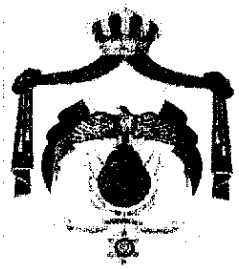

السياسات الوطنية لأمن وحماية المعلومات

إعـداد

اللجنة الوطنية الفنية لأمن وحماية المعلومات

التصـنيف

لاستخدام الدوائر الحكومية الأردنية

٢٠٠٨/١٠/٢٨

معتمدة من قبل: رئاسة الوزراء

Prepared by
The National Information Security Technical Committee (NISTC)

28 October 2008

Document Classification
Restricted for Jordanian Government Entities

Status
Approved by Prime Ministry

مراحل مراجعة الوثيقة

رقم النسخة	نوع الوثيقة	التاريخ	المؤلف	ملاحظات
1.0	مسودة	29 Oct 07		
1.1	مسودة	4 Nov 07		
2.0	مسودة	8 Nov 07		
3.0	مسودة	15 Nov 07		
3.1	مسودة	18 Nov 07		
4.0	مسودة	28 Nov 07		
4.1	مسودة	16 Dec 07		
4.2	مسودة	23 Dec 07		
4.3	مسودة	24 Dec 07		
5.0	معتمدة	28 Oct 08		

معتمدة من قبل

الاسم	المسمى الوظيفي	ملاحظات
رئاسة الوزراء		

المحتويات

الخلاصة

تعتبر المعلومات من أكثر الأشياء تأثيراً على المستوى الوطني والشخصي، لما لها من آثار عميقة وكبيرة في التطوير والتنمية في القطاعات المختلفة داخل المملكة، ولما لها من دور في تنظيم الحياة والعلاقات بين الأفراد والمؤسسات العامة والخاصة. ولهذا، فإنه يجب التعامل مع المعلومات بمستوىً عالٍ من الوعي، ودرجة عالية من المهنية من أجل أن تؤدي المعلومات دورها الفعال في تنمية المجتمع والاقتصاد المعرفي، وتحقيق الأمن والعدالة والحياة الكريمة لجميع المواطنين والمقيمين، وجميع فئات المجتمع أينما وجدوا.

من هنا، كان من الضروري وضع قواعد وأسس ومبادئ توضح آليات التعامل الصحيح والآمن للمعلومات داخل المؤسسات العامة من أجل المحافظة على هذه المعلومات من الضياع والتلف، والإفصاح عنها وتغييرها، وتحديد الأدوار والواجبات التي يجب أن يقوم بها المدراء والمختصون والموظفون من أجل تحقيق مستوى ملائم للأمن والحماية لهذه المعلومات وجميع الموارد المعلوماتية، وتوفيرها عند الحاجة إليها للأشخاص والجهات الذين لهم صلاحية الوصول إليها، اعتماداً على طبيعة العمل وخصوصية هذه المعلومات للأشخاص والجهات المسؤولة عنها.

تهدف هذه الوثيقة بمجملها إلى وضع أطر العمل، ووضع السياسات وتحديد الأدوار والمسؤوليات، وبيان الالتزام الأدنى المطلوب من جميع العاملين والمتعاملين مع الدوائر الحكومية لضمان أمن وحماية المعلومات التي يتعاملون معها على أي صورة، سواءً أكانت إلكترونية أو غير إلكترونية، أو مكتوبة أو مسموعة أو مرئية، أو تم تخزينها في ملفات أو أفلام أو صور أو وثائق أو أقراص أو أية وسائط تخزين مادية أو إلكترونية كانت، منذ إنشائها، مروراً بنقلها ومعالجتها وتخزينها، وانتهاءً بالتخلص منها بشكل آمن وصحيح.

تمثل هذه السياسة الحدود الدنيا للممارسات الخاصة بأمن وحماية المعلومات، ويمكن للدائرة أن تقوم برفع مستوى حدودها بحسب ما تقتضيه مصلحة العمل، ووضع التعليمات الخاصة بها لتطبيقها، وتطوير إجراءاتها الداخلية بحيث تكون منبثقة عن هذه السياسات والتعليمات، لتعزيز مستوى أمن وحماية المعلومات في الدائرة إلى أعلى مستوىً ممكن.

إن الالتزام الصحيح بالعمل بهذه السياسات يؤدي إلى تحقيق أعلى المستويات الممكنة لضمان أمن وحماية المعلومات في الحكومة، ويعزز الثقة بين المواطنين والحكومة بأن معلوماتهم وتعاملاتهم الإلكترونية وغير الإلكترونية ستكون بأمان ومعزل عن أية مخاوف أو تهديدات قد تؤثر على سلامتها وسريتها وإتاحيتها، كما يعزز الثقة المتبادلة بين الدوائر الحكومية المختلفة في تبادل المعلومات بشكل آمن، ويسهل من تطبيق آليات أمن وحماية المعلومات في الخدمات المشتركة والمتبادلة بينها لأنها جميعاً تلتزم بإطار العمل نفسه في أمن وحماية المعلومات.

لقد تم بذل مجهود كبير في وضع وتطوير هذه السياسات بعناية من أجل حمايتكم من المخاطر المتعلقة بأمن وحماية المعلومات، والتقليل ما أمكن من أية آثار سلبية قد تترتب على أي ممارسة أو فعل قد يفضي إلى الإضرار بالمعلومات والموارد المعلوماتية المملوكة للحكومة، مما يؤكد أن الالتزام الصحيح بالعمل بهذه السياسات يؤكد على منعة الأردن واستقراره من خلال منعة دوائره وموارده المعلوماتية.

شكر وامتنان

يتقدم برنامج الحكومة الإلكترونية الأردنية بعميق الشكر والامتنان إلى جميع الجهات التي ساهمت وشاركت بفاعلية في تطوير هذه السياسة من أجل تعزيز ضمان أمن وحماية المعلومات في المملكة، ونخص بالشكر الجهات المشاركة في اللجنة الوطنية الفنية لأمن وحماية المعلومات وهي:

١. وزارة الاتصالات وتكنولوجيا المعلومات.
٢. وزارة الداخلية.
٣. وزارة العدل.
٤. هيئة الأركان المشتركة.
٥. هيئة تنظيم قطاع الاتصالات.
٦. مديرية الأمن العام.
٧. دائرة المخابرات العامة.
٨. المركز الوطني للأمن وإدارة الأزمات.
٩. مركز تكنولوجيا المعلومات الوطني.
١٠. البنك المركزي الأردني.

قائمة المصطلحات

فيما يلي قائمة بالمصطلحات المستخدمة في هذه الوثيقة بأكملها، وأينما وردت فإنها تعني ما يقابلها في الجدول التالي:

المصطلح بالعربية	المصطلح بالإنجليزية	التعريف
ضوابط الدخول	*Access Control*	القواعد والآليات المستخدمة لتقييد الدخول إلى ملكيّة ما أو الوصول إلى موارد المعلومات والمناطق المختلفة ... الخ وللأشخاص المخولين فقط.
سجل الدخول	*Account*	مصطلح يصف غالباً معلومات المستخدم التي تسمح له بالدخول إلى الأنظمة المحوسبة، كما يمكن أن يشير أحياناً إلى عملية الحصول على حق الوصول من خلال الشبكات إلى الطابعات وأنظمة الأرشفة. وقد يعني أحياناً تطبيق امتيازات خاصة للتحكم بمستوى وصول المستخدم إلى موارد النظام بشكل فريد.
مدير النظام	*System Administrator*	الموظف المسؤول عن إدارة الشبكة أو النظام أو الخدمات الخاصة بالنظام
برامج مكافحة الفيروسات	*Antivirus Programs/Software*	برامج صممت خصّيصاً للكشف عن وجود الفيروسات (التي هي نوع من البرامج الخبيثة) والقضاء عليها، والحجر على الملفات التي تمت إصابتها بفيروسات لحين معالجتها منها لاحقاً.
التدقيق	*Audit*	هي عمليّة تقييم تحت ظروف ومعايير خاصة ومدروسة، والتي تهدف إلى معرفة مدى تقيد عمليّة أو نظام مع معايير أو سياسات معينة.
أدلة التدقيق	*Audit Trail*	مجموعة من الخطوات المتتابعة والمرتبة زمنياً ، والتي تقوم على ملف أو مجموعة من الملفات تسمح بتحديد عمليات المعالجة التي يتم القيام بها عن طريق نظام محوسب أو يدوي، كما يتم التحقق من صحة أية تعديلات أو تغييرات تتضمن المستخدمين الذين أنشئوا وأقروا هذه التعديلات أو التغييرات.
إثبات الهوية	*Authentication*	العملية التي يتم من خلالها التحقق والتأكد من هوية وبيانات المستخدم قبل إعطائه الصلاحية للوصول إلى موارد النظام، اعتماداً على ضوابط الدخول المستخدمة مثل كلمات المرور.
الصلاحية	*Authorization*	العملية التي يتم فيها التأكد من أن المعلومات التي يراد الدخول إليها أو العمليات التي يراد القيام بها أو الخدمات التي يراد الاستفادة منها أمر مسموح به وفقاً للحقوق والتراخيص الممنوحة للمستخدم فقط.
إعادة الإرسال بشكل آلي	*Auto Forward*	عملية تحويل الإرسال للرسالة الإلكترونيّة أو الملف من المستقبل إلى مستقبلين آخرين و بشكل آلي ومباشر.
الإتاحية	*Availability*	التأكد من أن أنظمة المعلومات سوف تبقى متوفرة وأن البيانات الضرورية متوفرة أو يمكن استرجاعها لاستخدامها عند الحاجة إليها.
النسخ الاحتياطي	*Backup*	عملية نسخ المعلومات على وسائط تخزين من أجل استرجاعها عند التلف أو الضياع أو الحاجة.
مستوى الأداء	*Baseline*	حالة من حالات النظام سواءً في الوضع الطبيعي أو في وقت معين، ويقاس بشكل عام عن طريق عمليات إحصائيّة حسابية متعددة تجرى على النظام في لحظة أو فترة معينة.
البيوس	*BIOS*	اختصار لجملة *Basic Input/Output System* أي نظام الإدخال والإخراج الأساسي، وهو برنامج يعمل قبل إقلاع نظام التشغيل، ويتحكم بتدفق

		المعلومات من وإلى نظام التشغيل والأجهزة الطرفية الملحقة مثل الطابعات، والأقراص الصلبة، ولوحة المفاتيح.
البلوتوث	***Bluetooth***	هي خاصيّة صناعيّة للشبكات الشخصيّة *Personal Area Networks (PANs)* ، والتي توفر طريقة لتبادل المعلومات الإلكترونيّة بين مجموعة من الأجهزة الإلكترونيّة المختلفة، وبشكل محمي، وباستخدام موجات راديوية قصيرة.
دراسة الجدوى	***Business Case***	دراسة الجدوى هي الأساس لأي مشروع، وهي تؤسس –مصطلحات التجارة والأعمال- الاحتياجات والتقييم والبدائل المقترحة لتحقيق هدف استراتيجي أو هدف متعلق بالعمل.
الرسائل التسلسلية	***Chain Email***	الرسائل الإلكترونيّة التي يقوم المستقبل لها بإرسالها لعدد آخر من المستقبلين ليقوموا بدورهم بالعمل نفسه بإرسالها من جديد إلى مع غيرهم ودواليك.
التغيير	***Change***	أي تعديل يتم إجراؤه على الأجهزة أو البرمجيات أو أي من مكوناتهما أو الإجراءات المعمول بها في الدائرة.
ضبط التغيير	***Change Control***	إدارة وضبط أي تغيير يحدث على الأنظمة المستخدمة ومكوناتها أو الأجهزة المختلفة ومكوناتها أو الإجراءات والتعليمات المتبعة في الدائرة.
عملية ضبط التغيير	***Change Control Process***	الإجراءات والعمليات المتبعة في الدائرة لطلب الموافقة على إجراء تغيير معين بعد رفع طلب خاص والموافقة عليه ثم مراجعته وأرشفته، بهدف المحافظة على أمان وكفاءة النظام، ولضمان حسن إدارة موارد الدوائر المختلفة والمحافظة عليها.
النص السري	***Cipher Text***	الرسالة السرية أو المعلومات بعد إجراء عملية التشفير عليها، والتي يتم إخفاء مضمونها.
المعلومات المصنفة	***Classified Information***	أي معلومات شفوية أو وثائق مكتوبة أو مطبوعة أو مختزلة أو مخزنة الكترونيا أو بأي طريقة أو مطبوعة على ورق مشمع أو ناسخ أو أشرطة تسجيل أو الصور الشمسية والأفلام أو المخططات أو الرسوم أو الخرائط أو ما يشابهها والمصنفة على أنها سرية أو وثائق محمية وفق أحكام التشريعات النافذة.
المكتب النظيف	***Clean Disk***	مبدأ من مبادئ الأمن والحماية ينص على عدم ترك أية معلومات أو وثائق على المكتب بشكل مكشوف للمحافظة على أمنها وسلامتها.
السرية	***Confidentiality***	التأكد من أنه يتم التعامل مع المعلومات من قبل الجهات المخولة بذلك فقط.
القنوات السرية	***Covert Channels***	الوسائل التي يمكن بوساطتها التواصل مع المعلومات بطريقة غير عادية أو متوقعة أو قابلة للكشف.
البيانات	***Data***	الحقائق الخام والأشكال التي ليس لها معنىً بذاتها، ويمكن توضيحها بالحروف والرموز والأرقام التي من الممكن أن تمثل الأشخاص أو الأشياء أو الأحداث.
كشف الأعطال	***Debugging***	عملية تتبع وإصلاح الأخطاء في البرامج الحاسوبية والأجهزة، وتقليلها من خلال إصلاحها أولاً بأول، حتى لا تؤثر على عمل هذه الأنظمة والأجهزة واستقرارها.
فك التشفير	***Decryption***	عملية استعادة المعلومات من شكل مبهم إلى شكل مقروء.
هجوم منع الخدمة	***Denial of Service Attack***	هجوم يهدف إلى محاولة القراصنة استهلاك موارد الخوادم المختلفة، لمنعها من تقديم الخدمة إلى الأشخاص المخولين بالاستفادة من هذه الخوادم، ومنها المحاولات التي تستهدف المواقع الإلكترونيّة لأهداف سياسية، أو لأنظمة ماليّة بهدف اختراق الأنظمة وتحقيق عائد مالي، الخ. وتتم باستخدام تقنيات وتطبيقات إلكترونيّة مختلفة.

