لموارد تكنولوجيا المعلومات الخاصة بالمؤسسة مرتبطة بمجالات العمل وبعمليات التعليم والبحث.

3.3.1.2 يمنع استخدام أي من الموارد التكنولوجية التابعة للمؤسسة لأي غرض شخصي، وفي حال اقتضت الحاجة لذلك يجب الحصول على موافقة أو استثناء من الإدارة المخولة.

3.3.1.3 في حال الحصول على موافقة أو استثناء يجب أن يكون الاستخدام الشخصي ضمن الحد المقبول، ويعتبر الاستخدام لأغراض شخصية زائداً عن حده عندما يكون الاستخدام الشخصي في ساعات الدوام الرسمية وبشكل يؤثر على جودة وسرعة العمل أو إلى استخدام سعة كبيرة من سعة الشبكة أو يزيد من التكاليف التشغيلية.

3.3.1.4 على المؤسسة أن تقوم بتوعية وتوجيه المستخدمين نحو الاستخدام الصحيح للموارد ووضع القوانين والضوابط التي تضمن عدم انتهاك أي خصوصية او الاضرار بالأخرين.

3.3.2 استخدام البريد الالكتروني

3.3.2.1 لا يجوز استخدام أو استغلال هذه الخدمة في حال كان المستخدم ليس أحد موظفي الجهة المستفيدة.

3.3.2.2 لا يجوز استخدام او استغلال هذه الخدمة لأغراض مخالفة أو تخريبية.

3.3.2.3 يعتبر البريد الالكتروني الحكومي الوسيلة الوحيدة والأمثل لتنائل المعلومات والملفات الخاصة بعمل المؤسسة، وعليه يمنع تنائل أي معلومات أو ملفات خاصة بعمل المؤسسة خارج البريد الالكتروني الحكومي أو على مواقع التواصل الاجتماعي.

3.3.2.4 يمنع على الموظف ارسال أي وثائق سرية خاصة بالمؤسسة الا بوجود تصريح من المسؤول وبشترط وجود الية تشفير واعدادات آمنة على خادم البريد الالكتروني.

3.3.2.5 لا يجوز استخدام أو استغلال هذه الخدمة لأغراض يمكن أن تتسبب في أي تهديد، أو ازعاج، أو اهانة لأي جهة، أو شخص من خارج أو داخل المؤسسة والذي قد يجعل المؤسسة هدف للرسائل التطفلية وغير الاخلاقية.

3.3.2.6 لا يجوز استخدام او استغلال هذه الخدمة للمراسلة باسم الجهة المستفيدة أو أحد أقسامها بدون اذن مصرح به.

3.3.2.7 لا يجوز استخدام أو استغلال هذه الخدمة لأرسال معلومات شخصية أو خاصة لا تتعلق بالعمل مثل كلمات المرور وارقام بطاقات الائتمان أو ارسال أي معلومات حساسة أو الدخول على حسابات الغير ومحاولة استخدامها بدون اذن مصرح به.

دولة فلسطين رئاسة الوزراء / الأمانة العامة

3.3.2.8 يمنع استخدام عنوان البريد الالكتروني الخاص بالمؤسسة لأغراض الدعاية والاعلانات التجارية ومواقع التواصل الاجتماعي أو أي مجموعات اخبارية كما يمنع استخدام البريد الالكتروني الشخصي للمراسلات التي تتعلق بالمؤسسة.

3.3.2.9 لا يجوز استخدام أو استغلال هذه الخدمة بطرق تعرض الشبكة الداخلية للخطر بفتح ثغرات أمنية في الشبكة أو غير ذلك.

3.3.2.10 لا يجوز نشر كلمة المرور الخاصة بأي حساب بريد الكتروني حكومي واطلاع الاخرين عليه ممن لا يملكون الحق بالاطلاع على هذه المعلومات.

3.3.2.11 يجب مراعاة المعايير الموضوعة عند انشاء حساب جديد لمستخدم جديد حسب ما يتم تزويد المخول، بما في ذلك استخدام كلمات مرور معقدة مكونة من **8** أحرف على الاقل وتحتوي على رموز واشارات واحرف ويتم تغييرها كل **3** أشهر.

3.3.2.12 اتباع اجراءات الامن والامان بالنسبة للأجهزة الالكترونية بما فيها الحواسيب والأجهزة الخلوية عند ربطها بالإيميل الحكومي بأن تكون خالية من الفايروسات وعدم الإرسال التلقائي لآلاف الرسائل، واخذ التدابير اللازمة لحماية البيانات الخاصة بالبريد في حال البيع والاستبدال أو الاتلاف.

3.3.2.13

3.3.2.14

3.3.2.15 يجب مراعاة عدم ارسال أكثر من **50** رسالة يوميا لكل حساب من حسابات البريد الالكتروني المخصص لأي مؤسسة حكومية منعا لتصنيف البريد الالكتروني الحكومي ضمن قوائم اللائحة السوداء للمواقع العالمية وهذا بشأنه يؤثر على الخدمة المقدمة لكافة المؤسسات الحكومية ويعرقل عملية ارسال واستلام الرسائل، وفي حال الحاجة لأكثر من ذلك يتم مراسلة مع مركز الحاسوب الحكومي.

3.3.2.16 يتيح البريد الالكتروني سعة تخزين مناسبة للاستخدام اليومي لكل بريد الكتروني **(3GB)** مع وجود مرونة عالية بالنسبة للمؤسسات التي تتطلب سعة تخزين أكبر يتم زيادتها حسب احتياج المؤسسة وبناء على طلبها.

3.3.2.17 تتحمل المؤسسة الحكومية المسؤولية الكاملة حول أي بريد الكتروني حكومي خاص بأحد موظفيها ومتابعة ووقف هذه الحسابات في حال انتهت خدمة الموظف او احيل للتقاعد، ولا يتحمل مركز الحاسوب الحكومي أي مسؤولية سوء استخدام مثل هذه الحسابات أو استخدامها في اغراض خاصة.

3.3.2.18 لمركز الحاسوب الحكومي الحق في إيقاف او إلغاء الخدمة عن أي مستخدم في حالة اساءة استخدام الخدمة أو الاخلال بالشروط المسبق ذكرها ويتم ذلك بعد التنويه بشكل رسمي لمرتين متتاليتين بضرورة الالتزام بشروط استخدام البريد الالكتروني ضمن سياسة مركز الحاسوب الحكومي وفي حال الاستمرار بالأخلال بالشروط فان مركز الحاسوب الحكومي غير مسؤول عن فقدان أي بيانات او رسائل عالية الاهمية تخص المستخدم.

17

3.3.2.19 عدد الحسابات المخصصة لكل مؤسسة حكومية هو **200** حساب عند بداية الاستضافة، ويمكن زيادة هذا العدد حسب طبيعة عمل المؤسسة بعد مراسلة مركز الحاسوب الحكومي بهذا الخصوص وتوضيح السبب والعدد المطلوب لزيادة الحسابات.

3.3.2.20 في حال حدوث خلل في احدى المجالات الخاصة بالبريد الالكتروني التابع لاي مؤسسة حكومية يتم الاتصال بالشخص المخول للمتابعة في المؤسسة وإبلاغه بالخلل، وعليه يجب حل المشكلة من طرفه خلال **10** ساعات وفي حال لم يتم حلها يقوم مركز الحاسوب الحكومي بإيقاف الخدمة عن الحساب المسبب لحدوث الخلل.

3.3.2.21 في حال حدوث خلل في إحدى المجالات الخاصة بالبريد الالكتروني التابع لاي مؤسسة حكومية يتم الاتصال بالشخص المخول للمتابعة في المؤسسة وابلاغه بالخلل، وعليه يجب حل المشكلة من طرفه خلال **72** ساعة وإذا لم يتم حلها يقوم مركز الحاسوب الحكومي بإيقاف الخدمة للنطاق المسبب لحدوث الخلل.

3.3.2.22 تتحمل المؤسسة المستفيدة من خدمة استضافة البريد الالكتروني بأرشفة الحسابات البريدية محلياً على نظام التخزين المركزي للمؤسسة وأجهزة المستخدمين.

3.3.2.23 يحظر على الموظف محاولة الدخول إلى أي حساب بريد الكتروني حكومي لموظف آخر وتحت طائلة المسؤولية.

3.3.2.24يجب على مستخدم البريد الالكتروني ابلاغ الجهات المختصة في مؤسسته/ها حال ورود اي ملف مرفق مشتبه به في الرسالة الالكترونية ويتحمل الموظف المسؤولية في حال فتح أو تشغيل المرفقات الموجودة في رسائل التصيد الالكتروني والرسائل المزعجة.

3.3.2.25 يقوم الحاسوب الحكومي بعمل نسخة احتياطية عن الحسابات البريدية المسجلة على الخادم بشكل يومي.

3.3.2.26 يلتزم الحاسوب الحكومي بصفته الجهة المستضيفة للبريد الحكومي باستخدام تقنيات وآليات الحماية الحديثة والمتقدمة للبريد الالكتروني وبما يشمل تحليل وتصفية الرسائل خصوصا رسائل التصيد الالكتروني والرسائل المزعجة على سبيل الذكر.

3.3.2.27 يلتزم الحاسوب الحكومي بإشعار المؤسسات المستفيدة بأي عمل فني يقوم به، وقد ينتج عنه تعطل الخدمة أو بطء في الخدمة.

18

3.3.3 استخدام الشبكات الداخلية

3.3.3.1 يجب أن يتم حماية جميع الأنظمة والمعدات وأجهزة الحاسوب التي تحتوي على معلومات أو تتعامل بالمعلومات الخاصة بالمؤسسة والمتصلة بالشبكة الداخلية بشكل دائم أو مؤقت بأنظمة التحكم بالنفاذ المعتمدة من قبل دائرة تقنية المعلومات والتي تعتمد على اسم المستخدم لتحديد الصلاحيات التي يملكها الموظف.