الحاسوب المكتبي	***Desktop Computer***	جهاز الحاسوب الثابت الذي يصعب حمله والتنقل به عادة.
التحطيم	***Destruction***	عملية التخلص من المعلومات بطريقة فيزيائية مثل الحرق أو التكسير أو التهشيم .
دورة حياة التطوير	***Development Lifecycle***	المراحل التي تمر بها عملية تطوير المشاريع والتطبيقات والأنظمة بدءاً بمعرفة المتطلبات ،ثم بدراسة الجدوى ثم بالتحليل و دراسة الجدوى الاقتصادية ثم التصميم ثم البناء ثم الاختبار ثم التشغيل ثم الصيانة.
الكارثة	***Disaster***	أي فعل يقع على النظام يؤدي إلى إحداث ضرر بليغ بالخدمات والموارد المعلوماتية فيه
إتلاف	***Disposal***	عملية التخلص من المعلومات ومواردها بطريقة فيزيائية أو منطقية.
بقدر الحذر	***Due Care***	مبدأ في أمن وحماية المعلومات ينص على استخدام الحذر بطريقة كافية ومعقولة وحكيمة لحماية الموارد المعلوماتية في الدائرة.
بقدر الاستطاعة	***Due Diligence***	مبدأ في أمن وحماية المعلومات ينص على بذل أقصى الجهود الممكنة في حماية الموارد المعلوماتية في الدائرة لتطبيق مبدأ بقدر الحذر.
البريد الإلكتروني	***Email***	الخدمة التي تمكن توفيرها للمستخدمين من إنشاء وإرسال واستقبال وتخزين الرسائل الإلكترونيّة باستخدام أنظمة الاتصالات الإلكترونيّة.
سجل البريد الإلكتروني	***Email Account***	الحساب الذي يعطى للمستخدم ضمن نظام البريد الإلكتروني لتمكينه من إرسال واستقبال الرسائل والملفات الإلكترونيّة بشكل فريد.
الأرشفة	***Email Archiving***	عملية حفظ الرسائل والمرفقات القديمة بشكل منظم على وسائط تخزين في مكان معروف و آمن.
مرفقات البريد الإلكتروني	***Email Attachments***	الملفات التي ترفق مع الرسالة المرسلة بالبريد الإلكتروني.
التغييرات الطارئة	***Emergency Change***	التغييرات التي يتم إجراؤها بشكل غير مخطط له لوقوع حادث.
التشفير	***Encryption***	عملية تحويل المعلومات من شكل مقروء إلى شكل مبهم.
الدائرة	***Entity***	الوزارة أو الدائرة أو السلطة أو الهيئة أو أي مؤسسة عامة أو مؤسسة رسمية عامة أو الشركة التي تتولى إدارة مرفق عام
الاستئصال	***Expunge***	عملية مسح للمعلومات تهدف إلى إعادة وسائط التخزين إلى الحالة التي كانت عليها قبل نسخ المعلومات إليها، من خلال إحلال الملفات الموجودة على وسائط التخزين المختلفة بأصفار أو واحدات *0,1s*.
نظام الملفات	***File System***	هو عبارة عن نظام يختص بالطرق المعمول بها لتخزين وتنظيم الملفات الإلكترونيّة، بالإضافة إلى المعلومات الضرورية التي تحتويها هذه الأنظمة لتسهيل عملية العثور على هذه الملفات واسترجاعها.
الجدار الناري	***Firewall***	أجهزة أمن وحماية بنوعيها البرمجية والعتادية ***Hardware*** و ***Software*** تحدد وتقلل من القدرة على اختراق الأنظمة المعلوماتية أو الوصول إليها، من خلال منع وصول الخدمات غير المعتمدة بين الشبكات المعلوماتية، والسماح للخدمات المعتمدة فحسب بالوصول.
إعادة التهيئة	***Format***	العملية التي تهدف إلى تنظيم تخزين الملفات على وسيط التخزين.
إعادة الإرسال	***Forward***	عملية إعادة إرسال نسخة عن الرسالة أو الملف من المستقبل إلى مستقبلين آخرين.
سرقة الهوية	***Identity Theft***	جريمة تتضمن استعمال هوية الآخرين بطريقة غير قانونية أو غير شرعية.

الحادثة	*Incident*	أي فعل يقع على النظام أو الإجراء قد يكون له أثر سلبيٌ عليه
الفرد	*Individual*	شخص واحد.
المعلومات	*Information*	أي بيانات شفوية أو مكتوبة أو سجلات أو إحصاءات أو وثائق مكتوبة أو مصورة أو مسجلة أو مخزنة الكترونيا أو بأي طريقة وتقع تحت إدارة المسؤول أو ولايته.
الموارد المعلوماتية	*Information Assets*	أية معلومات أو ملفات (إلكترونية أو غير إلكترونية) أو أجهزة أو وسائط تخزين أو تسهيلات أو أشخاص لهم علاقة بعملية تبادل المعلومات ومعالجتها.
تصنيف المعلومات	*Information Classification*	عملية إناطة مستوى الحساسية المناسب للمعلومات التي يتم إنشاؤها أو تغييرها أو نقلها أو تعديلها أو حفظها على أية وسائل كانت وبأية تقنيات ممكنة، من أجل تحديد المستوى اللازم لحمايتها والتحكم بها وبالوصول إليها بشكل آمن.
مؤتمن المعلومات	*Information Custodian*	الشخص المسؤول عن متابعة وتطبيق وسائل الأمن والحماية المناسبة لحماية الممتلكات المعلوماتية في الدائرة، حسب مستوى التصنيف الذي يقره مسؤول المعلومات.
تداول المعلومات	*Information Handling*	عملية معالجة ونقل المعلومات على أية وسائط كانت.
منشئ المعلومات أو مسؤول المعلومات	*Information Owner*	الشخص المسؤول عن إنشاء أو المبادرة في إنشاء أو حفظ المعلومات، ويكون عادة الشخص المسؤول عن الدائرة التي قامت بإنشاء هذه المعلومات.
أمن المعلومات	*Information Security*	هي عملية حماية سرية وسلامة وإتاحية الموارد المعلوماتية.
سياسة أمن وحماية المعلومات	*Information Security Policy*	وثيقة معتمدة تقرها الإدارة العليا للدائرة توضح وتحدد أدوار العاملين فيها في كيفية التعامل مع الموارد المعلوماتية للدائرة بطريقة آمنة وصحيحة.
السلامة	*Integrity*	التحقق من أن المعلومات التي يتم التعامل معها لم يطرأ عليها زيادة أو نقص أو تغيير بشكل غير مرخص.
أنظمة كشف ومنع التطفل والاختراق	*Intrusion Detection and Prevention Systems IDS/IPS*	أنظمة برمجية تعمل على مراقبة نشاط النظام أو الشبكة المعلوماتية باستخدام تقنيات مختلفة، ومن ثم تقوم بالكشف عن أية هجمات على الشبكة وربما منعها.
الآيزو ١٧٧٩٩	*ISO 17799*	في الأصل كان معياراً بريطانياً لأمن وحماية المعلومات نشر عام ١٩٩٩ من قسمين: القسم الأول: ميثاق الممارسة لإدارة أمن وحماية المعلومات، والقسم الثاني يحدد الاحتياجات اللازمة لتطبيق أمن وحماية المعلومات بالتوافق مع ميثاق الممارسة السابق. وقد تم تحويله إلى الآيزو١٧٧٩٩ *ISO/IEC 27002:2005* في عام ٢٠٠٧.
الوسم	*Labeling*	العملية التي تهدف إلى بيان مستوى تصنيف المعلومات من أجل التعامل معها بشكل آمن وصحيح.
الحاسوب المحمول	*Laptop*	اسم عام لحاسوب شخصي قابل للحمل والتنقل يتضمن شاشة ويتم تزويده بالطاقة الكهربائية عن طريقة بطارية مرافقة قابلة للشحن.
الأمن الطبقي	*Layered Security*	استخدام عدة ضوابط دخول بشكل متسلسل من أجل توفير الدرجة القصوى للأمان.
الامتيازات الدنيا أو الأقل	*Least Privilege Principle*	مبدأ في أمن وحماية المعلومات ينص على أنه يجب إعطاء المستخدمين أقل عدد ممكن من الامتيازات والصلاحيات اللازمة لإنجاز العمل المطلوب حسب الوصف الوظيفي.
الشبكة المحلية	*Local Area Network (LAN)*	شبكة اتصالات خاصة تغطي منطقة جغرافية صغيرة نسبياً، وتتم إدارتها من خلالها في مكان واحد، ولها سرعات عالية، أقل عرضة للأخطاء من الشبكات الأخرى، وهي

		والتي تربط الأجهزة الإلكترونيّة معاً داخل منطقة محدودة كبناية أو ما شابه.
ملفات تسجيل الحركات	***Log Files***	الملفات التي تقوم الأنظمة الالكترونية فيها بتسجيل أحداث معينة، مثل عمليّة قدوم بريد إلكتروني (في خادم بريد إلكتروني)، أو عملية التحقق من كلمات الدخول، التي تحدث في النظام – سواءً أكانت جهاز حاسوب أو شبكة أو قاعدة بيانات- وبشكل آلي من أجل المقدرة على التدقيق عبر تتبع الحالات التي تمر بها هذه الأنظمة، بالإضافة إلى عمليّة التدقيق على عملها وبشكل خارجي.
القنابل المنطقية	***Logical Bombs***	برامج خبيثة تتم إضافتها إلى البرامج المختلفة، للقيام بعمل غير صحيح، عند تحقق شرط معين أو تعمل عند وقوع حدث أو عند تاريخ معين.
الصيانة	***Maintenance***	تعديل مستمر على النظام أو التطبيق لإصلاح الأخطاء والمشاكل التي يمكن أن تحدث فيه أولاً بأول، وبالتالي تحسين الأداء والكفاءة لهما، ليوائم المتطلبات المتجددة للدائرة.
البرامج الخبيثة	***Malware***	البرامج التي تصمم وتبنى من أجل اختراق أجهزة وملفات المستخدم من خلال التسلل إلى الأنظمة الإلكترونيّة وتخريبها بغير إرادة مالكي هذه الأجهزة أو مشغليها، من أجل تحقيق أهداف تخص الجهات التي صممتها.
رسالة التحقق	***Message Authentication***	معلومات مختصرة يتم استخدمها للتثبت من صحة وسلامة الرسائل.
المعرفة على قدر الحاجة	***Need-to-know, Need-to-do***	مبدأ في أمن وحماية المعلومات ينص على أنه يسمح للمستخدم بالوصول إلى المعلومات بالقدر الذي يحتاج إليه لأداء عمله فقط.
اتفاقية عدم الإفصاح عن المعلومات	***Non Disclosure Agreement (NDA)***	وثيقة قانونية تلزم الأطراف الموقعين عليها بالمحافظة على سرية الأفكار والتصاميم والخطط والمفاهيم التي تعتبر حساسة، وعدم الإفصاح عنها أو استخدامها أو إساءة استغلالها بدون إذن خطي ومكتوب، ويتم ملاحقة منتهكيها عن طريق القضاء.
التعاقد الخارجي	***Outsourcing***	الاستعانة بمزود خارجي أو تفويضه لتوفير خدمة معينة.
كلمة المرور	***Password***	طريقة تحقق تستخدم للتحكم بالدخول إلى الموارد المختلفة ، وهي تتكون من سلسلة سرية من الرموز معروفة في النظام يدخلها المستخدم من أجل إثبات هويته للنظام.
لوحة التوزيع	***Patch Panel***	لوحة مرفوعة على رفوف تستخدم لربط نهايات الأسلاك ضمن مبنى الدوائر ، مع أجهزة الشبكات الداخلية.
الإصلاحات	***Patches***	مجموعة من التحديثات التي يقوم صانع البرنامج لتقوية الأنظمة من الناحية الأمنية نظراً لوجود إمكانية اختراق أمني ويمكن تنزيلها عادة عبر الإنترنت من مواقع الشركات المزودة لهذه الأنظمة بشكل أوتوماتيكي أو يدوي لحين تجهيز نسخة محدثة كاملة فيما بعد.
الأمن الماديّ	***Physical Security***	معايير و إجراءات الحماية التي تراقب أو تحدد الدخول إلى أي مرفق، أو مورد ، أو معلومات مخزنة على وسائط فيزيائية بدون صلاحية ، أو لمنع التماس المباشر مع الموارد المعلوماتية والأنظمة ، مثل المباني وخزائن الملفات والأجهزة المكتبية والخادمة والمحمولة والمعدات...الخ.
النص المقروء	***Plain Text***	النص الأصلي المقروء قبل إجراء عملية التشفير.
حاسوب الجيب	***Pocket PC***	حاسوب محمول صغيرة بحجم اليد، إلى درجة أنه يمكن حمله في الجيب يعمل على نظام تشغيل متنقل خاص به، وله قدرات أجهزة الحاسوب الحديثة.
الامتيازات	***Privileges***	مستوى الصلاحيات أو السلطات التي تعطى للمستخدم داخل النظام لتحديد إمكانية القيام بأي عمل.

البروكسي	***Proxy***	جهاز أو تطبيق خادم يقوم مقام المستخدمين عند الربط بالإنترنت، عن طريق إرسال طلبات المستخدمين لمواقع الإنترنت، ومن ثم استقبال المعلومات المطلوبة للمستخدمين مرة أخرى ، وتخزينها، لاستعمالها عند طلبها لمستخدمين آخرين، وبالتالي تسريع عملية استرجاع الصفحات الإلكترونيّة، بالإضافة إلى إمكانية فلترة المواقع غير المرغوب بها.
الاسترجاع / الاسترداد	***Restore / Recovery***	عملية إعادة المعلومات المخزنة على وسائط النسخ الاحتياطي عند تلف أو فقدان المعلومات الأصلية أو الحاجة إليها بعد مدة من الزمن.
التغييرات المجدولة	***Scheduled Change***	التغييرات التي يتم إجراؤها بعد رفع طلب ثم مراجعته ثم الموافقة عليه من الجهة المخولة بشكل مسبق.
الجدولة	***Scheduling***	التخطيط لعملية معينة على فترات زمنية معينة.
المسح	***Screening***	عملية تهدف إلى التحقق من الخلفية الأمنية للشخص.
الفصل بين المهام	***Separation of Duties***	مبدأ في أمن وحماية المعلومات ينص على الفصل بين وظائف وصلاحيات المستخدمين في الوصول إلى المعلومات ومواردها وعدم إعطاء صلاحيات مطلقة للمستخدم.
اتفاقية مستوى الخدمة	***Service Level Agreement (SLA)***	اتفاقية بين الدائرة والجهة المزودة للخدمة، لضمان توفير مدىً مناسب من الدعم للخدمات اعتماداً على معايير دنيا متفق عليها مسبقا، ويتم فيها تحديد العقوبات المترتبة في حال الإخلال بهذه الاتفاقية.
مزود الخدمات	***Service Provider***	أي طرف له القدرة على تزويد خدمة معينة أو أكثر، مثل خدمة الإنترنت، الخ.
اختلاس النظر	***Shoulder Surfing***	هي عملية المشاهدة المباشرة من قبل أي شخص غير مخوّل لما هو مكتوب أو معروض على شاشات الحاسوب، وتتم بالعادة في الأماكن المزدحمة، مثل شاشات المطارات.
البرمجية المصدرية	***Source Code***	البرنامج الأصلي الذي قام المبرمج بكتابته باستخدام سلسلة من الجمل أو العبارات المكتوبة بإحدى لغات البرمجة المتعارف عليها. قبل أن تتم ترجمته إلى لغة الآلة.
المحتوى الدعائي	***Spam***	المحتوى الدعائي غير المرغوب فيه والذي يصل إلى المستخدم عادة عن طريق البريد الإلكتروني
البرامج التجسسية	***Spyware***	برامج خبيثة تنزل بشكل سري على أجهزة المستخدمين، لتختلس المعلومات الخاصة عن المستخدم وكيفية تفاعله مع الجهاز، و تهدف إلى جمع المعلومات الشخصية عن المستخدم.
المتعاملون مع	***Stakeholders***	جميع الأشخاص والجهات التي تتعامل مع الدائرة وتنتفع من خدماتها، مثل المواطنين، والطلاب، والدوائر الأخرى ذات العلاقة والموظفين...الخ.
كلمة المرور الفعّالة	***Strong Password***	كلمة المرور التي يسهل تذكرها من قبل المستخدم، ويصعب على الآخرين تخمينها
برمجية طروادة	***Trojan Code***	شيفرة خبيثة يقوم بكتابتها مبرمج داخل برنامج أو نظام ما تبدو كأنها تقوم بعمل مفيد، بينما تعمل في الحقيقة للقيام بعمل غير شرعي، وغير الهدف الذي تدعي عمله.
أحصنة طروادة	***Trojan Horses***	برامج خبيثة تظهر عملها لمهام محددة ، ولكنها بالواقع تقوم بأعمال غير الأعمال المسندة إليها، وتعمل عادة تحت غطاء برامج معروفة ومعتمدة.
ترقية (تحديث وتطوير)	***Upgrade***	عملية إحلال نسخة جديدة لبرنامج أو جهاز بدلاً من طبعة أقدم ، بحيث تحتوي هذه النسخة على تحسينات من النواحي الوظيفية للبرنامج أو الجهاز، وتعمل على تحسين مستوى الأداء والفاعلية، كما وأنها في حالة البرامج تزيد من الخصائص والواجهات والعمليات التي يمكن عملها.

اسم المستخدم	***Username***	اسم سجل الدخول الإلكتروني إلى نظام ما.
الفيروسات	***Viruses***	برامج خبيثة تقوم بنسخ نفسها على أجهزة المستخدمين ،من غير معرفتهم، وتسعى إلى إحداث خلل أو تدمير في ملفات أو جهاز المستخدم.
الشبكة واسعة النطاق	***Wide Area Network (WAN)***	الشبكة المعلوماتية التي تربط دائرتين فأكثر، و تغطي مساحات واسعة جغرافياً.
الواي-فاي	***WiFi***	تقنية لاسلكية حديثة تستخدم للربط مع الشبكات المحلية اللاسلكية.لربط المستخدمين المتنقلين مع الشبكة الداخلية.
الديدان	***Worms***	برامج خبيثة تنتقل غالباً عبر الشبكات والبريد الإلكتروني وتتناسخ بشكل آلي، على نفس الجهاز، لتعاود الانتشار عبر الشبكات ، وتؤثر على الموارد الخاصة بالأجهزة مثل الذاكرة، وسرعة الجهاز، وسرعة الشبكة ، الخ.

المقدمة

تعد السياسات الوطنية لأمن وحماية المعلومات خطوطاً أساسيةً توضح أطر العمل، وتحدد الأدوار والمسؤوليات، وتبين الممارسات الفضلى والالتزام الأدنى المطلوب مراعاته والعمل به من قبل العاملين والمتعاملين مع الدوائر الحكومية - على اختلاف درجاتهم وفئاتهم ومناصبهم- من أجل تحقيق أمن وسلامة وإتاحية المعلومات التي يتم تداولها بين الدوائر الحكومية والمواطنين والمؤسسات العامة والخاصة على حد سواء.

تشمل السياسات الوطنية لأمن وحماية المعلومات سبع عشرة سياسة، يعتمد أكثرها على البعض الآخر، وهي:

١. سياسة حساسية وتصنيف المعلومات.
٢. سياسة الاستعمال المقبول.
٣. سياسة ضبط التغيير.
٤. ميثاق السلوك الخاص بأمن المعلومات.
٥. سياسة التدقيق الخاص بأمن المعلومات.
٦. سياسة الأمن المادي.
٧. سياسة أمن الموظفين.
٨. سياسة الحاسوب المكتبي.
٩. سياسة الأجهزة المحمولة.
١٠. سياسة كلمات المرور.
١١. سياسة مكافحة الفيروسات والبرامج الخبيثة.
١٢. سياسة البريد الإلكتروني.
١٣. سياسة النسخ الاحتياطي.
١٤. سياسة أمن الشبكات.
١٥. سياسة تطوير وصيانة الأنظمة.
١٦. سياسة التعاقد الخارجي.
١٧. سياسة التشفير.

وكل سياسة من هذه السياسات تقسم إلى ثلاثة موضوعات رئيسية:

١. الهدف: ويوضح الأهداف الرئيسة التي ترمي كل سياسة إلى تحقيقها.
٢. المجال: ويحدد طبيعة الأشخاص والأشياء والموارد المعلوماتية المشمولة بكل سياسة على حدة.
٣. تفاصيل السياسة: وتوضح بإسهاب الأدوار والواجبات المناطة بكل من الدائرة وموظفيها المشمولين بمجال السياسة، من أجل تحقيق الهدف المنشود منها.

كما توضح هذه السياسات كيفية ارتباط بعضها ببعض حسبما تقتضيه الحاجة، كما توضح للقارئ بعض ارتباط هذه السياسات بالتشريعات الأردنية من قوانين وأنظمة وتعليمات التي لها علاقة وثيقة بهذه السياسات.

لهذا، فإنه من الضروري التركيز على الملحوظات التالية حول السياسات الوطنية لأمن وحماية المعلومات:

١. تحقق هذه السياسات الحدود الدنيا الواجب العمل بها في كافة الدوائر الحكومية، وللدائرة أن تزيد عليها ما تراه ملائماً لطبيعة وظروف عملها حسبما تقتضيه مصلحة العمل.

٢. تطبق هذه السياسات مع مراعاة القوانين والتشريعات المعمول بها في الدولة والمنصوص عليها بأحكام القانون الأردني، ونخص بالذكر:

أ. قانون حماية أسرار الدولة رقم ٥٠ لسنة ١٩٧١.

ب. قانون ضمان حق الحصول على المعلومات رقم ٤٧ لسنة ٢٠٠٧.

ج. قانون المعاملات الإلكترونية رقم ٨٥ لسنة ٢٠٠١.

د. قانون توظيف موارد تكنولوجيا المعلومات في المؤسسات الحكومية رقم ٨١ لسنة ٢٠٠٣.

٣. لا تتطرق هذه السياسات للتعليمات والإجراءات والتوجيهات الداخلية لكل دائرة فيما يخص الكيفية التي تراها الدائرة مناسبة لتطبيق هذه السياسات.

٤. وضعت الأدوار والمسؤوليات والواجبات العامة التي يكثر تكرارها والتي يجب تطبيقها في جميع السياسات الوطنية لأمن وحماية المعلومات في الفصل الأول بشكل يسبق بيان السياسات، وذلك من أجل معرفتها مسبقاً وعدم تكرارها لاحقاً.

٥. وضعت قائمة بالمصطلحات لبيان المرادفات العربية للمصطلحات الإنجليزية التي يكثر استعمالها في مجال أمن وحماية المعلومات.