3.3.3.2 ينبغي فصل الشبكات الداخلية مع تحديد صلاحيات كل منها بشكل موثق.

3.3.3.3 حماية الشبكة من الفيروسات والبرامج الضارة واي تهديدات الكترونية للشبكة الداخلية.

3.3.3.4 استخدام جدار حماية لفصل الشبكات الداخلية عن الخارجية لحماية المستخدمين والاجهزة الموجودة داخل المؤسسة ويفضل استخدام جدار حماية اضافي منفصل للشبكة الخاصة بمركز البيانات على ان يكون من مزود اخر.

3.3.3.5 يجب على دائرة الشبكات تطبيق انظمة الحماية الخاصة بمنع ربط اي جهاز الكتروني خارجي (مثل جهاز الحاسوب المحمول) بالشبكة الداخلية او تغيير مواقع الأجهزة الحواسيب للموظفين. حيث يتم اغلاق منفذ الاتصال مع الشبكة وبشكل اوتوماتيكي من قبل النظام وتبليغ مسؤول الشبكة بالمحاولة لاتخاذ الاجراءات المناسبة بذات الخصوص

3.3.4 استخدام الشبكات الخارجية

3.3.4.1 يجب أن يتم حماية الشبكات والأنظمة بحيث يكون النفاذ إليها من الخارج محمي باستخدام أنظمة التحكم بالنفاذ للتحقق من هوية المستخدم والخدمات المسوح له النفاذ إليها.

3.3.4.2 يجب أن يتم استخدام الوسائل والآليات المعتمدة من قبل دائرة تقنية المعلومات للنفاذ للشبكات الخارجية المختلفة، أما بخصوص الاتصال بالمكاتب الفرعية للمؤسسات فيجب مراعاة تشفير البيانات المتناقلة.

3.3.5 استخدام الانترنت

3.3.5.1 يجب أن يكون استخدام الانترنت للقيام بمهام العمل.

3.3.5.2 يسمح بأن يستخدم الانترنت للأغراض البحثية والتعليمية الخاصة أو المتعلقة بالعمل.

3.3.5.3 يمنع نشر معلومات خاصة بالمؤسسة على شبكة الانترنت ما لم يتم الموافقة على ذلك من مدير أمن / مالك النظام الخاص بالمعلومات المراد نشرها ودائرة أمن المعلومات، وتقوم المؤسسة بمراقبة استخدام الانترنت للتأكد من الالتزام بسياسات أمن المعلومات وأن استخدامها يتم للقيام بمهام العمل.

3.3.5.4 ينبغي استخدام وصلات الانترنت الرسمية فقط، ومن غير المسموح لأحد أن يتصل بالأنترنت بأي وسيلة اخرى غير شبكة المؤسسة على أجهزة المؤسسة.

3.3.5.5 عند استخدام الانترنت لا يسمح لأي شخص أن يسيء أو يشوه سمعة او يلاحق او يضايق او يهدد اي شخص آخر او ينتهك الحقوق القانونية المحلية او الدولية.

3.3.5.6 لا يسمح لأي شخص بأن يرفع ملفات أو يرسل أو ينشر أو يوزع اية معلومات، أو مواد غير ملائمة، أو غير لائقة، أو فاحشة، أو مدنسة، أو منتهكة لحرمات، أو افترائية، أو غير قانونية، او محمية بحقوق النشر والطبع على الانترنت عند استخدامه لموارد المؤسسة.

3.3.5.7 لا يسمح لأي شخص زيارة أية موقع فاحشة أو مخلة بالآداب أو مصنفة ذات محتوى سيء او غير أخلاقي او ما شابه ذلك.

3.3.5.8 يمنع استخدام الانترنت الخاص بالمؤسسة لتصفح مواقع التواصل الاجتماعي الا بموافقة الادارة المختصة وفي حال السماح بذلك يتم اتباع سياسة استخدام الانترنت لضمان سرية وامن المعلومات والموارد الخاصة بالمؤسسة.

3.3.5.9 في حالة استخدام وسائل التواصل الاجتماعي للنشر والتعليق باسم المؤسسة ينبغي تغذية الموقع الرسمي من خلال شبكة المؤسسة فقط، ولا يجوز الوصول الى إدارة المحتوى من خارج المؤسسة.

3.3.5.10قد تطلب بعض المنشورات من الموظفين وضع ملاحظة على حساباتهم توضح أن ما ينشرونه يعبر فقط عن رأيهم الشخصي وليس رأي المؤسسة التي يعملون فيها.

3.3.5.11يقع على عاتق دائرة الشبكات أو دائرة أمن المعلومات متابعة جميع المنافذ واغلاق غير المستخدم منها.

3.3.6 حجز النطاقات الالكترونية

3.3.6.1 عند اختيار اسم النطاق، يجب أن يتكون من حروف باللغة الانجليزية (من "A" الى "Z") ومن "0" الى "9" بالإضافة الى الرمز "-"، شريطة أن يبدأ بحرف وألا ينتهي بالرمز "-"، ولا يتأثر اسم النطاق بكون الاحرف صغيرة أو كبيرة.

3.3.6.2 يحق لمقدم الطلب تقديم عدة مقترحات اسماء نطاقات على أن يكون لها علاقة باسم المؤسسة المعنية أو نشاطه ويتم اختيار الأنسب من وجهة نظر مركز الحاسوب الحكومي.

3.3.6.3 لا يسمح بتسجيل الأسماء التي تحتوي على كلمات غير لائقة أو تتنافى مع أنظمة دولة فلسطين.

3.3.6.4 يحق لمركز الحاسوب الحكومي بعدم تسجيل أي نطاق ضمن الأنظمة والقوانين المعمول بها.

3.3.6.5 لا يجوز استخدام أو استغلال هذه الخدمة في حال كان المستخدم ليس أحد موظفي الجهة المستفيدة.

3.3.6.6 لا يجوز استخدام أو استغلال هذه الخدمة لأغراض مخالفة أو تخريبية أو ما شابه ذلك.

3.3.6.7 لا يجوز استخدام أو استغلال هذه الخدمة لأغراض يمكن أن تتسبب في أي تهديد، أو ازعاج، أو مضايقة لأي شخص، أو جهة أو يكون فيه إهانة للآخرين.

3.3.6.8 لا يجوز استخدام أو استغلال هذه الخدمة لأغراض الدعاية والاعلانات التجارية.

3.3.6.9 لا يجوز استخدام أو استغلال هذه الخدمة بطريقة تعرض الشبكة الداخلية للخطر بفتح ثغرات أمنية في الشبكة أو غير ذلك.

3.3.7 استضافة المواقع الالكترونية

3.3.7.1 يحق لمركز الحاسوب الحكومي ايقاف الاستضافة في حال عدم تجاوب المؤسسة الحكومية وعدم تحديث التعليمات البرمجية الخاصة بهم، ويتم إيقاف الاستضافة بعد التنويه للمؤسسة الحكومية بشكل رسمي لمرتين متتاليتين من خلال الشخص المفوض بالمتابعة بناء على مهلة يتم تحديدها من قبل مركز الحاسوب الحكومي بناء على مدى خطورة الوضع

3.3.7.2 يحق لمركز الحاسوب الحكومي ايقاف الاستضافة فوراً في الحالات المصنفة بالخطيرة أو الخطيرة جداً، ثم التنويه للمؤسسة الحكومية بشكل رسمي لمرتين متتاليتين من خلال الشخص المفوض بالمتابعة بناء على مهلة يتم تحديدها من قبل مركز الحاسوب الحكومي بناء على مدى خطورة الوضع.

3.3.7.3 في حال عدم تجاوب الشخص المفوض في المؤسسة بعد 5 ايام عمل يتم ارسال كتاب رسمي موجه إلى الإدارة العليا بالمؤسسة بأعلامهم بذلك، في حال عدم تجاوب المؤسسة الحكومية لمدة شهر يتم إلغاء الاستضافة.

3.3.7.4 يلتزم مركز الحاسوب الحكومي بإعطاء المؤسسة الحكومية نسخة احتياطية للموقع بعد الغاء الاستضافة المذكورة اعلاه، ولا يلتزم مركز الحاسوب الحكومي بتوفير أي نسخة بعد انتهاء شهر من ايقاف الاستضافة.

3.3.7.5 يلتزم مركز الحاسوب الحكومي بتوفير نسخة احتياطية للموقع الالكتروني (يومية، اسبوعية، شهرية) عند طلبه وتسليمه النسخة كاملة.

3.3.7.6 في حال الصيانة الدورية وتحديث الخوادم يحق لمركز الحاسوب الحكومي ايقاف الخدمة عن جميع المواقع المستضافة لديه على ان تكون فترة الصيانة والتحديث في ايام العطل والمناسبات على ان تعود الخدمة بأقصى سرعة ممكنة، بعد التنسيق وابلاغ الشخص المفوض بالمتابعة، لذلك يجب على الشخص المفوض بمتابعة الاعلانات حول الموضوع من خلال البريد الالكتروني الذي زود المركز به.

3.3.7.7 في حال ارادت المؤسسة الحكومية تغيير الاستضافة لخوادم خارجية يقوم فريق العمل في مركز الحاسوب بالسماح للمؤسسة الحكومية مدة ثلاث ايام عمل لنقل ملفات الاستضافة ومن ثم يتم ايقاف الاستضافة، يلتزم مركز الحاسوب الحكومي بتوفير نسخ احتياطية لملفات المؤسسة لآخر نسخة من موقعهم ويتم بعد ذلك حذف الملفات نهائيا بعد شهر من تاريخ ايقاف الخمة.

3.3.7.8 في حال استنزاف موارد الخوادم بشكل كبير يتم ابلاغ الشخص المفوض بالمتابعة للعمل على حل المشكلة، في حال عدم الاستجابة من طرف المؤسسة الحكومية يتم ايقاف الخدمة عنها مؤقتا حفاظا على المصلحة العامة.

3.3.7.9 ان أي محاولة للتسلل الى الخوادم أو اختراق المواقع المستضافة من خلال موقع الجهة المستفيدة، يقوم مركز الحاسوب الحكومي بايقاف الموقع المسبب للمشكلة مؤقتا، والتواصل مع الجهة المستفيدة بشكل رسمي من خلال الرسائل على البريد الالكتروني المعتمد ومن خلال الاتصال الهاتفي بالشخص المخول بمتابعة الامور الفنية، في حال عدم الاستجابة والتعاون يتم ايقاف الخدمة.

3.3.7.10 على الجهة المستفيدة ان تقوم بعمل مسح شامل ودوري على محتويات موقعهم الالكتروني، وفي حال وجود ملفات ضارة بالموقع او ما يتعلق بالاختراق، أو التجسس، او أي برامج ضارة، او فيروسات، او مواد اباحية، او مخلة بالآداب العامة، فان المؤسسة الحكومية تتحمل الضرر الناتج والمسؤولية كاملة، تقوم الجهة المستفيدة بحذف جميع الملفات الضارة والتأكد من جميع الملفات الموجودة على حاسبهم.

3.3.7.11 على المؤسسة المستفيدة تحديث البرمجيات باستمرار سواء كانت برمجيات خاصة أو برمجيات جاهزة مثل ورد برس وغيرها.

3.3.7.12 منع الارسال الجماعي والاغراق البريدي بالقوائم البريدية وتتحمل المؤسسة المستفيدة من ذات الموقع المخالف الضرر الناتج ويغلق الموقع فورا بعد العام الشخص المفوض بالضرر.

3.3.7.13 يمنع استغلال الاستضافة المخصصة للجهة المستفيدة لأي اغراض شخصية.

3.3.7.14 يمنع منعا باتا استخدام الخادم لتنفيذ هجمات او استخدام الخادم للهجوم على خوادم او مواقع الكترونية او شبكات اخرى.

3.3.7.15 منع استخدام خادم الاستضافة من خلال لوحة التحكم الخاصة بكم من عمل نسخ احتياطية على نفس خادم الاستضافة.

3.3. استخدام الشبكات اللاسلكية

3.3.8.1 فصل الشبكة اللاسلكية بشكل كلي عن الشبكة الداخلية للمؤسسة.

3.3.8.2 لا يسمح للضيوف بالاتصال على الشبكة اللاسلكية الخاصة بالموظفين ويفضل وجود شبكة خاصة بالضيوف.

3.3.8.3 يفضل الدخول الى الشبكة اللاسلكية من خلال اسم مستخدم وكلمة مرور.

3.3.8.4 يجب تفعيل كلمة السر للدخول او الربط على الشبكات اللاسلكية.

3.3.8.5 يجب تغيير كلمة سر الشبكات بشكل دوري (3 أشهر على الأكثر).

3.3.8.6 يفضل تعطيل خاصية بث اسم الشبكة (SSID) للشبكة الداخلية الرسمية.

3.3.8.7 يجب تشفير الشبكات اللاسلكية باستخدام آخر إصدار بروتوكول التشفير.

3.3.8.8 يمنع استخدام الأجهزة الخاصة بالموظف على شبكة المؤسسة الا بعد الحصول على الموافقات اللازمة.

3.3.8.9 يمنع ازدواجية ربط جهاز الحاسوب على الشبكة الداخلية للمؤسسة والشبكة اللاسلكية في آن واحد مهما كانت الأسباب.

3.3.8.10 يمنع ربط الطابعات التي تملك خاصية الاتصال اللاسلكي من الاتصال بالشبكة اللاسلكية للمؤسسة مهما كانت الاسباب".

3.3.8.11 يمنع استخدام اي تقنية تحويل لخدمة الانترنت الداخلي الى خدمة الاتصال اللاسلكي (Hotspot).

3.3.9 وسائل التواصل الاجتماعي

3.3.9.1 يمنع استخدام الحسابات الشخصية على اجهزة وموارد تكنولوجيا المعلومات الخاصة بالمؤسسة.

3.3.9.2 يمنع استخدام وسائل التواصل الاجتماعي لأرسال وتبادل أي ملفات أو معلومات خاصة بعمل المؤسسة، ويعتبر البريد الالكتروني الحكومي الوسيلة الوحيدة والأمثل لتناقل هذه المعلومات والملفات.

3.3.9.3 يمنع نشر معلومات خاصة بالمؤسسة على مواقع التواصل الاجتماعي ما لم يتم الموافقة على ذلك من مدير أمن/مالك النظام الخاص بالمعلومات المراد نشرها ودائرة أمن المعلومات.

3.3.9.4 لا يسمح لأي شخص أن يقوم بنشر أو يوزع أو يرسل أية معلومات، أو مواد غير ملائمة، أو غير لائقة، أو فاحشة، أو مدنسة، أو منتهكة لحرمات، أو افترائية، أو غير قانونية على مواقع التواصل الاجتماعي عند استخدامه لموارد المؤسسة.

3.3.9.5 ينبغي على المؤسسة عقد ورشات عمل دورية يتم من خلالها شرح أساسيات الاستخدام الآمن لمواقع التواصل الاجتماعي والكيفية التي يمكنهم بها الاستفادة من هذه المواقع دون إلحاق الضرر بالمؤسسة.

3.3.9.6 يجب على المستخدم أخذ التدابير اللازمة للمحافظة على الأمن والسرية عند استخدام مواقع التواصل الاجتماعي مثل ضبط إعدادات الخصوصية، واختيار كلمة سر قوية، واعتماد خاصية التحقق الثنائي، ومراجعة شروط الخدمة الخاصة بكل موقع من مواقع التواصل الاجتماعي.

3.3.9.7 قد تطلب بعض المنشورات من الموظفين وضع ملاحظة على حساباتهم توضح أن ما ينشرونه يعبر فقط عن رأيهم الشخصي وليس رأي المؤسسة التي يعملون فيها.

3.3.9.8 ينبغي تغذية المواقع الرسمية من خلال شبكة المؤسسة فقط، ولا يجوز الوصول الى إدارة المحتوى من خارج المؤسسة.

23

3.3.9.9 ينبغي حصر استخدام وسائل التواصل الاجتماعي الخاصة بالمؤسسة بالإدارة العامة للعلاقات العامة والإعلام أو الادارة الموكلة بعملها، وعليه تقع المسؤولية بتوكيل مهام الأشخاص أو ما يتم نشره على هذه الإدارة.

3.3.9.10 يجب على الموظف التأكد من أن كافة المواقع الالكترونية الرسمية، والتي يقوم بتصفحها والتعامل معها عبر شبكة المؤسسة يتوافر فيها خاصية تشفير البيانات المتناقلة، وذلك من خلال التأكد من توافر شهادتيSSL، TLSوبرتوكول HTTPS إن كانت تتطلب ادخال بيانات خاصة أو حساسة مثل اسم المستخدم أو كلمة المرور أو أرقام بطاقات الائتمان وذلك لضمان تشفير البيانات خلال نقلها.

3.3.9.11 توثيق جميع الحسابات والصفحات الرسمية للمؤسسة.

4 سياسة حصر وادارة الاصول والبرمجيات

4.1 الهدف

توفير معلومات أساسية عن الأصول، البرمجيات والمعدات الموجودة في المؤسسة لتسهيل الحصول عليها وقت الحاجة.

4.2 النطاق

تطبق هذه السياسة على جميع الاصول والبرمجيات والمعدات المتوفرة في الوزارة او المؤسسة.

4.3 عناصر السياسة

4.3.1 حصر الاشخاص

4.3.1.1 ينبغي توفير المعلومات الأساسية حول كافة الموظفين العاملين في المؤسسة بشكل ثابت او مؤقت او اي طرف ثالث يتم التعاقد معه.

4.3.1.2 ينبغي توفير معلومات اتصال للتواصل مع الموظف.

4.3.1.3 يجب ان يتم تحديد الدائرة التشغيلية أو الوحدة التي يعمل بها الموظف لتسهيل التواصل مع الشخص البديل او المسؤول في حالة الحاجة او عدم القدرة على التواصل مع الشخص نفسه.

4.3.1.4 يجب تحديد المسؤول المباشر للموظف.

4.3.1.5 يمكن ان يتم طلب معلومات إضافية عن الموظف إذا اقتضت الحاجة لذلك.

4.3.1.6 ينبغي اعلام الموظف بالمعلومات التي يتم جمعها عنه والاهداف التي يتم جمع المعلومات لتحقيقها.

4.3.1.7 ينبغي ان يتم السماح للموظف بمراجعة المعلومات التي تم جمعها عنه وذلك لضمان دقتها وضمان عدم استخدامها بما يتعارض او يضر مصلحة الموظف.

4.3.1.8 ينبغي ان يتم تحديث هذه البيانات بشكل دوري لضمان سلامتها وصحتها.

4.3.2 حصر الأجهزة والمعدات

4.3.2.1 ينبغي تحديد نوع الجهاز المستخدم من حيث مواصفات المعدات المستخدمة في تجهيزه مثل نوع الرام والمعالج على سبيل المثال وليس الحصر.

4.3.2.2 ينبغي تحديد جميع المواصفات الفنية/البرمجية المستخدمة في اعدادات الجهاز مثل نظام التشغيل وعنوان الانترنت على سبيل المثال وليس الحصر.

4.3.2.3 تحديد الية اتصال الجهاز بالشبكة بشكل سلكي، لاسلكي او منع اتصاله نهائيا بالشبكة

4.3.2.4 تحديد الية اتصال الجهاز بالأنترنت مثل وصول كامل، محدود، اتصال من داخل المؤسسة الى الخارج او من خارج المؤسسة الى الداخل او منع كامل للاتصال بالأنترنت.