الفصل الأول

الأدوار والمسؤوليات والواجبات العامة

فيما يلي بيان مختصر لأهم الأدوار والمسؤوليات المطلوبة من الدائرة ومدراء الأنظمة وضباط أمن المعلومات والمستخدمين والتي يكثر تكرارها في هذه الوثيقة، مع العلم أن تفصيل هذه الأدوار والمسؤوليات سيأتي بيانه في حينه حسب ما يقتضيه المقام.

١ الدائرة

١. تطبيق السياسات الوطنية لأمن وحماية المعلومات التي تعتبر الحدود الدنيا للممارسات المتعلقة بأمن وحماية المعلومات في الدائرة.
٢. وضع التعليمات والإجراءات المناسبة لتطبيق هذه السياسات.
٣. تعميم هذه السياسات على جميع الموظفين والعاملين في الدائرة وجعلها في متناول أيديهم بشكل مستمر.
٤. تعيين ضابط أمن معلومات وتوفير الدعم اللازم له من أجل توفير المهارات والتدريب الكافي للموظفين والعاملين في الدائرة والإشراف على فهم وتطبيق السياسات والتعليمات الخاصة بأمن وحماية المعلومات فيها.
٥. التدقيق على مدى الالتزام بهذه السياسات داخل الدائرة بهدف تحديد ومعالجة أي قصور أو ثغرات لوحظت فيها.
٦. وضع وتوضيح الإجراءات المناسبة لمحاسبة الموظفين والعاملين في الدائرة عن أي خلل أو قصور من شأنه الإخلال بأمن وحماية أي من الموارد المعلوماتية في الدائرة طبقاً للأنظمة المعمول بها في الدائرة.

٢ مدير النظام (مؤتمن المعلومات)

١. تطبيق التعليمات والإجراءات على جميع الموارد المعلوماتية الموجودة في الدائرة بالتوافق مع السياسات الوطنية لأمن وحماية المعلومات.
٢. توفير الدعم الفني الكافي الذي يضمن تطبيق هذه السياسات.
٣. التعاون مع مدققي أمن المعلومات للقيام بمهامهم بيسر وسهولة.

٣ ضابط أمن المعلومات

١. التأكد من تطبيق السياسات الوطنية لأمن وحماية المعلومات والتعليمات والإجراءات المتعلقة بها في الدائرة.
٢. التعاون مع جميع العاملين والمتعاملين مع الدائرة من أجل تطبيق هذه السياسات والتعليمات والإجراءات بأعلى مستويات الجودة الممكنة.
٣. القيام بالدور التوعوي المناسب لتدريب ورفع مستوى مهارات العاملين في الدائرة في مجال أمن وحماية المعلومات من خلال تطبيق برامج التوعية الخاصة بأمن وحماية المعلومات، والمشاركة في ورش العمل والندوات ذات العلاقة، من أجل العمل بالممارسات الفضلى في أمن وحماية المعلومات والالتزام بالسياسات الوطنية لأمن وحماية المعلومات، وبيان الآثار السلبية المترتبة على عدم الالتزام بها أو ترك العمل بها.
٤. التدقيق على مدى التزام جميع العاملين والمتعاملين مع الدائرة بهذه السياسات والتعليمات المتعلقة بها.
٥. مساعدة الموظفين والعاملين في الدائرة لمعالجة أية مشاكل لها علاقة بأمن وحماية المعلومات في الدائرة.

٤ المستخدم

١. قراءة هذه السياسات وفهمها والرجوع إليها عند الحاجة، والتوقيع على التقيد بما جاء فيها.
٢. بذل أقصى الجهود الممكنة لتنفيذ هذه السياسات والتعليمات المتعلقة بها في الدائرة.

٣. التعاون مع المختصين في مجال تكنولوجيا وأمن وحماية المعلومات والرجوع إليهم عند الحاجة.

الفصل الثاني

السياسات الوطنية لأمن وحماية المعلومات

السياسة الأولى: سياسة حساسية وتصنيف المعلومات

أولاً: الهدف

حماية كافة أنواع المعلومات وبأي صورة كانت وعلى جميع الوسائط، من الوصول إليها أو استعمالها أو تغييرها أو الإفصاح عنها أو إتلافها بشكل غير مرخص، في جميع مراحل دورة حياتها، بطريقة تتناسب وحساسيتها وأهميتها.

ثانياً: المجال

تغطي هذه السياسة جميع الموارد المعلوماتية للدائرة، سواءً أكانت إلكترونية أو غير إلكترونية.

ثالثاً: تفاصيل السياسة

١ تعريف المعلومات

أ- تتضمن المعلومات المعنيّة في هذه السياسة -دون تحديد- المعلومات التي يتم حفظها أو تبادلها بشتى الوسائل، سواءً أكانت إلكترونية أو غير إلكترونية، مثل المعلومات المكتوبة، أو تلك التي يتم تبادلها مشافهةً -مثل الهاتف- أو بشكل مرئي - مثل الاجتماعات المرئية والمسموعة -.

ب- على الدائرة وضع معايير شاملة تتضمن تفاصيل مواردها المعلوماتية بهدف تحديد أهميتها وحساسيتها وآثارها القانونية، واستخدام خطة التصنيف المتبعة في هذه السياسة.

٢ تصنيف المعلومات

أ- يجب تصنيف جميع المعلومات المملوكة للدائرة، استناداً إلى أحكام قانون ضمان حق الحصول على المعلومات رقم ٤٧ لسنة ٢٠٠٧.

ب- ليس لجميع المعلومات القدر نفسه من الحساسية والأهمية، وبالتالي فإن المعلومات تحتاج مستويات مختلفة من الحماية.

ج- يجب أن تتم إدارة المعلومات بشكل صحيح ابتداءً من مرحلة إنشائها، مروراً بالاستخدام المرخص لها، وانتهاءً بالطريقة الصحيحة لإتلافها.

د- الدائرة مسؤولة عن تصنيف المعلومات التي تملكها بالتوافق مع هذه السياسة، ولهذا يجب تصنيف وإدارة جميع المعلومات والوثائق بدقة حسب مستوى حساسيتها وأهميتها إلى أربعة مستويات: "عادية"، و"محدودة"، و"سرية"، و"سرية للغاية"، استناداً إلى أحكام قانون حماية أسرار الدولة رقم ٥٠ لسنة ١٩٧١ وأية تعديلات طرأت عليه.

ه- أية معلومات مملوكة للدائرة، مثل الوثائق الموجودة منذ أمد بعيد فيها و لم يتم تصنيفها قبل تطبيق هذه السياسة- يجب أن تعامل معاملة المعلومات "المحدودة"، وبصفة "لاستخدام الدائرة فقط" ما لم يقرر مسؤول المعلومات تصنيفها إلى معلومات "عادية" أو "سرية" أو "سرية للغاية"، استناداً إلى أحكام قانون ضمان حق الحصول على المعلومات.

٢-١ المستوى الأول: المعلومات العادية

أ- المعلومات العادية هي معلومات قليلة الحساسية، لا يؤثر الإفصاح عنها على خصوصية أو أمن الدائرة أو أي من المتعاملين معها مثل الموظفين والعملاء والشركاء ، أو تؤدي إلى إيذاء أي من المصالح السياسية أو الاقتصادية أو غيرها من المصالح الحكومية، وتكون عادة متاحة للنشر عبر وسائل الاتصال والإعلام، بالطرق الإلكترونية، أو الشفوية، أو المكتوبة، مثل المطبوعات المنشورة والنشرات والكتيبات وصفحات الإنترنت.

ب- لا توجد صلاحيات أو تحديدات على هذه النوع من التصنيف.

٢-٢ المستوى الثاني: المعلومات المحدودة

أ- هي معلومات حساسة معدة للاستخدام الرسمي، وإذا ما تم الإفصاح عنها فإنها يمكن أن تعرض خصوصية وأمن الدائرة أو أي من المتعاملين معها للخطر، أو تسبب إيذاءً محدوداً للمصالح السياسية أو الاقتصادية للدائرة، وبالتالي فإن الإفصاح غير المرخص عن المعلومات المحدودة يمكن أن يؤثر سلباً على الثقة بالموظفين والمواطنين، مثل البريد الإلكتروني غير المشفّر، والتعميمات والمذكرات الداخلية، والمعلومات التي يتم وسمها بطريقة تعكس محدوديتها، مثل: "لاستخدام الدائرة فقط" ، " لاستخدام القسم فقط".

ب- يجب على الدائرة وضع وإعلان التعليمات المناسبة للكشف عن هذه المعلومات قبل تقديمها لأي جهات خارجية.

ج- يتم تصنيف المعلومات الشخصية على أنها "محدودة" ما لم تحدد تعليمات الدائرة غير ذلك.

٢-٣ المستوى الثالث: المعلومات السرية

أ- معلومات حساسة معدّة للاستخدام الرسمي المحدود، وإذا تم الإفصاح عنها فإنها ستعرض أمن وخصوصية الدائرة والمتعاملين معها للخطر، أو تسبب لهم إيذاءً سياسياً أو اقتصادياً، مثل المعلومات التي من المتوقع أن تكون مفيدة للبلاد الأجنبية أو الجهات غير الحكومية، مثل وثائق العطاءات التي لم يتم طرحها بعد، والمعلومات المستثناة من الإفصاح عن المعلومات العادية والمحدودة.

ب- إن تصنيف المعلومات على أنها "سرية" أو "سرية للغاية" يجب ألا يتم بشكل عشوائي، وإنما يجب أن يكون حسب التعليمات والأنظمة، بما فيها قانون ضمان حق الحصول على المعلومات و قانون حماية أسرار الدولة.

ج- إن مسؤول المعلومات وحده له صلاحية إقرار هذا المستوى من التصنيف أو تغييره وتحديد كيفية الإفصاح عن هذه المعلومات.

٢-٤ المستوى الرابع: المعلومات السرية للغاية

أ- هي المعلومات التي تعتبر غاية في الحساسية والأهمية للدائرة، والتي تعرض أمنها وخصوصيتها والمتعاملين معها للخطر الشديد، أو تلك المعلومات المعدة للاستخدام من قبل جهات معينة، ويمكن أن يؤدي الإفصاح عنها بشكل غير مرخص إلى تهديد حياة الأشخاص، أو أضرار مادية أو معنوية للدائرة أو المتعاملين معها، أو يسبب إيذاءً هائلاً للحكومة ويعرض أمن الدولة للخطر، بالإضافة إلى المعلومات التي يترتب على الإفصاح عنها بشكل غير مرخص مساءلة قانونية، مثل معلومات الحسابات الشخصية، والتحقيقات الجارية، ومعلومات تتعلق بأمن الدولة، والمعلومات ذات الأهمية الاستخبارية أو العسكرية.

ب- إن مسؤول المعلومات وحده له صلاحية إقرار هذا المستوى من التصنيف أو تغييره وتحديد كيفية الإفصاح عن هذه المعلومات.

٣ حفظ المعلومات وتداولها وإتلافها

٣-١ حفظ المعلومات

أ- يجب أن تتوافق عملية حفظ المعلومات مع مستويات تصنيفها.

ب- يجب حفظ جميع وسائط التخزين في مكان آمن حسب تصنيف المعلومات المخزنة فيها. فمثلاً تحفظ المعلومات العادية دون الحاجة إلى تطبيق إجراءات أمنية صارمة، في حين يجب حفظ المعلومات "السرية" و"السرية للغاية" بطريقة صحيحة من أية تهديدات أو أخطار، أو الوصول إليها أو تداولها بشكل غير مرخص.

٣-٢ تداول المعلومات ونقلها

أ- يجب تداول المعلومات في الدائرة بطريقة تضمن حمايتها من الوصول إليها أو الإفصاح عنها أو تغييرها بشكل غير مرخص أو فقدانها ، ولهذا، فإنها يجب أن تعالج وتحفظ حسب مستويات تصنيفها في سبيل حماية سريتها ومستوى حساسيتها وسلامتها وإتاحيتها.

ب- على الدائرة التي تستخدم معلومات سرية متابعة إجراءات الحماية المناسبة واللازمة لتصنيفها، ولهذا فإن على كل مستخدم تطبيق مبدأ " المكتب النظيف" أثناء تداول معلومات "محدودة" أو معلومات ذات تصنيف أعلى.

٣-٣ إتلاف المعلومات

أ- على الدائرة وضع التعليمات الخاصة بإتلاف المعلومات عند الحاجة إلى ذلك.