4.3.2.5 تحديد اهمية الجهاز المستخدم خلال عملية الحصر وذلك لتقييم الضرر المحتمل وقوعه على المؤسسة في حالة حدوث مشكلة عليه ويتم التقييم بناء على الشخص الذي يستخدم الجهاز ونوع البيانات التي يتم معالجتها او تخزينها عليه.

4.3.2.6 تحديد مالك الجهاز.

4.3.2.7 يحظر على أي من الموظفين غير المخولين إدخال أي معدات خاصة بالشبكة إلى داخل المؤسسة واستخدام أو ربط هذه المعدات والأجهزة الطرفية من روترات وموزعات انترنت ومقويات اشارة وغيرها على شبكة المؤسسة.

4.3.2.8 مكان تواجده جغرافيا (اسم المنطقة، خطوط الطول والعرض)

4.3.2.9 يحظر على أي من الموظفين فك، أو فصل، أو اعادة ضبط، أو اعادة تهيئة، أو برمجة لأي من معدات الشبكة وملحقاتها وأجهزتها الطرفية، وتتولى الدائرة المختصة فقط المسؤولية عن القيام بهذه الاجراءات.

4.3.2.10الدائرة أو الوحدة التشغيلية المتواجد فيها

4 حصر البرمجيات والتطبيقات

4.3.3.1 أسماء البرمجيات.

4.3.3.2 إصدارات البرمجيات.

4.3.3.3 مطور ومالك البرمجيات.

4.3.3.4 اصدار اخر تحديث تم تطبيقه للبرمجية.

4.3.3.5 الهدف من البرمجية المستخدمة.

4 اعتماد البرمجيات والأنظمة

4.3.4.1 يجب اعتماد البرمجيات والمعدات والأجهزة والأنظمة الجديدة أو التعديلات التي تتم عليها من قبل دائرة تكنولوجيا المعلومات ومسؤول أمن المعلومات قبل أن يتم استخدامها وذلك فيما يتعلق بتوافقها مع متطلبات واحتياجات أمن المعلومات في المؤسسة.

25

4.3.4.2 ينبغي توفير شهادة امن وامان للنظام او التطبيق الذي يتم شراؤه وذلك من قبل طرف ثالث على ان يشمل على سبيل المثال لا الحصر (تدقيق الشيفرة المصدرية، فحص إمكانية الاختراق، .....).

4.3.4.3 يحظر على الموظفين تنزيل و/أو تثبيت أي برمجية الا بعد موافقة مسؤول امن المعلومات او الدائرة التقنية في المؤسسة.

4.3.4.4 بعد الحصول على الموافقة اللازمة لتثبيت البرمجيات يتم تثبيتها فقط من خلال الدائرة التقنية/الدعم الفني أو الدائرة المتخصصة.

4.3.4.5 ينبغي حصر البرمجيات المستخدمة داخل المؤسسة بما يتوافق مع سياسة حصر البرمجيات والتطبيقات.

4.3. استخدام البرمجيات

4.3.5.1 تسمح المؤسسة باستخدام البرمجيات التي يتم بناؤها وتطويرها داخل المؤسسة والبرمجيات التي يتم الحصول عليها من الجهات الموثوقة لدى المؤسسة او البرمجيات التجارية التي تعتمدها المؤسسة وتقوم بشرائها او الحصول على رخصتها، ويمنع استخدام البرمجيات التي يتم الحصول عليها من شبكة الانترنت أو غيرها من المصادر الأخرى ما لم يتم فحصها واعتمادها من قبل دائرة تقنية/أمن المعلومات.

4.3.5.2 لا يسمح باستخدام البرامج المقرصنة او غير الشرعية في المؤسسة.

4.3.5.3 لا يسمح بتنصيب البرامج المرخصة والتي يتم شراؤها على أجهزة المؤسسة الا بموافقة المسؤول المباشر والدائرة المختصة ويتم ذلك من قبل دائرة تقنية المعلمات/الدعم الفني او الدائرة المختصة بالمؤسسة.

4.3.5.4 ينبغي فحص كافة البرمجيات والتطبيقات قبل البدء بالعمل بها.

4.3. نسخ البرمجيات

4.3.6.1 يمنع الموظفون من نسخ البرمجيات الخاصة بالمؤسسة على وسائط نقل المعلومات مثل الأقراص الليزرية، أو الأقراص المرنة، او ذاكرة فلاش، او أي وسيلة لحفظ للبيانات من الوسائط ويمنع استخدامها على أجهزة حاسوب غير مملوكة للمؤسسة أو تزويدها لأطراف خارجية (ما لم يحصل على موافقة مسؤوله المباشر) وفقط يسمح النسخ الاحتياطي للبرمجيات.

4.3. سياسة ادارة التراخيص والبرمجيات

4.3.7.1 ينبغي أن تكون جميع البرامج والنظم المستخدمة داخل المؤسسة مرخصة.

4.3.7.2 ينبغي تدقيق الرخص لكافة البرامج والنظم المستخدمة داخل المؤسسة عن طريق أخذ عينات عشوائية بشكل دوري. يجب أن تكون تراخيص البرمجيات وأنظمة التشغيل تحت عهدة إدارة تكنولوجيا المعلومات.

4.3.7.3 يجب الاحتفاظ بتراخيص جميع البرامج المستخدمة داخل إدارة تكنولوجيا المعلومات.

5 سياسة صلاحيات الوصول

5.1 الهدف

تنظيم وصول المستخدمين الى الموارد المعلوماتية في المؤسسة مع ضبط صلاحياتهم وحماية الموارد المعلوماتية من الوصول غير المصرح به.

5.2 النطاق

تطبق هذه السياسة على جميع موارد المؤسسة والموظفين والزوار او اي طرف ثالث.

5.3 عناصر السياسة

5.3.1 منح \ إلغاء الصلاحيات

5.3.1.1 تمتلك الدائرة المختصة الحق بإلغاء صلاحيات أي موظف بشكل كلي او جزئي ولفترة محدودة او غير محدودة بناء على تعليمات الوزير أو مسؤول المؤسسة أو رئيسها أو من ينوب عنهم في المنصب او في حال وقوع خلل قد يسبب ضرر لموارد المؤسسة على ان يتم ابلاغ المالك (الموظف) ومسؤوله المباشر ومسؤول امن المعلومات.

5.3.2 صلاحيات الاستخدام

5.3.2.1 يسمح للموظف استخدام المعلومات التي تمكنه من القيام بعمله على الأنظمة المختلفة وذلك من خلال اعتماد نظام طلب صلاحيات الاستخدام والموافقة عليه من قبل مسئوله المباشر ومدير أمن و/أو مالك النظام قبل أن يتم إعطاء صلاحيات استخدام للموظف، ويمنع الموظف من استخدام أو محاولة استخدام المعلومات أو الأنظمة التي لا يحتاجها في عمله أو استخدامها لغير غايات وأهداف العمل.

5.3.2.2 في حال تغيير الوضع الوظيفي للموظف من حيث الترقية، أو تغير مهام العمل، أو النقل، أو انتهاء عمله في المؤسسة أو غيره من الأسباب، يجب على مديره المباشر إبلاغ دائرة تقنية المعلومات وفني الأمن على النظام أو الأنظمة التي يستخدمها الموظف وبشكل خطي.

5.3.2.3 يفضل أن يحدد تاريخ انتهاء لكل الصلاحيات لا يتجاوز السنة من تاريخ إعطاء الصلاحية، ويتم تجديدها حسب الحاجة.

5.3.2.4 يجب توثيق جميع الصلاحيات خطياً وإلكترونياً لدى دائرة أمن المعلومات وان يتم توثيق التغير فيها.

5.3.2.5 الأمن هو مسؤولية الجميع، وينبغي على كل الموظفين إتباع سياسات الأمن القابلة للتطبيق على مجالات عملهم.

5.3.2.6 كل المعلومات المخزنة أو المرسلة تبقى ملك للمؤسسة ولها الحق في مراقبة وتدقيق تلك المعلومات مع مراعاة الضوابط والأصول التي تتضمن الخصوصية.

27

5.3.2.7 يتم التعامل مع جميع معلومات المؤسسة بسرية تامة، ويحظر نشر هذه المعلومات أو إرسالها لأي طرف إلا بعد الحصول على موافقة خطية من قبل الوزير أو مسؤول المؤسسة أو رئيسها أو من ينوب عنهم.

5.3.2.8 ينبغي أن تتم حماية كل المعلومات الحساسة المخزنة في أجهزة الحاسب الآلي المحمولة بكلمة سر مع توفير الأدوات اللازمة لحمايتها.

5.3.2.9 يجب أن تحتوي كل أجهزة الحاسب الحالي والاجهزة ذات الصلة على مضاد الفيروسات، ولن يسمح لأي موظف بأن يعطل أو يوقف محركات كشف الفيروسات تلك.

5.3.2.10 لا يسمح باستخدام أي نسخ من برامج غير مصرح بها وخاصة غير المرخصة.

5.3.2.11اعتماد سياسة منع تنزيل اي برامج على اجهزة المؤسسة من قبل الموظفين حيث يتم اغلاق هذه الصلاحية من خلال الخادم الرئيسي للمؤسسة وفي حال الرغبة في تنزيل واستخدام اي برنامج فلا بد ان يتم ذلك من قبل موظف دائرة الشبكات المخول وبعد اخذ الموافقات اللازمة على ان تكون نسخة البرنامج مرخصة

5.3.2.12 يمنع استخدام الشبكات الافتراضية من داخل المؤسسة "VPN" إلا إذا سمح بذلك خطيا بمنع منعا باتاً الفحص ومسح المنافذ الا إذا كان جزءاً من اختبار الاختراق الرسمي الذي تقوم به المؤسسة مع الأخذ بالتدابير الوقائية.