ب- يجب إتلاف المعلومات سواءً أكانت إلكترونية أو غير إلكترونية عند الحاجة بطريقة تتفق مع مستوى تصنيفها وبطريقة تتفق مع القوانين والتشريعات الحكومية والأحكام والأنظمة والتعليمات. يلخص الجدول (١) بعض التوجيهات المتعلقة بحفظ المعلومات وتداولها وإتلافها.

الجدول ١ : دليل التعامل مع وسائط تخزين المعلومات

التصنيف	التخزين		التداول		الإتلاف	
	الإلكتروني	غير الإلكتروني	الإلكتروني	غير الإلكتروني	الإلكتروني	غير الإلكتروني
العادي	نص غير مشفر	غير محدد	نص غير مشفر	غير محدد	الحذف العادي	غير محدد
المحدود	إجراءات التحكم	إجراءات التحكم الفيزيائية	نص غير مشفر	المظروف المغلق	إعادة التهيئة	التحطيم**
السري	التشفير**	الخزنة الغرف المغلقة**	التشفير**	باليد بالبريد الرسمي**	الاستئصال** والتحطيم**	التحطيم**
السري للغاية	التشفير**	الخزنة الغرف المغلقة**	عدم استخدام الشبكات ولكن باليد**	باليد**	الاستئصال* والتحطيم**	التحطيم**

* يتم استخدام الاستئصال في حالة إعادة الاستخدام والتدمير في الإتلاف النهائية

**يجب العمل بالقوانين والأنظمة والتعليمات، ويكون التحطيم عادة بالطرق الفيزيائية مثل التكسير والتقطيع والتهشيم والطحن والعجن والحرق.

٤ عزل المعلومات

أ- على الدائرة وضع التعليمات المناسبة لتقديم المستويات الملائمة لحماية المعلومات بما يتناسب وحساسية المعلومات وأهميتها.

ب- يجب تخزين جميع المعلومات "السرية للغاية" في مكان معزول وآمن.

ج- يجب عزل جميع المعلومات ضمن تصنيفاتها بطريقة فيزيائية أو إلكترونية حسب مستوى حساسيتها.

٥ مسؤولية أمن وحماية المعلومات

أ- جميع المعلومات المملوكة للدائرة هي مسؤولية كل من يتعامل معها.

ب- يتحمل مسؤول المعلومات (الإدارة العليا) المسؤولية النهائية في أمن وحماية الموارد المعلوماتية في الدائرة.

٥-١ واجبات مسؤول المعلومات

يجب أن يكون لجميع المعلومات في الدائرة "مسؤول معلومات" لتحقيق المهام الرئيسية التالية:

أ- إيجاد تصنيف مبدئي للمعلومات، يتضمن إعطاء مستويات تصنيف لجميع المعلومات داخل الدائرة.

ب- المصادقة على التوصيات المتعلقة بالضوابط والصلاحيات والعمليات الخاصة بإدارة المعلومات.

ج- التأكد من أن المعلومات يتم مراجعتها بانتظام حسب أهميتها ومدى التغيرات المؤثرة على أهميتها عند وقوع المخاطر: كالتهديدات الجديدة، أو نقاط الضعف المكتشفة في الأنظمة، أو أية تغيرات في البيئة المحيطة بها.

د- مراجعة وتعديل التصنيف بين فترة وأخرى حسب التغيرات في أولويات العمل أو القوانين والتعليمات والأنظمة.

ه- تطبيق التعليمات الخاصة بحفظ وأرشفة الوثائق وما ينبني على هذه التعليمات من إعادة ترتيب لجميع الوثائق داخل الدائرة.

٥-٢ دور مؤتمن المعلومات

يجب أن يكون لجميع المعلومات في الدائرة "مؤتمن معلومات" لتحقيق المهام الرئيسية التالية:

أ- المتابعة اليومية لعمليات تصنيف المعلومات وكيفية تطبيقها داخل الدائرة.

ب- حماية المعلومات المصنفة حسب تصنيف مسؤول المعلومات.

ج- تطبيق وتنفيذ إجراءات الأمن والحماية المناسبة من أجل حماية المعلومات المصنفة.

٥-٣ واجبات ضابط أمن المعلومات

أ- مراقبة أي خروقات لسياسة أمن المعلومات ورفع التقارير بشأنها لمسؤول المعلومات.

ب- التأكد من أن جميع المستخدمين على علم بكيفية تداول وحماية المعلومات بطريقة تتناسب مع تصنيفها.

ج- تطوير إجراءات أمن وحماية المعلومات في الدائرة.

٦ وسم المعلومات

أ- على الدائرة وضع التعليمات المناسبة لوسم المعلومات بطريقة توضح المسؤولية عن المعلومات وتصنيفها.

ب- يمكّن الوسم الصحيح لوسائط تخزين المعلومات المستخدمين من تداول المعلومات وفقاً للتوجيهات المذكورة في الجدول أعلاه بشكل آمن وصحيح.

ج- يضمن تطبيق وتطوير الإجراءات الصحيحة لوسم المعلومات توافق هذه المعلومات مع السياسات الوطنية لأمن وحماية المعلومات.

٧ الإفصاح عن المعلومات

٧-١ الوعي الخاص بالإفصاح عن المعلومات

أ- إن الفهم الصحيح لجميع المستخدمين بتصنيف المعلومات يساعد على تطبيق التعليمات المناسبة للإفصاح عنها.

ب- على جميع المستخدمين إدراك التأثيرات المترتبة على الإفصاح عن المعلومات التي من شأنها تعريض مصالح الدائرة خاصة والمصالح الحكومية عامة للخطر، ويجب وضع تعليمات لضمان تطبيق هذه السياسة.

ج- يمكن الإفصاح عن المعلومات "المحدودة" لطرف ثالث بعد تقديم "اتفاقية عدم الإفصاح عن المعلومات" ومراجعتها قانونياً وتوقيعها من قبل الأشخاص المخولين بذلك شريطة موافقة مسؤول المعلومات.

٧-٢ العقوبات المترتبة على الإفصاح غير المرخص عن المعلومات

أ- يجب التعميم على المستخدمين بالإجراءات التأديبية والعقوبات المترتبة على الإفصاح عن المعلومات بشكل غير مرخص حسب تصنيفها ووسمها بالتوافق مع التشريعات والقوانين النافذة.

ب- يجب أن تغطي هذه الإجراءات سرقة المعلومات وقراءتها والوصول إليها، ونسخ وطباعة المعلومات المصنفة بدرجة "محدود" فأكثر.

ج- يجب أن تعتمد هذه الإجراءات ضد هذه الأفعال أو ما شابهها على:

١. القوانين والأنظمة والسياسات.
٢. تصنيف المعلومات التي تم الإفصاح عنها بشكل غير مرخص.
٣. تأثيرات الإفصاح غير المرخص لهذه المعلومات على الدائرة بشكل خاص وعلى الحكومة ككل.
٤. نسبة انتشار المعلومات التي تم الإفصاح عنها بشكل غير مرخص بين الجهات غير المخولة.
٥. طبيعة الجهات غير المخولة التي تم الإفصاح لها بشكل غير مرخص عن المعلومات، كأن يكونوا مواطنين أو مقيمين أو أعداء.

السياسة الثانية: سياسة الاستعمال المقبول

أولاً: الهدف

توفير بيئة نظم معلومات آمنة وموثوقة ومريحة للاستخدام بحيث يتحمل جميع العاملين في الدائرة المسؤولية في الاستعمال الصحيح للمعلومات ومواردها والبنية التحتية التكنولوجية لها.

ثانياً: المجال

توضح هذه السياسة الممارسات الفضلى للاستعمالات المقبولة والممنوعة التي يجب على جميع مستخدمي الموارد المعلوماتية في الدائرة أخذها بعين الاعتبار عند التعامل معها.

ثالثاً: تفاصيل السياسة

١ أجهزة الحاسوب

يوضح هذا البند الاستعمالات المقبولة والممنوعة لأجهزة الحاسوب في الدائرة، بما يتضمنه ذلك من أنظمة التشغيل، وبرامج وملفات المستخدمين، وبرمجيات المحاسبة، وجميع أنظمة المعلومات في الدائرة.

١-١ الممارسات المقبولة

أ- تنصيب وتحديث وإعداد البرمجيات المرخصة الخاصة بالعمل عن طريق مدير النظام اعتماداً على الوصف الوظيفي للمستخدم والمسؤوليات المناطة به.

ب- استخدام البرمجيات المرخصة لتحقيق أهداف الدائرة والمهمات الملقاة على عاتقها.

ج- إنشاء ومعالجة وأرشفة وحذف ملفات المستخدم حسبما تقتضيه طبيعة ومصلحة العمل.

١-٢ الممارسات الممنوعة

أ- إزالة أو حذف أي من البرمجيات أو الملفات الضرورية التي يحتاجها المستخدم لأداء واجباته حسب وصفه الوظيفي ومسؤولياته ومصلحة العمل.

ب- نسخ البرمجيات أو الملفات إلى وسائط تخزين خارجية لغير أغراض العمل الرسمي.

ج- تنصيب أيّة برمجيات غير مرخصة أو مشبوهة أو البرامج المساعدة أو اللهو بالألعاب.

د- تنصيب وتشغيل برمجيات أو تطبيقات مصابة بالفيروسات أو الديدان أو أحصنة طروادة أو البرامج الإعلانية أو أي نوع من البرمجيات الخبيثة.

ه- استعمال البرمجيات والتطبيقات المرخصة للمنفعة الخاصة أو تطوير برمجيات خبيثة أو استخدمها لغير أغراض العمل الرسمي.

٢ الإنترنت

يوضح هذا البند الاستعمالات المقبولة والممنوعة لخدمة الإنترنت في الدائرة لتحقيق أهدافها ومصلحة العمل فيها.

٢-١ الممارسات المقبولة

أ- البحث عبر الإنترنت لأغراض العمل الرسمي.

ب- الدخول إلى مواقع الإنترنت الموثوقة والمرخصة لتنزيل التحديثات والإصلاحات للبرمجيات المرخصة العاملة في الدائرة، ويكون ذلك من قبل مدير النظام، وحسب عملية ضبط التغيير المتبعة في الدائرة استناداً إلى سياسة ضبط التغيير.

ج- تنزيل أي محتوى له علاقة بطبيعة العمل للموظف شريطة تحقق جميع الشروط التالية:

١. أن يكون الموقع موثوقاً. (بقدر الحذر)

٢. التأكد أن مادة المحتوى مرخصة.

٣. التأكد أن مادة المحتوى خالية من البرامج الخبيثة. (بقدر الاستطاعة)

٤. ألا تؤثر مادة المحتوى سلباً على الأداء العام للربط بالإنترنت في الدائرة.

٥. أن يتم ذلك بالرجوع إلى مدير النظام في الدائرة.

٢-٢ الممارسات الممنوعة

أ- تنزيل مواد غير قانونية أو معادية أو ليست لها علاقة بطبيعة ومصلحة العمل.

ب- تنزيل البرامج من الإنترنت وتشغيلها بدون موافقة مسبقة من الإدارة العليا في الدائرة.

ج- اللهو بالألعاب واستخدام غرف الدردشة لأغراض شخصية.

د- المشاركة والمساهمة في المجموعات الإخبارية التي لا علاقة لها بالعمل الرسمي.

ه- تصفح الإنترنت بشكل زائد عن الحد المقبول لغير أغراض العمل الرسمي، ويحدد ذلك الأمين العام أو المدير العام للدائرة اعتماداً على التعليمات المتبعة داخل الدائرة.

٣ الشبكات المعلوماتية الحكومية

يوضح هذه البند الاستخدامات المقبولة والممنوعة للشبكات المعلوماتية في الدائرة بما يتضمنه ذلك من خوادم وموجهات وجدران نارية وأسلاك وبروتوكولات.

٣-١ الممارسات المقبولة

أ- استخدام أجهزة وعناصر الشبكات والبنية التحتية المعلوماتية لأغراض العمل الرسمي.

ب- اتباع عملية ضبط التغير المتبعة في الدائرة عند تغيير أو إزالة عناصر وأجهزة الشبكات أو تغيير حزم الاتصالات والتمديدات عند الحاجة عن طريق مختصّي الشبكات المخولين بذلك.

ج- تنصيب وتحديث وضبط إعدادات البرمجيات والأجهزة المرخصة لمراقبة وحماية الاتصالات عبر الشبكات، مثل الجدران النارية وأنظمة كشف ومنع التطفل والاختراق بالتوافق مع تعليمات الدائرة.

د- إنشاء وإلغاء ومعالجة سجلات الدخول الإلكترونية للمستخدمين على الشبكات، إضافة إلى منح وحجب الصلاحيات حسب الوصف الوظيفي للمستخدمين، شريطة وجود موافقة مسبقة ومكتوبة من الإدارة العليا في الدائرة.

٣-٢ الممارسات الممنوعة

أ- إتلاف أو فصل أي عنصر أو جهاز تابع للشبكة بدون صلاحية أو موافقة مسبقة ومكتوبة من الإدارة العليا في الدائرة.

ب- استخدام أجهزة الشبكات في غير أغراض العمل الرسمي.

ج- تناول الأطعمة والمشروبات أو التدخين في غرف مراكز البيانات أو قرب أجهزة الشبكات مثل الموجّهات والمفاتيح.

د- محاولة التأثير بشكل سلبي على الأداء الفيزيائي أو المنطقي للشبكات بشكل مباشر أو غير مباشر بالقيام بواحد أو أكثر من الأفعال التالية:

١. تنزيل أو تحميل كميات ضخمة من الملفات أو البيانات لغير الضرورة.

٢. التسبب برفع درجة حرارة أجهزة الشبكات باستخدام المدافئ أو تخريب أنظمة التكييف والتبريد.

مراقبة ***Monitoring*** واقتناص ***Capturing*** تدفق المعلومات عبر الشبكات أو التجسس عليها بدون موافقة مسبقة ومكتوبة من الإدارة العليا في الدائرة.

ه- منح وحجب الصلاحيات لسجلات الدخول الإلكترونية للمستخدمين الحاليين أو الجدد بدون تصريح.

و- تنصيب أجهزة أو برمجيات على الشبكات بدون موافقة مسبقة ومكتوبة من الإدارة العليا في الدائرة بالتوافق مع سياسة ضبط التغيير.

٤ أنظمة البريد الإلكتروني

يوضح هذا البند الممارسات المقبولة والممنوعة عند استخدام أنظمة البريد الإلكتروني الحكومية.

٤-١ الممارسات المقبولة

أ- فتح وقراءة وإرسال وتخزين البريد الإلكتروني الرسمي.

ب- إدارة سجل البريد الإلكتروني الخاص بالمستخدم.

ج- إرسال المرفقات ذات المحتوى الرسمي للجهات الرسمية بالتوافق مع سياسة حساسية وتصنيف المعلومات.

د- تنزيل المرفقات من المصادر الرسمية، بعد مسحها بإجراءات الحماية الملائمة للتأكد من خلوها من أية تهديدات تتعلق بالبرامج الخبيثة.

ه- استعمال أنظمة البريد الإلكتروني الشخصي بشكل مناسب يتوافق مع ميثاق السلوك الخاص بأمن المعلومات.

٤-٢ الممارسات الممنوعة

أ- استخدام أنظمة البريد الإلكتروني لغير الأغراض الرسمية أو بطريقة تؤثر سلباً على سير العمل.

ب- إرسال وتنزيل مرفقات كبيرة الحجم لغير الاستعمالات الرسمية مثل ملفات الصوت والصورة التي قد تؤثر سلباً على كفاءة أنظمة الدائرة.

ج- التجسس على البريد الإلكتروني للمستخدمين الآخرين أو اختراقه.

٥ سجلات الدخول الإلكترونية للمستخدمين

يوضح هذا البند الاستعمالات المقبولة والممنوعة في التعامل مع سجلات الدخول الإلكترونية للمستخدمين التي يتم إنشاؤها ضمن أنظمة وإجراءات الحكومة.

٥-١ الممارسات المقبولة

أ- منح وحجب وتغيير الصلاحيات لسجلات الدخول الإلكترونية للمستخدمين عن طريق مدراء النظام المخولين بذلك حسب حاجة الدائرة وحسب الوصف الوظيفي لهؤلاء المستخدمين وطبيعة أعمالهم.

ب- إدارة ملف المستخدم ***User Profile*** عن طريق المستخدم صاحب السجل فقط.

٥-٢ الممارسات الممنوعة

أ- انتهاك واختراق سجلات الدخول الإلكترونية للمستخدمين.

ب- استخدام سجلات الدخول الإلكترونية للمستخدمين بدون ترخيص للشروع في هجوم المنع من الخدمة ضد أي جهة كانت.

ج- إضافة أو حذف سجلات الدخول الإلكترونية للمستخدمين، أو منح أو حجب صلاحيات معينة بدون ترخيص مسبق ومكتوب من الإدارة العليا في الدائرة.

د- جمع المعلومات من سجلات الدخول الإلكترونية للمستخدمين لأي غرض كان بدون ترخيص مسبق ومكتوب من الإدارة العليا في الدائرة.

ه- تبادل المعلومات الخاصة بسجلات الدخول الإلكترونية.

٦ المعدات

يوضح هذا البند الاستخدامات المقبولة والممنوعة للمعدات في الدائرة، مثل الحواسيب الشخصية للمستخدمين، وأجهزة الاتصالات مثل الهاتف، والطابعات، وأجهزة التكييف، والمولدات الكهربائية.

٦-١ الممارسات المقبولة

أ- تنصيب وتحديث وضبط إعدادات واستخدام المعدات المرخصة التي تعود ملكيتها للدائرة بما يتوافق مع سياسة ضبط التغيير.

ب- إصلاح هذه المعدات عن طريق المختصّين المخولين بذلك عند الحاجة، حسب عملية ضبط التغيير المعتمدة في الدائرة بالتوافق مع سياسة ضبط التغيير.

ج- حفظ ونقل واستقبال وعرض ومعالجة أيّ محتوىً رسمي باستخدام هذه المعدات حسب الصلاحيات الممنوحة للمستخدم.

٦-٢ الممارسات الممنوعة

أ- القيام بأي عمل من شأنه تخريب الأجهزة أو أيّة برمجيات تتعلق بها أو إحداث قصور فيها بشكل مباشر أو غير مباشر.

ب- تركيب أو إزالة شيء من المعدات بدون تصريح مكتوب وموافق عليه من الإدارة العليا في الدائرة بذلك حسب عملية ضبط التغيير المعتمدة فيها.

ج- استغلال أي من هذه المعدات للمنفعة الشخصية.

٧ الدعم الفني

يوضح هذا البند الممارسات الفضلى للدعم الفني في الدائرة، بما يتضمنه ذلك من تنصيب للبرمجيات والمعدات، وإعدادها وتحديثها، إضافة إلى كشف الأعطال وإصلاحها.

٧-١ الممارسات المقبولة

أ- إن فريق الدعم الفني مسؤول عن تنصيب وإعداد وتحديث وكشف الأعطال وإصلاحها لأي جهاز أو برمجية حسب عملية ضبط التغيير.

٧-٢ الممارسات الممنوعة

أ- إصلاح أو محاولة تغيير أي من المعدات من قبل الأشخاص غير المتخصصين وغير المخولين بذلك.

٨ ملحوظات هامة

إن تحديد الاستعمال الشخصي الذي له سبب مقبول متروك للدائرة شريطة أن تأخذ بعين الاعتبار النقاط التالية:

أ- الأداء العام للموارد المعلوماتية.

ب- القوانين والأنظمة والتعليمات المعمول بها في الدولة.

ج- طبيعة وبيئة العمل.

د- الوصف الوظيفي للمستخدمين.

ه- السياسات الوطنية لأمن وحماية المعلومات الأخرى.

السياسة الثالثة: سياسة ضبط التغيير

أولاً: الهدف

ضمان أمن وحماية الموارد المعلوماتية عند القيام بأي تغيير قد يؤثر عليها.

ثانياً: المجال

تغطي هذه السياسة أي تغيير قد يؤثر على إعدادات أو تنصيب أو إزالة أو إتلاف أي من الموارد المعلوماتية المملوكة للدائرة، مثل الملفات والبرمجيات والأجهزة والمعدات والشبكات ووسائط التخزين والوثائق ، كما تغطي كذلك الأشخاص المسؤولين عن تقديم طلبات التغيير (مثل مدير النظام) ومراجعتها والموافقة عليها (مثل ضابط أمن المعلومات ومدير تكنولوجيا المعلومات، وفي بعض الحالات الإدارة العليا).

ثالثاً: تفاصيل السياسة

١ قواعد عامة

أ- على الدائرة وضع التعليمات والإجراءات المناسبة لتنظيم عملية ضبط التغيير داخل الدائرة بالتوافق مع هذه السياسة،

ب- على الدائرة متابعة عمليات ضبط التغيير والتدقيق على مدى تطبيقها بالتوافق مع هذه السياسة.

ج- لا يسمح بإجراء أي تغيير يتعلق بأيٍّ من الموارد المعلوماتية المملوكة للدائرة بدون المرور في عملية ضبط التغيير المعمول بها في الدائرة.

د- تقسم طلبات التغيير إلى نوعين رئيسيين:

١. تغييرات مجدولة: وهي التي تحتاج إلى موافقة مسبقة.

٢. تغييرات طارئة: وتتعلق عادة بالتغييرات غير المخطط لها، وهنا يرجع فيها إلى المسؤول المباشر، ومن ثمّ يتم الإبلاغ عن التغييرات التي تم إجراؤها فيما بعد من أجل توثيقها حسب الأصول.

ه- على الدائرة تحديد المسؤولين عن تقديم طلبات التغيير والجهة المسؤولة عن مراجعته والموافقة عليه، وتوثيق طلبات التغيير، والإجراءات التي تبعت هذه الطلبات بعد القبول أو الرفض.

٢ واجبات مدير النظام

أ- تقديم طلبات التغيير من أجل الموافقة عليها من قبل ضابط أمن المعلومات والشخص المسؤول عن الموافقة في الدائرة.

ب- التنسيق مع ضابط أمن المعلومات من أجل مراجعة طلبات التغيير المقدمة وإرفاق التوصيات الخاصة بأمن المعلومات بهذه الطلبات.

ج- إجراء التغيير المطلوب بعد موافقة الإدارة العليا في الدائرة، أو الإيعاز بإجرائها لمن يلزم.

٣ واجبات المستخدم

أ- عدم إجراء أي تغيير على أي من الموارد المعلوماتية المملوكة للدائرة.

ب- إبلاغ مدير النظام عند الحاجة لإجراء أي عملية تغيير تتعلق بعمل المستخدم والقيام بمسؤولياته في الدائرة.

السياسة الرابعة: ميثاق السلوك الخاص بأمن المعلومات

أولاً: الهدف

تعزيز السلامة العامة وإيجاد بيئة عمل مهنية آمنة يتعامل فيها موظفو الحكومة بمستوىً عال من الأخلاق والمسؤولية أثناء استخدامهم المعلومات وجميع الموارد المعلوماتية ممارسة الطرق الصحيحة لحمايتها.

ثانياً: المجال

تنطبق هذه السياسة على جميع العاملين في الدائرة، إضافة إلى منتسبي هذه الدوائر والمتعاملين معها.

ثالثاً: تفاصيل السياسة

١ مقدمة

ميثاق السلوك الخاص بأمن المعلومات هو مجموعة من القواعد والأحكام التي تحدد وترسم مسؤوليات الممارسات الصحيحة للفرد أو الدائرة، والتي يجب تطبيقها من أجل توفير بيئة عمل آمنة ومستقرة تساعد في الحفاظ على الموارد المعلوماتية في الدائرة.

٢ قواعد عامة

أ- اتباع قوانين الدولة والأنظمة والتعليمات الداخلية في الدائرة.

ب- تنفيذ سياسات أمن وحماية المعلومات التابعة للدائرة التي تعتمد على السياسات الوطنية لأمن وحماية المعلومات.

ج- استخدام الموارد المعلوماتية الحكومية في مصلحة استمرارية العمل في الدائرة والحفاظ على سمعتها.

د- التعامل بشفافية، وعدم حجب المعلومات عن الآخرين، تبعاً لقانون ضمان حق الحصول على المعلومات وبالتوافق مع سياسة حساسية وتصنيف المعلومات.

ه- عدم إهدار الوقت والجهد في استخدام المعلومات ومواردها لخدمة أي مصلحة خارجية، أو للمصلحة الشخصية، مثل الأنشطة التجارية (كالأسهم) والأنشطة السياسية، وذلك بالتوافق مع سياسة الاستعمال المقبول.

و- سجلات الدخول الإلكتروني ذات خصوصية وسرية، والموظفون غير مخولين بتبادل المعلومات الخاصة بسجلاتهم.