5.3.2.13لا ينبغي لأي برنامج يفحص امكانية الاصابة باختراقات أمنية أو أية برامج مماثلة أن يتواجد على أية أجهزة ويسمح باستخدام تلك البرمجيات والتطبيقات لأغراض التقييم من قبل الدائرة المختصة في دائرة أمن المعلومات وبموافقة خطية من رئيس المؤسسة ولوقت محدود.

5.3.2.14 مراعاة تحديث أنظمة التشغيل بشكل دوري ومستمر.

5.3.3 اسم المستخدم وكلمة المرور

5.3.3.1 يجب أن يتم إنشاء اسم مستخدم لكل موظف يتطلب عمله استخدام الأدوات او الخدمات الالكترونية.

5.3.3.2 يتم ربط صلاحيات الاستخدام للموظف باسم المستخدم الخاص به.

5.3.3.3 يتحمل الموظف المسؤولية الكاملة عن الأعمال التي تتم من خلال استخدام الحساب الخاص به.

5.3.3.4 يجب اعادة ضبط كلمات المرور التلقائية فور استلامها.

5.3.3.5 يجب على المستخدم اختيار كلمة مرور تتوافق مع سياسة أمن المعلومات والضوابط المحددة من قبل المؤسسة.

5.3.3.6 يجب ألا يقل طول كلمة المرور عن 14 خانة.

5.3.3.7 يجب ان تحتوي على أحرف كبيرة، وصغيرة، وأرقام، ورموز.

5.3.3.8 يفضل دمج مجموعة كلمات مع بعضها البعض، أو استخدام العبارات

28

5.3.3.9 يجب ان تختلف كلمة المرور الجديدة عن آخر 5 كلمات مرور سابقة على الاقل.

5.3.3.10 يجب عدم إتباع نمط معين في تغيير كلمة المرور.

5.3.3.11 يفضل استخدام التحقق الثنائي ان أمكن.

5.3.3.12 يجب تحديد فترة صلاحية لكلمة المرور على ان لا تزيد عن 3 أشهر ويتم تحديدها من قبل مالك النظام.

5.3.3.13 يجب ان يتم توفير آلية تخزين آمنة لكلمات المرور وذلك للوصول إليها في حالات الضرورة.

5.3.3.14 يمنع بشكل مطلق مشاركة اسم المستخدم وكلمة المرور الخاصة بالموظف أو إعطائها لشخص أخر.

5.3.3.15 لا يحق لأحد طلب كلمة المرور الخاصة بالموظف

5.3.3.16 إذا كان هناك حاجة لمشاركة الملفات بين أكثر من موظف فيجب استخدام تقنيات مشاركة الملفات المعتمدة من دائرة تقنية المعلومات وليس الاشتراك في استخدام كلمة المرور من قبل أكثر من موظف.

5.3.3.17 يحظر تخزين كلمات المرور بأي شكل من الأشكال سواء كان الكترونيا او ورقيا الا في حالة اتباع الية محددة مسبقاً من قبل ادارة المؤسسة.

5.3.3.18 ضرورة اشعار المستخدمين لتغيير كلمة المرور بوقت كافي قبل انتهاء صلاحية كلمة المرور.

5.3.3.19 على الموظف أن يختار كلمة مرور من الصعب أن يتوقعها غيره في حال لم يدعم النظام السياسات السابقة.

5.3.3.20يتم ايقاف كلمة المرور او تعطيل اسم المستخدم في حالة كان هناك سلوك مشتبه به او لا يتناسب مع سياسة امن المعلومات او قد يعرض موارد المؤسسة للخطر، على سبيل المثال وليس الحصر.

5.3.3.20.1 تكرار إدخال كلمة مرور أكثر من خمس محاولات.

5.3.3.20.2 استقالة أو توقف عمل أحد الموظفين أو أصحاب الطرف الثالث.

5.3.3.20.3 في حالة اكتشاف أي نوع من التهديد قد يسبب ضرر للمؤسسة.

5.3.3.20.4 ينطبق ذلك على الاجهزة المكتبية والخوادم.

5.3.4 العمل والاتصال عن بعد

5.3.4.1 يسمح للموظف القيام بالعمل عن بُعد وذلك بعد الحصول على موافقة مديره المباشر ومسؤول أمن المعلومات وذلك بناءً على مهام العمل المكلف بها، ويجب على الموظف الالتزام بسياسة أمن المعلومات المتعلقة بالعمل عن بُعد.

5.3.4.2 يوصى الأخذ بعين الاعتبار أنه في حال ضرورة عمل الموظف عن بعد أن يتم توفير جهاز حاسوب محمول من المؤسسة للموظف مطبق عليه سياسات الشبكة وأمن معلومات المؤسسة.

5.3.4.3 ينبغي رفض الاتصال عن بعد إذا كان الجهاز المستخدم غير مطابق للمواصفات الامنية للمؤسسة.

5.3.4.4 ينبغي أن يستخدم الاتصال عن بعد لأغراض العمل فقط مع ضرورة تشفير الاتصال ويكون فقط باستخدام ال " SSL VPN".

5.3.4.5 يعتبر الاتصال عن بعد امتداداً لشبكات المؤسسة وعليه فان جميع سياسات المؤسسة تطبق على جميع الاتصالات عن بعد.

5.3.4.6 ينبغي مراقبة واضافة سجل لجميع الاتصالات عن بعد.

5.3.4.7 في حالة تم وضع نظام لكشف التسلل ينبغي على النظام اصدار تنبيه للكشف عن خرق أمني.

5.3.4.8 أن يتم تزويد أجهزة الحاسوب المتصلة بالنظام عن بعد بجدار ناري شخصي وبرنامج لمكافحة الفيروسات الضارة على الأقل ويتم تفعيل هذه الضوابط الامنية في جميع الاوقات.

5.3.4.9 ألا يقوم المستخدمون بالدخول الى الانظمة الداخلية للمؤسسات من خلال أجهزة الحاسوب العامة.

6 سياسة ادارة المخاطر والحوادث

6.1 الهدف

تحديد الإجراءات المتبعة لإدارة وتقييم المخاطر والحوادث الأمنية والتعامل معها وتحديد الطرق الافضل لاحتوائها/معالجتها حال حدوثها.

6.2 النطاق

تطبق هذه السياسة على جميع موارد المؤسسة والموظفين والزوار او أي طرف ثالث.

6.3 عناصر السياسة

6.3.1 مراقبة الانظمة

6.3.1.1 تمتلك دائرة تكنولوجيا المعلومات ودائرة أمن المعلومات موافقة رسمية من إدارة المؤسسة تسمح لها بالمراقبة والفحص والبحث في أنظمة المعلومات في أي وقت كان شريطة اعلام المالك قبل البدء بعملية الفحص واعلام مسؤوله المباشر خطياً.

6.3.1.2 قد تتم هذه العملية بوجود الموظف أو غيابه وتشمل هذه الموافقة كافة أنظمة المعلومات المستخدمة في المؤسسة مثل البريد الالكتروني وأجهزة الحاسوب الشخصية والأقراص الصلبة وغيرها.

6.3.1.3 لا يتمتع الموظف بأية خصوصية في المعلومات على الأنظمة المستخدمة في المؤسسة لأن هذه الأنظمة مخصصة لأغراض العمل وليس للاستخدام الشخصي.

6.3.2 سجلات توثيق الحوادث

6.3.2.1 يجب ضبط كل جهاز/خادم في المؤسسة لتسجيل جميع الحوادث المتعلقة بنظام التشغيل، الحوادث الامنية او التطبيقات المثبتة عليه.

6.3.2.2 يجب عمل نسخ احتياطية لسجلات التوثيق عن طريق عمل خادم مخصص لتخزين الحوادث التي تحصل على الشبكة او الانظمة المستخدمة داخل المؤسسة Syslog server.

6.3.2.3 يجب الاحتفاظ بسجلات الحوادث على الخادم المخصص لسجلات الحوادث لمدة لا تقل عن سنة.

6.3.2.4 يتم طلب الوصول إلى سجلات الحوادث المتعلقة بالمؤسسة بعد الحصول على تصريح من مسؤول أمن المعلومات.

6.3.2.5 يجب مراجعة سجلات الحوادث بشكل دوري بالإضافة الى عمل مراجعة سنوية شاملة لسجلات الحوادث.

6.3.3 الاستجابة للحوادث وإدارتها

6.3.3.1 يجب التبليغ عن أحداث أمن المعلومات من خلال قنوات الإدارة المناسبة بأسرع وقت ممكن.

6.3.3.2 يجب أن يطلب من جميع الموظفين والمتعهدين ومستخدمي الطرف الثالث لأنظمة المعلومات والخدمات أن يلاحظوا ويبلغوا عن أي نقاط ضعف او أحداث تلاحظ أو يشك بها في الأنظمة أو الخدمات.

6.3.3.3 يجب ابلاغ مسؤول امن المعلومات بالحادث.

6.3.3.4 ينبغي توفر قاعدة بيانات عن جميع الحوادث لدى مسؤول أمن المعلومات.

6.3.3.5 يقوم مسؤول امن المعلومات مع مدير تكنولوجيا المعلومات:

6.3.3.5.1 تحليل الحادث واسبابه.

6.3.3.5.2 تقييم المخاطر.

6.3.3.5.3 وضع آلية للمعالجة.

6.3.3.5.4 المدة الزمنية المطلوبة للتعافي.

6.3.3.5.5 تنفيذ آليات المعالجة بأسرع وقت ممكن.

6.3.3.6 يقوم مسؤول امن المعلومات في المؤسسة بإبلاغ فريق فلسطين للاستجابة لطوارئ الحاسوب "بالسيرت" بالحادث ان كان مصدره خارج شبكة المؤسسة.

6.3.3.7 حال استدعت الحاجة الى مساعدة في الحادث يقوم مسؤول امن المعلومات بتصعيد البلاغ الى فريق فلسطين للاستجابة لطوارئ الحاسوب "بالسيرت".

6.3.3.8 يجب تحديد المسؤوليات والإجراءات الإدارية لضمان الاستجابة السريعة والفعالة في المؤسسة لأحداث أمن المعلومات.