ز- على جميع الموظفين تطبيق " الوصايا العشر في أخلاقيات الحاسوب" التي أوصى بها معهد أخلاقيات الحاسوب وهي:

١. عدم استخدام الحاسوب لإيذاء الآخرين.
٢. عدم التدخل في عمل الآخرين على الحاسوب.
٣. عدم التطفل على ملفات الحاسوب للآخرين.
٤. عدم استخدام الحاسوب في السرقة.
٥. عدم استخدام الحاسوب للإدلاء بشهادة الزور.
٦. عدم نسخ أو استعمال برمجية محفوظة الملكية ما لم تكن مدفوعة السعر.
٧. عدم استخدام مصادر الحاسوب للآخرين بدون تصريح أو تفويض صحيح.
٨. عدم الاستيلاء على النتاجات الفكرية للآخرين.
٩. التفكير في التداعيات الاجتماعية للبرنامج الذي تتم كتابته للنظام الذي يراد تصميمه.
١٠. استخدام الحاسوب بالوسائل التي تضمن الاحترام للآخرين.

٣ التوظيف والتنقلات

٣-١التوظيف

أ) قبل التوظيف

١. على الدائرة تحديد ووضع قائمة بالمهام والمسؤوليات المناطة بشكل يحقق مبدأ " الفصل بين المهام".

ب) بعد التوظيف

١. يجب إعطاء جميع الموظفين الذين تم تعيينهم الحد الأدنى من الصلاحيات والامتيازات اللازمة لإتمام أعمالهم حسب الوصف الوظيفي لكل منهم، اعتماداً على مبدأ " المعرفة على قدر الحاجة ".

٢. على الموظفين الجدد توقيع اتفاقية "عدم الإفصاح عن المعلومات" عند البدء بممارسة أعمالهم، والتي يتم مراجعتها وإقرارها بشكل قانوني بين الموظفين الجدد وبين الدائرة.

٣-٢ التنقلات

١. يجب عدم نقل الموظفين من وظيفة إلى أخرى بدون قرار مسبق ومكتوب من الإدارة العليا في الدائرة بذلك.

٢. يجب أن يتم تغيير جميع المهام والصلاحيات المسندة للموظفين المنتقلين لكل منهم حسب اللازم، وبموجب موافقة مسبقة ومكتوبة من الإدارة العليا في الدائرة

٤ إنهاء الخدمات

أ- يجب تغيير سجل الدخول الإلكتروني وإلغاء أية صلاحيات أخرى للموظف الذي أنهيت خدماته، بعد التأكد من تسليم جميع المعلومات الخاصة بالعمل إلى الشخص المسؤول عنه أو الذي سوف ينوب عنه في عمله.

ب- يجب على الموظف الذي أنهيت خدماته تسليم كل ما بحوزته من المفاتيح، والأدوات، والمعدات، وبطاقات المرور التي هي ملك للدائرة التي يعمل فيها.

ج- على الموظف توقيع تعهد أو إقرار مع الدائرة بأنه لا يحتفظ بأية معلومات سرية هي ملك لها على أية وسائط تخزين سواء أكانت إلكترونية أو غير إلكترونية، وأنه يتحمل المسؤولية في حالة الإفصاح عنها بشكل غير مرخص بعد إنهاء الخدمة.

د- لا يسمح للموظف الذي أنهيت خدمته باستخدام الأجهزة والوصول إلى المعلومات المملوكة للدائرة.

ه- يجب حفظ نسخة من صندوق البريد الإلكتروني الخاص بالموظف المنهي عقده لفترة مناسبة لاستخدامه في حال استدعت الحاجة، وتحويل جميع الرسائل الموجهة إلى بريده الإلكتروني إلى الموظف الذي سينوب عنه.

٥. السلامة والأمان

أ- على جميع الموظفين حماية المعلومات والأجهزة والمحافظة عليها من التلف أو التخريب أو الضياع.

٦. الخصوصية

أ- معلومات الموظفين الشخصية ذات خصوصية ويجب حمايتها من الإفصاح عنها بشكل غير مرخص.

ب- للموظفين الحق في استخدام موارد المعلومات المخول لهم باستخدامها والدخول إليها ما دام في نطاق مهامهم.

ج- على الموظفين عدم انتهاك خصوصية معلومات أي من الموظفين الآخرين.

٧. قواعد التقارير والتدقيق والمتابعة

أ- يجب على الموظفين اتباع التسلسل الإداري عند رفع التقارير.

ب- على المسؤولين تطبيق التعليمات ضد أي خروقات من الموظفين ضمن القوانين والأنظمة والتعليمات والسياسات في دوائرهم.

ج- ليس لأي موظف الحق في ممارسة دور " المدقق" أو القيام بتدقيق أو تحقيق بدون تصريح مسبق ومكتوب من الإدارة العليا في الدائرة.

د- على الموظفين الالتزام بتعليمات التدقيق الصادرة عن الدائرة، بالتوافق مع سياسة التدقيق الخاص بأمن المعلومات.

٨ التعامل مع المعلومات

أ- على الموظفين التعامل مع المعلومات وحفظها وإتلافها بشكل موثوق به حسب تصنيف هذه المعلومات، بالتوافق مع سياسة حساسية وتصنيف المعلومات.

ب- لا يسمح للموظفين بالتصريح عن المعلومات السرية أو الإفصاح عنها بدون تصريح مسبق من مسؤول المعلومات.

ج- على الموظفين تطبيق مبدأ " المكتب النظيف".

د- لا يسمح للموظفين بمحاولة الدخول إلى المعلومات السرية سواءً بشكل مباشر أو غير مباشر بدون الحصول على الصلاحيات المناسبة لذلك من مسؤول المعلومات.

ه- على الموظفين حماية المعلومات التي تقع ضمن اختصاصهم بقدر الاستطاعة.

و- جميع المعلومات المحفوظة أو المطبوعة أو المنقولة على أجهزة الدائرة أو وسائطها هي ملك للدائرة الحكومية.

٩ موارد المعلومات

أ- على جميع الموظفين عدم ترك أجهزة الحاسوب (الثابتة أو المتنقلة) مفتوحة أثناء عدم تواجدهم عندها.

ب- لا يسمح للموظفين بالدخول إلى أي مورد معلومات حكومي بدون تصريح مسبق من الإدارة العليا في الدائرة بذلك.

ج- أي خرق أو تعارض مع سياسات الدائرة أو السياسات الوطنية لأمن وحماية المعلومات أو القوانين والتشريعات الأردنية فإنه يجب أن يتم رفع تقرير فيه إلى الإدارة العليا حسب تعليمات الدائرة.

د- عند استعمال الهاتف أو البريد الإلكتروني، فعلى الموظفين التأكد من هوية المتحدث أو المصدر قبل الإدلاء بأية معلومات.

١٠ ميثاق السلوك لضباط أمن المعلومات

على ضباط أمن المعلومات العمل بميثاق الأخلاقيات الأمنية في أعمالهم، والموضحة أدناه:

أ- أن يتحلى الضابط بأعلى المستويات الأخلاقية والعقلانية والسلوك السديد.

ب- ألا يكون مرتبطاً أو عضواً في أي عمل غير قانوني أو غير أخلاقي يمكن أن يؤثر سلباً على سمعته المهنية أو سمعة وظيفته.

ج- رفع التقارير بخصوص الأعمال الواقعة ضمن تخصصه والتي يعتقد أنها غير قانونية وأن يتعاون في حال أدى ذلك إلى إجراء تحقيق بخصوص تلك الأعمال.

د- دعم الجهود التي تساعد في نشر الوعي الخاص بأمن وحماية المعلومات وتفعيل إجراءات أمن وحماية المعلومات عبر القطاعات العامة والخاصة والأكاديمية.

ه- تنفيذ الإجراءات الخاصة بأمن المعلومات للموظفين والعملاء بأعلى مستويات الجودة الممكنة، وعليه المساعدة في منع وحل أي مخالفات أو خلافات يمكن أن تنشأ بينهم.

و- تنفيذ المسؤوليات المسندة إليه بطريقة تتوافق مع أعلى مستويات التخصص.

ز- عدم إساءة استخدام المعلومات التي يتعامل معها أثناء أداء واجباته، وعليه المحافظة على سريتها وسرية جميع المعلومات التي تقع تحت حوزته.

السياسة الخامسة: سياسة التدقيق الخاص بأمن المعلومات

أولاً: الهدف

التأكد من سلامة وأمن وإتاحية المعلومات ومواردها، والكشف عن إمكانية وقوع الحوادث الأمنية، وضمان وجود وفاعلية الإجراءات المتبعة في الدوائر وتوافقها مع سياسات أمن وحماية المعلومات فيها، وتقييم المخاطر الإجمالية الواقعة على الأنظمة المعمول بها في الدائرة، ودعم الإجراءات التي تساعد على تحديد نقاط الضعف فيها.

ثانياً: المجال

تعطي هذه السياسة جميع الموارد المعلوماتية والسجلات وموارد المعلومات المملوكة للدوائر الحكومية المدنية (مثل أنظمة الحاسبات والاتصالات) ، والسياسات والإجراءات والتعليمات والسلطات والمسؤوليات وأية أعمال ترتبط بأية وثائق أخرى داخلية أو خارجية، والمعمول بها في هذه الدوائر.

ثالثاً: تفاصيل السياسة

١ الصلاحيات

أ- التدقيق نوعان:

١. داخلي: تقوم به الدائرة لتدقيق الموارد المعلوماتية فيها والإجراءات المعمول بها داخل الدائرة، ويقرّ الصلاحية فيه مدير الدائرة.

٢. خارجي: يقوم به مركز تكنولوجيا المعلومات الوطني على أي من الدوائر الأخرى.

ب- يمكن للدائرة أن تقوم بعملية تدقيق داخلي بالاستعانة بفريق تدقيق من القطاع الخاص، ويقرّ الصلاحية فيه مدير الدائرة، بعد توقيع اتفاقية واضحة تحدد الامتيازات والصلاحيات اللازمة لإجراء عملية التدقيق، بعد موافقة مركز تكنولوجيا المعلومات الوطني بالتوافق مع سياسة التعاقد الخارجي.

ج- مدير الدائرة هو صاحب الصلاحية في ترخيص وإقرار التدقيق الداخلي في دائرته.

د- لفريق التدقيق استقلالية مهنية عن الجهة التي يقوم بالتدقيق عليها وألاّ يكون عاملاً فيها.

ه- لفريق التدقيق استقلالية مؤسسية عن المنطقة أو النشاط الذي يتم إجراء عملية التدقيق له.

و- يجب تحديد شكل وطبيعة العلاقات بين الجهات العليا وفريق التدقيق والجهة القائمة على مراجعة التدقيق.

ز- لا يجوز لأي من الموظفين إجراء أي عملية تدقيق داخلي بدون الحصول على تصريح مسبق من مدير الدائرة.

ح- على جميع الموظفين التعاون مع المدققين أثناء عملية التدقيق، وتسهيل عملهم، وعدم وضع العوائق التي تحول دون قيامهم بواجبهم الرسمي.

ط- يجب منح الصلاحيات المناسبة والكافية لطاقم تدقيق أمن المعلومات من أجل إجراء عملية التدقيق بفاعلية، على سبيل المثال:

١. الوصول إلى أي من الحواسيب أو أجهزة الاتصالات بمستوى مستخدم عادي أو مدير النظام.

٢. الوصول إلى المعلومات بجميع أشكالها الإلكترونية وغير الإلكترونية التي يتم إنشاؤها وحفظها ونقلها عبر شبكات الحاسوب في الدائرة، بما يخدم عملية التدقيق.

٣. الوصول إلى مرافق الدائرة المختلفة، مثل الأرشيف ومراكز البيانات والخوادم ومكاتب الموظفين والمختبرات.

٤. مراقبة وتسجيل حركة البيانات عبر الشبكات المعلوماتية.

٢ واجبات فريق التدقيق

أ- تخطيط وجدولة عمليات التدقيق.