6.3.3.9 ينبغي توثيق الحادث والمخاطر وآلية المعالجة والدروس المستفادة.

6.3.3.10 رفع التقرير النهائي الى الوزير أو مسؤول المؤسسة أو رئيسها أو من ينوب عنهم في المنصب وفريق فلسطين للاستجابة لطوارئ الحاسوب "بالسيرت".

6.3.3.11 ينبغي تضمين اجراءات ومسؤوليات إدارة حوادث أمن المعلومات في خطط الطوارئ وإدارة الازمات وخطط استمرارية العمل المعتمدة لدى المؤسسة.

6.3.4 اختبار الاختراق ومنع النشاطات المحظورة

6.3.4.1 يجب اجراء اختبار اختراق للمؤسسة بشكل دوري يتم تحديد المدة بناء على طبيعة المؤسسة وحاجتها على ان تكون مرة سنويا على الاقل

6.3.4.2 تقوم المؤسسة بتزويد الجهة المعنية بإجراء الاختبار بتصريح خطي.

6.3.4.3 إذا كان هناك حاجة للقيام باختبار الاختراق ضمن مهام العمل داخليا فيجب الحصول على موافقة خطيه مسبقة من مسؤول أمن المعلومات تسمح للموظف القيام بذلك، ويعتبر أي اختراق أو محاولة اختراق عمل غير قانوني وانتهاك جدي ومقصود للسياسات الداخلية للمؤسسة

6.3.4.4 فيما عدا ذلك يمنع اختراق أو محاولة اختراق أنظمة الحاسوب المستخدمة في المؤسسة في أي شكل من الأشكال، أو امتلاك، أو استخدام، أو نشر، أو التعامل بالأدوات والبرمجيات والأجهزة التي من الممكن أن تساعد أو تستخدم في اختراق أو محاولة اختراق أنظمة المعلومات وأنظمة الحماية المستخدمة في المؤسسة

6.3.4.5 يحظر التعامل او امتلاك الادوات الخاصة باختبار الاختراق او اجراء اي خطوة من خطوات اختبار الاختراق من قبل الموظفين أو أي جهة غير معنية بهذا الامر بالإضافة إلى الجهات المعنية لحين الحصول على التصريح.

6.3.5 النسخ الاحتياطي والاستعادة من الكوارث

6.3.5.1 تحديد جدول النسخ الاحتياطي: على أن يكون يومي، اسبوعي، شهري، سنوي تبعاً لما يقتضيه عمل المؤسسة.

6.3.5.2 تحديد نوع النسخ الاحتياطي.

6.3.5.3 تحديد عدد النسخ الاحتياطية.

6.3.5.4 تحديد نوع الأدوات المستخدمة في عملية النسخ.

6.3.5.5 التأكد من سلامة النسخ الاحتياطية.

6.3.5.6 تحديد أماكن حفظ النسخ الاحتياطية داخل المؤسسة وخارجها على ان تشمل موقعين متباعدين جغرافيا.

6.3.5.7 تحديد المدة الزمنية للبقاء على النسخ الاحتياطية قيد الحفظ.

6.3.5.8 يجب أن يتم تشفير بيانات النسخة الاحتياطية بالكامل.

6.3.6 اكتشاف الثغرات والابلاغ عنها

6.3.6.1 يتم الإبلاغ عن الثغرات المكتشفة سواء كان من خلال فحص مخصص او عن طريق الصدفة الى مسؤول امن المعلومات.

6.3.6.2 يقوم مسؤول امن المعلومات بتقييم الأثر على تلك الثغرة ويقدم توصياته للإدارة العليا في المؤسسة لاتخاذ الاجراء المناسب.

6.3.6.3 يجب الاحتفاظ بسجلات التوثيق اللازمة والخاصة بالثغرة على وسيطة تخزين غير متصلة بالشبكة فور اكتشاف الثغرة بعد اعلام وموافقة الإدارة العليا.

6.3.6.4 تقوم الإدارة العليا بالإيعاز لجهة الاختصاص في المؤسسة لتحليل الثغرة وتقديم حلول وتوصيات لإغلاقها.

33

6.3.6.5

7 سياسة الأمن المادي والبيئي

7.1 الهدف

ضمان منع الوصول غير المصرح به إلى المرافق والمعدات والموارد المعلوماتية المحوسبة وحمايتها من الحوادث الفيزيائية التي يمكن أن تسبب خسائر وأضرار للوزارة، ويشمل ذلك حمايتها من الحرائق والكوارث الطبيعية والسطو والتخريب، بالإضافة إلى حماية الأفراد والممتلكات من التلف أو الضرر.

7.2 النطاق

تنطبق هذه السياسة على جميع الاماكن/المباني او مقرات العمل التابعة للمؤسسة.

7.3 عناصر السياسة

7.3.1 الامن المادي

7.3.1.1 يجب أن يكون الباب الخاص لمركز البيانات مقاوم للحريق ويتحمل درجة الحرارة العالية والتي تنتج عن الحرائق.

7.3.1.2 التحكم بالدخول الى غرفة الخوادم للأشخاص المخولين فقط الكترونيا وماديا ضمن قائمة محددة مسبقاً ويتم توثيقه خطيا او الكترونيا

7.3.1.3 لا يسمح بأي زيارة عامة أو جولات لغرفة الخوادم.

7.3.1.4 ينبغي مرافقة الموردين وممثلي الطرف الثالث عند زيارتهم الغرفة ويتم توثيقه خطيا او الكترونيا.

7.3.1.5 ينبغي الحفاظ على تسجيل الدخول والخروج لغرفة الخوادم من قبل المستخدمين جميعاً ويتم توثيقه خطيا والكترونيا.

7.3.1.6 تركيب كاميرات مراقبة داخل وفي محيط مركز البيانات

7.3.1.7 ينبغي تواجد نظام مناسب خاص بإنذار واطفاء الحريق.

7.3.1.8 ينبغي تنفيذ وصيانة ادوات التحكم بالرطوبة وتركيب نظام انذار في حال زيادة الرطوبة عن المعدل المسموح به.

7.3.1.9 ينبغي تنفيذ وصيانة أدوات التحكم بالحرارة المناسبة وتركيب نظام انذار في حال زيادة أو نقص الحرارة عن المعدل المسموح به.

7.3.1.10 ينبغي تطوير اجراء طوارئ مناسب لغرفة الخوادم وأن تكون سهلة الوصول اليها، وكما ينبغي تدريب الأفراد حتى ينفذوا اجراء الطوارئ بشكل فعال، وينبغي التدقيق على جميع الاجراءات بشكل دوري.

7.3.1.11 لا يسمح الأكل أو الشرب أو التدخين في غرفة الخوادم.

7.3.1.12 ينبغي تركيب نظام مناسب لتصريف المياه ونظام انذار لرفض تسريب المياه في غرفة الخوادم.

7.3.1.13 ينبغي ربط مجمع توزيع الكهرباء لغرفة الخوادم ببطاريات تزويد طاقة مؤقتة لحين الحصول على الطاقة البديلة اللازمة.

7.3.1.14 ينبغي ربط مجمع توزيع الكهرباء لغرفة الخوادم بمولد الكهرباء حيث يعمل مباشرة فور انقطاع الكهرباء لضمان عدم انقطاع الكهرباء عن أجهزة الغرفة بما فيها اجهزة مراقبة وتكييف الغرفة.

7.3.2 الحماية من السرقة

7.3.2.1 يجب أن يتم حماية جميع أجهزة وأنظمة الحاسوب الموجودة في الأماكن المفتوحة في المؤسسة من السرقة وذلك باستخدام الوسائل المناسبة.

7.3.2.2 يجب استخدام الخزائن والقاعات المغلقة والوسائل الأخرى لحماية الخوادم الرئيسية وأجهزة ومعدات الشبكة من السرقة.

7.3.2.3 يحتاج نقل أو إخراج أجهزة الحاسوب ومعدات الشبكات من مكاتب المؤسسة موافقة خطية من إدارة المبنى وفني الأمن المسؤول عن هذه الأجهزة والمعدات.

7.3.2.4 يجب ان تطبق سياسة الامن المادي والبيئي على الأجهزة وأنظمة الحاسوب في عملية التناقل الفيزيائي.

7.3.3 النقل العادي والتخلص من المعلومات والوسائط

7.3.3.1 يجب أن تكون آلية نقل الوسائط التي يتم نقلها خارج موقع السيرفرات (مركز المعلومات) آمنة وموكلة لشخص مؤهل لذلك، وأن تكون البيانات مشفرة بحيث يتم تسجيل كل حركة نقل لتلك الوسائط.

7.3.3.2 يتم اتلاف أي جهاز أو وسيط الكتروني فقط من خلال لجنة يشكلها الوزير أو مسؤول المؤسسة أو رئيسها أو من ينوب عنهم.

7.3.3.3 يجب اعتماد إجراءات عمل للتخلص من الوسائط والمعلومات بشكل آمن وسليم عند انتهاء الحاجة لها وبعد انتهاء الدورة المستندية (Retention Period) التي تعتمدها المؤسسة وذلك باتباع الإجراءات الرسمية

7.3.3.4 يجب أن تعمل الإجراءات الرسمية للتخلص الآمن من الوسائل على الحد من خطر تسرب المعلومات الحساسة للأشخاص غير المصرح لهم.

7.3.3.5 يجب أن تتناسب إجراءات التخلص الآمن من الوسائط التي تحتوي معلومات حساسة مع درجة حساسية تلك المعلومات.

7.3.3.6 يمنع نقل أي من الموارد من موقع إلى آخر داخل المؤسسة أو من فروعها إلا بإذن خطي رسمي من خلال موظف تكنولوجيا المعلومات.

7.3.3.7 يمنع نقل أي من الموارد من موقع إلى خارج المؤسسة أو من فروعها إلا بإذن خطي رسمي من خلال موظف تكنولوجيا لمعلومات.

7.3.3.8 يمنع احضار أي أجهزة خارجية إلى المؤسسة واستخدامها بغير اذن خطي رسمي.

8 سياسة حماية المعدات والخوادم

8.1 الهدف

حماية البنية التحتية المعلوماتية للمؤسسات من هجمات اختراق البيانات، والتجسس ومحاولات السيطرة على الأجهزة والمعدات والخوادم عن بعد والتي يمكن أن تتم من خلال الأجهزة والمعدات الخاصة بالمؤسسات الحكومية.

8.2 النطاق

تنطبق هذه السياسة على جميع المعدات والأجهزة والخوادم التابعة للمؤسسات.

8.3 عناصر السياسة

8.3.1 الأجهزة المحمولة الخاصة بالمؤسسات

8.3.1.1 يحظر اخراج أجهزة الحاسوب المحمولة والتي تعود ملكيتها للمؤسسات إلى خارج المؤسسات الحكومية والعمل عليها إلا بوجود تصريح من المسؤول المباشر.

8.3.1.2 يقوم الموظف بتقديم طلب الى المسؤول المباشر يوضح أسباب الحاجة إلى استخدام الأجهزة المحمولة التي تعود ملكيتها للمؤسسات إذا اقتضت الحاجة لذلك.

8.3.1.3 ينبغي تشفير البيانات المخزنة على الأجهزة المحمولة عندما تكون البيانات مصنفة على أنها سرية أو سرية للغاية.

8.3.1.4 يجب الالتزام بسياسة كلمة المرور عند استخدام الأجهزة المحمولة.

8.3.1.5 يتم تهيئة الأجهزة المحمولة للسماح للحد الأدنى من الميزات والوظائف والخدمات اللازمة لتنفيذ متطلبات العمل.

8.3.1.6 ينبغي اتخاذ كافة الإجراءات اللازمة من أجل حماية أجهزة المؤسسات المحمولة، حيث يشمل ذلك البرامج المضادة للفيروسات وكافة الأدوات الخاصة بمنع الاختراقات وتسريب البيانات.

8.3.1.7 ينبغي تحميل برامج تعقب واستعادة الأجهزة.

8.3.1.8 في حالة فقد جهاز محمول يجب على المستخدم أن يخطر المسؤول المباشر على الفور بالحادث ومتابعته بتبليغ خطي في أقرب وقت ممكن

8.3.1.9 منع الوصول من الأجهزة المحمولة للأنظمة الحساسة وفي حال الحاجة لذلك تعطى صلاحية الوصول لفترة مؤقتة فقط، تحدد من قبل المسؤول المباشر.

8.3.2 الأجهزة المحمولة الخاصة بالموظف

8.3.2.1 يحظر إدخال أجهزة الحاسوب المحمولة والتي لا تعود ملكيتها للمؤسسات الحكومية اليها والعمل عليها إلا بوجود تصريح من المؤول المخول ومسؤول أمن المعلومات.

8.3.2.2 يقوم الموظف بتقديم طلب الى مسؤول أمن المعلومات يوضح أسباب الحاجة إلى استخدام الأجهزة المحمولة الشخصية التي لا تعود ملكيتها للمؤسسات الحكومية إذا اقتضت الحاجة لذلك ويقوم مسؤول امن المعلومات بفحصه.

8.3.2.3 منع الوصول من الأجهزة المحمولة للأنظمة الحساسة وفي حال الحاجة لذلك تعطى صلاحية الوصول لفترة مؤقتة فقط، تحدد من قبل المسؤول المباشر.

8.3.3 الهواتف النقالة

8.3.3.1 يعتمد تطبيق سياسة الهواتف النقالة على طبيعة عمل المؤسسة ووضعها الأمني.

8.3.3.2 ينبغي على المؤسسة تفعيل شبكة خاصة للزوار (Guest) لغايات اتصال هواتفهم المحمولة بالأنترنت.

8.3.3.3 يحظر على الموظف أو الزائر توصيل الهاتف المحمول على جهاز حاسوب.

8.3.3.4 يحظر ادخال الهواتف المحمولة على المؤسسات ذات الطابع الأمني الا بعد الحصول على موافقة خطية أو/ والكترونية من جهة الاختصاص.

8.3.3.5 يمنع تخزين أي بيانات خاصة بالعمل على الهاتف المحمول الخاص بالموظف.

8.3.3.6 يمنع تخزين أي بيانات خاصة بالموظف على الهواتف المحمولة التي تعود ملكيتها للمؤسسة.

8.3.3.7 يمنع استخدام كاميرا الهاتف المحمول لتصوير اي مرافق او مواقع حساسة او وثائق خاصة للمؤسسة ويشمل ذلك استخدام تقنية التسجيل الصوتي.

8.3.4 الخوادم

8.3.4.1 ينبغي وضع الخوادم في مكان آمن فيزيائيا.

8.3.4.2 توفير نسخة اخرى من كل خادم في مكان مختلف جغرافيا لغايات الاستعادة من الكوارث.

8.3.4.3 ايقاف وتعطيل الخدمات غير اللازمة على الخوادم.

8.3.4.4 يجب فصل شبكة الخوادم عن الشبكات الاخرى في الوزارة واستخدام جدار حماية مختلف في النوع/المزود عن جدار الحماية المستخدم للاتصال بالأنترنت.

8.3.4.5 ينبغي ألا تعرض شاشة دخول الخادم أية عبارات ترحيبية وإنما ينبغي أن يظهر تحذير "هذه شبكة خاصة"، يمنع أي دخول غير مخول به منعاً باتاً، إذا لم تكن مخولاً فعليك الخروج الآن، كل النشاطات مسجلة وكل منتهك سيعرض نفسه للمساءلة القانونية.

8.3.4.6 ينبغي حفظ جميع اعدادات الخوادم في مكان آمن ومعروف لدى المؤسسة.

8.3.4.7 ينبغي أن يكون لكل خادم توثيق خاص لإعداداته واصدار نظامه والتحديثات المثبتة واجراءات النسخ الاحتياطي واستعادته، وانتهاء مدة الدعم الفني.

8.3.4.8 ينبغي تقديم طلب تغيير (change request) عن طريق كتاب خطي عند محاولة إجراء أي تغيير على اعدادات الخادم موقع من قبل المسؤول المباشر ويتم تدقيق طلبات التغيير مع حالة الخادم بشكل دوري لضمان توثيق جميع التغيير.

8.3.4.9 ينبغي تنفيذ جميع سياسات ادارة التغيير بشكل صارم على الخوادم.

8.3.4.10 ينبغي تثبيت جميع تحديثات الأمن على الخوادم بعد التأكد من أنه ان يكون لها تأثير سلبي على التطبيقات التي تعمل فيها.

8.3.4.11 ينبغي تعطيل جميع حسابات الزوار والحسابات الافتراضية والحسابات المميزة ويتم اضافة المستخدمين الذين لديهم صلاحيات الى المجموعات الإدارية.

8.3.4.12عند طلب الادارة عن بعد للخوادم فينبغي استخدام قناة آمنة وفي هذه الحالة يكون تسجيل الدخول بمستخدم عادي ثم رفع الصلاحيات بعد تسجيل الدخول للنظام.

8.3.5 جدر الحماية

8.3.5.1 ينبغي وضع جدر الحماية في مكان آمن.

8.3.5.2 ينبغي حجب أي خدمة لم يسمح بها بشكل صريح على جدار الحماية ويتم ضبط جدار الحماية لإعطاء الوصول المطلوب بشكل محدود لصاحب الطلب/الخدمة مع تحديد كل من

- مصدر الاتصال
- مستقبل الاتصال.
- نوع الخدمة.
- رقم المنفذ الخاص بالخدمة.

8.3.5.3 ينبغي أن تمنع جدر الحماية جميع عناوين الشبكات غير الصالحة القادمة من الانترنت باستثناء القادمة من الشبكات الافتراضية الخاصة.

8.3.5.4 ينبغي ألا تسمح جدر الحماية ببث عناوين الشبكات.

8.3.5.5 ينبغي ألا يفعل بروتوكول ادارة شبكات البسيط "SNMP" غير المشفر على جدر الحماية حيث يمكن استخدام بروتوكول SNMPv3 بدلا منه.

8.3.5.6 ينبغي أن يعد جدار الحماية ليوقف هجمات الحرمان من الخدمة " DDOS Attack".

8.3.5.7 ينبغي على جدار الحماية أن يوقف هجمات انتحال عناوين الشبكات وهجمات الحزم المجزأة وغيرها من الهجمات التي تستحدث مستقبلاً.

8.3.5.8 ينبغي حفظ النسخ الاحتياطية عن ملفات الاعدادات لجدار الحماية في مكان آمن.

8.3.5.9 يجب على جدار الحماية اخفاء جميع عناوين الشبكات الداخلية عن العالم الخارجي.

8.3.5.10ينبغي على جدار الحماية بأن يصفي برامج "ActiveX" برامج الجافا بالكامل والتصفية على أساس نوع الملفات وامتدادها.

8.3.5.11ينبغي ان يتوفر في جدار الحماية نظام كشف/منع التطفل لضمان صد الهجمات المستقبلية من خلال تحليل اتصالات الشبكات ووضع قواعد خاصة.

8.3.6 قواعد البيانات

8.3.6.1 يجب تصنيف قواعد البيانات حسب حساسيتها.

8.3.6.2 يجب فصل قواعد البيانات عن تطبيقاتها لأغراض امنية.

8.3.6.3 يجب توفير بيئة حاضنة لقواعد البيانات التجريبية منفصلة تماماً عن الخوادم والشبكة التشغيلية.

8.3.6.4 مراجعة كل حسابات وطرق الوصول الى البيانات ومراقبتها بشكل دوري.

8.3.6.5 استخدام سياسة قوية لحماية اسم المستخدم وكلمة المرور على ان تشمل سياسة كلمة المرور العامة.

8.3.6.6 العمل على تقوية الخادم وقواعد البيانات بحسب المعايير العالمية والنشرات الخاصة بمزودي الأنظمة.

8.3.6.7 استخدام خيارات تشفير التي توفرها منتجات قاعدة البيانات لتوفير مبدأ الحماية على مراحل بما فيها جدار الحماية، مضاد الفيروس، مكتشف محاولات الاختراق وغيرها.

8.3.6.8 تصنيف البيانات الحساسة وتشفير البيانات الخاصة بها داخل قواعد البيانات.

8.3.6.9 تسجيل أي تعديلات للبيانات الحساسة (سواء من خلال قواعد البيانات بشكل مباشر، أو من خلال التطبيقات الإلكترونية).

8.3.6.10 حماية سجلات الحوادث بشكل مناسب من أي تعديلات (سواء من خلال قواعد البيانات بشكل مباشر، أو من خلال التطبيقات الإلكترونية).

8.3.7 الفيروسات والبرامج الضارة

8.3.7.1 يجب تركيب واستخدام برامج الحماية من الفيروسات والبرامج الضارة المعتمدة من دائرة تقنية المعلومات على جميع أجهزة الحاسوب والخوادم في المؤسسة، بحيث يتم تفعيل الحماية التلقائية وتفعيل التحديث التلقائي.

8.3.7.2 يجب تحديث قاعدة البيانات الخاصة بنظام الحماية من الفيروسات والبرامج الضارة من قبل موظف أمن المعلومات المسؤول وبشكل دوري لضمان ارفادها بآخر التحديثات العالمية

8.3.7.3 يجب أن يتم فحص الملفات والبرمجيات التي يتم الحصول عليها من أطراف خارجية قبل أن يتم استخدامها بأي شكل على أجهزة الحاسوب.

8.3.7.4 يحظر على الموظفين محاولة معالجة الفيروسات والبرامج الضارة والقضاء وبتم ذلك من خلال دائرة الدعم الفني في المؤسسة.

8.3.7.5 حال اشتباه الموظف باحتمال إصابة جهاز الحاسوب الذي يستخدمه بالفيروسات او البرامج الضارة، أو أن برنامج الحماية كشف أن جهاز الحاسوب مصاب بالفيروسات او البرامج الضارة فيجب على الموظف فوراً التوقف عن استخدام الجهاز وفصله عن جميع الشبكات المتصل بها والاتصال بدائرة دعم الفني.

8.3.7.6 يمنع استخدام وسائط نقل البيانات المصابة بالفيروسات والبرامج الضارة مثل أجهزة التخزين الخارجية وغيرها قبل أن يتم التخلص من الفيروسات والبرامج الضارة والتأكد من سلامتها.

8.3.7.7 على الدائرة المختصة في الوزارة بمعالجة الفيروسات والبرامج الضارة المحافظة على البيانات المخزنة على الجهاز وعدم الاضرار بها قدر الامكان وفي حال تعذر ذلك يجب اخذ نسخة احتياطية عن وحدة التخزين.

9 سياسة استخدام وأمن الحوسبة السحابية

تقسم خدمات الحوسبة السحابية إلى ثلاثة أقسام رئيسية:

- البرامج كخدمة(SaaS)
- المنصة كخدمة(PaaS)
- البنية التحتية كخدمة(IaaS)

عادةً ما يقوم مقدمو خدمات الحوسبة السحابية بتقديم لوحة تحكم يتم تشغيلها خلال المتصفح، لإدارة الحسابات الخاصة بهذه الخدمات، بالإضافة الى واجهة لبيئة عمل التطبيقات لتوفير طرق لإدارة موارد السحابة مما يتيح المرونة في التعامل وإدارة الخدمات، حيث تقسم التحديات الأمنية المتعلقة بالحوسبة السحابية الى قسمين:

- المصاعب والتحديات الأمنية التي تواجه مقدمي خدمة الحوسبة السحابية.
- المصاعب والتحديات الأمنية التي تواجه مستخدمي خدمة الحوسبة السحابية.

9.1 الهدف

ضمان أمن وسرية التطبيقات والموارد المعلوماتية المحوسبة المخزنة لدى طرف ثالث.

9.2 النطاق

تطبق هذه السياسة على جميع موارد المؤسسة والموظفين وأي طرف ثالث.

9.3 عناصر السياسة

9.3.1 السياسات التي يجب اتباعها من قبل المؤسسة.

9.3.1.1 ينبغي على ادارة المؤسسة توفير البنية التحتية اللازمة لاستضافة الخدمات وتخزين البيانات الخاصة بالعمل داخليا والابتعاد عن الخدمات السحابية المقدمة من الطرف الثالث.

9.3.1.2 في حالة عدم امكانية توفير البنية التحتية اللازمة يمكن الاتجاه لخدمات الطرف الثالث شريطة ان تتوافق الخدمة مع سياسة الحوسبة السحابية.

9.3.2 السياسات التي يجب اتباعها من قبل المستخدمين وموظفي المؤسسات

9.3.2.1 التأكد من الاتصال بأنه آمن.

9.3.2.2 تجنب استخدام الشبكات اللاسلكية المفتوحة.

9.3.2.3 تحديث المتصفح بشكل مستمر .

9.3.2.4 عدم حفظ كلمات السر لأي موقع.

9.3.2.5 مسح ملفات (cookies) باستمرار .

9.3.2.6 المصادقة:

- استخدام خاصية التحقق الثنائي .

- اختيار كلمة مرور قوية.
- تغيير كلمة المرور باستمرار.

9.3.2.7 استخدام برامج مكافحة الفايروسات وتحديثها باستمرار.

9.3.2.8 عمل نسخ احتياطية باستمرار.

9.3.2.9 تحديث أنظمة التشغيل والبرامج.

9.3.2.10استخدام الحوسبة السحابية المعتمدة من الحكومة.

9.3.3 السياسات التي يجب اتباعها من قبل مزودي الخدمة السحابية

9.3.3.1 ينبغي أن تكون البيانات محمية ومفصولة بين المستخدمين ويجب أن يتم تخزينها ونقلها بشكل آمن كما يجب أن تكون البيانات مشفرة ضمن أفضل تقنيات التشفير.

9.3.3.2 يجب أن تكون البيانات والانظمة والتطبيقات الخاصة بالمؤسسة متوافرة وقابلة للوصول بشكل منتظم ومتاحة طوال فترة الخدمة وبدون أي توقف.

9.3.3.3 ينبغي أن يضمن المزود السرية التامة للبيانات بكل أنواعها وعدم السماح بالوصول لها إلا للأشخاص المخولين من المؤسسة أو الدائرة المختصة.

9.3.3.4 على مزود الخدمة اعلام المؤسسة وبكتاب خطي رسمي بأي تعديل سيتم على الخدمة كنقل الاجهزة، او البرامج، او المنصة من موقع الى اخر او اجراء اي تحديثات عليها بما في ذلك تعطل الخدمة لأي سبب من الاسباب خارج عن ارادة المزود على ألا تزيد مدة توقف الخدمة عن 24 ساعة .*

9.3.3.5 ينبغي اعتماد نظام معلومات يهدف الى التحقق من هوية المستخدم. ينبغي من مزود الخدمة أن يضمن أن الاجهزة والمعدات آمنة بشكل كامل ولا يمكن الوصول اليها بأي شكل من الأشكال ومقيدة بنظام دخول متكامل وموثوق للرجوع اليها عند الحاجة وقد يكون جزء من نظام ادارة الهوية في حالة المستخدمين ذوي الامتيازات الخاصة.

9.3.3.6 يجب على مزود الخدمة أن يضمن أمن وسلامة التطبيقات والأنظمة المقدمة ضمن الخدمة من خلال تنفيذ الاختبارات وتطبيق السياسات والاجراءات ونظم الحماية متعددة الطبقات.

9.3.4 استخدام التخزين السحابية

9.3.4.1 ينبغي على المؤسسة توفير تخزين سحابي خاص لمشاركة الملفات الخاصة بالعمل.

9.3.4.2 يمنع استخدام اي خدمة تخزين سحابي غير الخدمة الموفرة من قبل المؤسسة.

9.3.4.3 يمنع تخزين اي ملفات شخصية على التخزين السحابية الخاص بالمؤسسة، حيث ان اي ملفات خاصة يتم رفعها تفقد خصوصيتها.

9.3.4.4 تشفير البيانات الحساسة في حالة رفع اي ملف يحتوي على معلومات حساسة خاصة بعمل المؤسسة.

10 الاتصال والتواصل

10.1.1.1 يقوم مسؤول أمن المعلومات بالإبلاغ فوراً عن الأحداث الأمنية والاختراقات لمركز فلسطين للاستجابة لطوارئ الحاسوب " بالسيرت" في حال كانت مصدر الهجمات او الاختراقات من خارج نطاق شبكة المؤسسة.

10.1.1.2 يرى مسؤول أمن المعلومات ضرورة ابلاغ مركز فلسطين للاستجابة لطوارئ الحاسوب "بالسيرت" من عدمه بالأحداث الأمنية والاختراقات في حال كانت مصدر الهجمات أو الاختراقات من داخل نطاق شبكة المؤسسة.

10.1.1.3 رفع تقارير في كلا الحالتين الى مركز فلسطين للاستجابة لطوارئ الحاسوب " بالسيرت".

10.1.1.4 يقوم مسؤول أمن المعلومات في المؤسسة بتلقي الاشعارات والتنبيهات الأمنية.

11 التعهد

وعليه أتعهد أنا الموظف / ة ..... صاحب التوقيع .....
بالالتزام بكافة البنود الواردة في الوثيقة أعلاه.

دولة فلسطين
رئاسة الوزراء / الأمانة العامة
Council of Ministers / Cabinet Secretariat
State of Palestine

42