ب- أداء عملية التدقيق بالاستناد إلى المعايير والمقاييس العالمية مثل ***ISO 17799*** والتي تشمل اثني عشر حقلاً هي:

١. إدارة المخاطر. ***Risk Management***

٢. سياسات الأمن والحماية. ***Security Policy***

٣. تنظيم أمن المعلومات. ***Organization Of Information Security***

٤. إدارة الموارد. ***Asset Management***

٥. أمن الموارد البشرية. ***Human Resource Security***

٦. الأمن المادي والبيئي. ***Physical And Environmental Security***

٧. إدارة العمليات والاتصالات. ***Communication And Operation Management***

٨. ضبط التحكم. ***Access Control***

٩. الحصول على نظم المعلومات وتطويرها وصيانتها. ***Information Systems Acquisition, Development And Maintenance***

١٠. إدارة الحوادث الخاصة بأمن وحماية المعلومات. ***Information Security Incident Management***

١١. إدارة عمليات استمرارية الخدمة. ***Business Continuity Management***

١٢. التوافق والملاءمة مع السياسات القائمة. ***Compliance***

ج- مراجعة العمليات والبرامج للتأكد من أن موارد المعلومات في الدائرة يتم استخدامها بشكل صحيح يتوافق مع السياسات الوطنية لأمن وحماية المعلومات والأهداف التي وضعت هذه الموارد من أجلها.

د- تقييم الإجراءات والتعليمات الداخلية للتأكد من موافقتها للسياسات والتعليمات المتداولة داخل الدائرة، مثل مبدأ "الفصل بين الوظائف"، و"المعرفة على قدر الحاجة" و "العمل بقدر الاستطاعة والحذر".

ه- جمع وتقييم الأدلة المناسبة لتقرير وجود أي خلل أو عدم توافق للإجراءات أو الموارد المعلوماتية مع السياسات الوطنية لأمن وحماية المعلومات المعمول بها داخل الدائرة.

و- التأكد من ضمان جودة عملية التدقيق والتقارير والوثائق الصادرة عنها.

ز- القيام بعملية التدقيق بشكل دوري للتحقق من مدى التزام الدائرة بتوصيات فريق التدقيق وإعلام مدير الدائرة (في حالة التدقيق الداخلي) أو مركز تكنولوجيا المعلومات الوطني (في حالة التدقيق الخارجي).

٣ التقارير

أ- على فريق تدقيق أمن المعلومات إصدار تقرير مفصل بجميع نتائج التدقيق من أجل متابعة الإجراءات اللازمة لمعالجة أي استثناءات أو أخطاء حسب الحالات التالية:

١. إذا كان التدقيق داخلياً فإن التقارير ترفع فيه لمدير الدائرة.

٢. إذا كان التدقيق خارجياً فإن التقارير ترفع فيه إلى مركز تكنولوجيا المعلومات الوطني.

ب- يجب أن يحتوي تقرير التدقيق على الأمور التالية:

١. مقدمة تشمل تحديد الأهداف الإجمالية لعملية التدقيق ومجاله، والمدة التي استغرقتها عملية التدقيق، والمكان الذي أجريت فيه عملية التدقيق، وطبيعة ومحددات إجراءات التدقيق التي تم اختبارها أثناء التدقيق.

٢. حدود وإطار التدقيق.

٣. استنتاجات ورأي المدقق في مدى تناسب الضوابط التي تم اختبارها أثناء التدقيق.

٤. ذكر الأسباب التي أدت إلى عدم تنفيذ خطة التدقيق بشكل كامل والحصول على استنتاجات صحيحة -إن وجدت-.

٥. النتائج التفصيلية والتوصيات.

٤ التوثيق والأدلة

يجب على الدائرة وضع التعليمات الخاصة بتوثيق عملية التدقيق على أن يشمل التوثيق العناصر التالية:

أ- التخطيط والتحضير لمجال وأهداف التدقيق.

ب- الوصف العام والتفصيلي لمجال التدقيق.

ج- برنامج التدقيق.

د- خطوات التدقيق التي تم إنجازها.

ه- الأدلة التي تم جمعها أثناء التدقيق.

و- الخدمات التي تم الاستفادة منها من المدققين والخبراء الآخرين.

ز- النتائج والاستنتاجات والتوصيات.

ح- نسخة من التقرير الذي تم طبعه من عملية التدقيق.

٥ ميثاق السلوك الخاص بتدقيق أمن المعلومات

على مدققي أمن المعلومات الالتزام بميثاق السلوك الأخلاقي الخاص بأمن المعلومات الذي أقره اتحاد إدارة وتدقيق نظم المعلومات العالمي ***ISACA*** والذي تم تلخيصه في النقاط الثمانية التالية:

أ- دعم تطبيق السياسات والمعايير والتوجيهات والإجراءات المناسبة لأمن وحماية نظم المعلومات، وتشجيع الدوائر على القيام بذلك.

ب- أداء الواجبات الموكولة للمدقق بشكل هادف وبعناية فائقة بقدر الاستطاعة، اعتماداً على المعايير المهنية المتبعة، ودعم العمل بأفضل الممارسات دون تحيز أو محاباة.

ج- تسهيل إنجاز مصالح المتعاملين مع الدائرة بشكل قانوني يعكس صورة مهنية عالية لمهنة التدقيق.

د- التعهد بالمحافظة على سرية وخصوصية المعلومات التي تم جمعها أثناء عملية التدقيق، وعدم استخدامها للمصلحة الشخصية. ويجوز الإفصاح عنها عند الحاجة للسلطات والجهات المخولة بذلك.

ه- لا يجب الشروع بالتدقيق سوى في المجالات التي يكون المدقق فيها مؤهلاً مهنياً بشكل كاف والتي يستطيع من خلالها إثبات كفاءته.

و- تقديم نتائج دقيقة لعملية التدقيق بأكملها واستخلاص الحقائق الهامة التي تم التوصّل إليها ورفعها إلى الجهات المخولة بذلك.

ز- دعم الجهود التوعوية التي تهدف إلى مساعدة المتعاملين مع الدوائر في تطوير فهمهم لأمن وإدارة نظم المعلومات.

ح- إن إخفاق المدقق في العمل بهذا الميثاق في أخلاقيات المهنة يمكن أن يؤدي إلى الشروع في تحقيق مع إمكانية إيقاع عقوبات رادعة وصارمة بحقه.

السياسة السادسة: سياسة الأمن المادي

أولاً: الهدف

ضمان أمن وسلامة الموارد المعلوماتية المادية في الدائرة وتقليل أثر المخاطر والتهديدات البشرية والبيئية التي تؤثر على سلامتها وسريتها.

ثانياً: المجال

تغطي هذه السياسة الموارد المعلوماتية المادية المملوكة للدائرة والأشخاص العاملين فيها والمتعاملين معها.

ثالثاً: تفاصيل السياسة

١ قواعد عامة

أ- يتم تقسيم الدائرة من الناحية الأمنية إلى ثلاث مناطق:

١. مناطق عامة: وهي المناطق التي يسمح لأي شخص بالتواجد فيها داخل الدائرة.

٢. مناطق محدودة: وهي المناطق الخاصة بموظفي الدائرة، ولا يسمح لأي زائر خارجي دخولها بدون صلاحية (أو بطاقة).

٣. مناطق آمنة: وهي المناطق التي لا يسمح فيها لأي شخص بالتواجد فيها، حتى من الموظفين والعاملين فيها، إلا بصلاحية أو موافقة مسبقة ومكتوبة من الإدارة العليا في الدائرة.

ب- على جميع العاملين في الدائرة والمتعاملين فيها تحمل مسؤولية الالتزام بالسياسات الوطنية لأمن وحماية المعلومات.

ج- لا يسمح بالتدخين أو الأكل أو الشرب داخل المناطق الآمنة.

د- لا يسمح بتركيب ونقل وصيانة الأجهزة بجميع أنواعها إلا بالتوافق مع تعليمات الدائرة وسياسة الاستعمال المقبول، وسياسة التغيير، وسياسة الحاسوب المكتبي.

٢ واجبات الدائرة

أ- وضع التعليمات الخاصة بتحديد المناطق الآمنة، والصلاحيات الممنوحة للأشخاص المسموح لهم بدخولها.

ب- وضع التعليمات الخاصة بالزوار، والصلاحيات الممنوحة لكل منهم في الوصول إلى مرافق الدائرة أو الموارد المعلوماتية داخلها، وكيفية مراقبة سلوك الزوار والإشراف على تحركاتهم داخل الدائرة.

ج- وضع التعليمات الخاصة بحماية مصادر الطاقة وتوفير مصادر طاقة احتياطية للخوادم بالتوافق مع سياسة أمن الشبكات.

د- وضع التعليمات الخاصة بأمن التمديدات - لكل من الشبكات المعلوماتية والاتصالات والتهوية والمياه والكهرباء – وخاصة في المناطق الآمنة.

ه- فصل التمديدات بجميع أنواعها عن بعضها بقدر الاستطاعة، لمنع التأثيرات السلبية لكل منها على الآخر، مع الحرص على عدم مرورها في المناطق العامة أو المكشوفة.

و- توفير واختبار ضوابط الدخول الخاصة بإطفاء الحرائق.

ز- إبعاد المواد القابلة للاشتعال أو الانفجار عن المناطق الآمنة بقدر الاستطاعة.

ح- استخدام وتوظيف ضوابط الأمن والحماية المناسبة للتأكد من خلو الداخلين إلى الدائرة من أية تهديدات تؤثر على أمنها وسلامة الموارد المعلوماتية داخلها، مثل توظيف حراس الأمن، وأجهزة كشف المعادن، وكاميرات المراقبة، وأجهزة الإنذار.

ط- استخدام الإشارات الإرشادية والتحذيرية لبيان الطريقة الصحيحة والآمنة في العمل، مع عدم استخدام أي إشارات أو لافتات تدل على الأماكن الحساسة مثل مراكز البيانات، وغرف المراقبة.

ي- الاحتفاظ بالوسائط والمعدات الاحتياطية في أماكن آمنة تكون في متناول اليد عند الحاجة حسب الآليات التي تحددها الدائرة.

ك- وضع التعليمات الخاصة بالدخول إلى الأقسام المختلفة في الدائرة، وتحديد الأشخاص المخولين بالاحتفاظ بالمفاتيح الخاصة بالأقسام والأبواب والغرف، وتمييز الأقسام الحساسة بضوابط دخول مناسبة، مثل بطاقات المرور.

ل- توظيف وسائل الحماية المناسبة لكل من النوافذ والأبواب والأقسام، مثل شبك الحماية على النوافذ، والأقفال على أبواب الأقسام.

م- توفير القاصات والخزائن والغرف القابلة للقفل والمضادة للحريق لحماية الموارد المعلوماتية الحساسة.

ن- توظيف مبدأ الحماية الطبقية في حماية الدائرة ومواردها المعلوماتية بما يتناسب وأهميتها.

٣ واجبات ضابط أمن المعلومات

أ- القيام بعملية التوعية الخاصة بالأمن الماديّ داخل الدائرة.

ب- التنسيق مع الجهات المعنية في الدائرة (وخارجها) في تطوير وتقييم وإعادة هيكلة إجراءات أمن وحماية المعلومات المطبقة في الدائرة، ورفع التوصيات الخاصة بذلك إلى الإدارة العليا في الدائرة.

ج- متابعة البلاغات والتقارير الخاصة بوقوع أية مخاطر أو تهديدات تتعلق بأمن المعلومات ومواردها، والتنسيق مع الجهات المعنية داخل الدائرة ومركز تكنولوجيا المعلومات الوطني في التعامل معها بطريقة تتوافق مع السياسات الوطنية لأمن وحماية المعلومات.

د- التدقيق على مدى توافق الضوابط والإجراءات الخاصة بالأمن المادي في الدائرة مع السياسات الوطنية لأمن وحماية المعلومات وخاصة سياسة الأمن الماديّ، ورفع التقارير الدورية للإدارة العليا في الدائرة.

ه- الإشراف والتدقيق على تطبيق التعليمات الخاصة بالأمن الماديّ داخل الدائرة.

٤ واجبات المستخدم

أ- تطبيق مبدأ المكتب النظيف وتأمينه عند المغادرة من خلال التأكد من إغلاق النوافذ والخزائن مثلاً.

ب- الابتعاد عن التدخين والأكل والشرب واستخدام المواد القابلة للاشتعال أو الانفجار داخل المناطق الآمنة.

السياسة السابعة: سياسة أمن الموظفين

أولاً: الهدف

منع و تقليل المخاطر الناتجة عن الخطأ البشري وسوء الاستعمال– مثل الإتلاف والتدمير – عند التعامل مع الموارد المعلوماتية.

ثانياً: المجال

تغطي هذه السياسة جميع الموظفين والعاملين في الدائرة بشكل دائم أو مؤقت، والموظفين والعاملين في الدائرة بسبب اتفاقية التعاقد الخارجي.

ثالثاً: تفاصيل السياسة

١ قواعد عامة

أ- هذه السياسة معنيّة بالجوانب الخاصة بأمن المعلومات عند تعيين وتقييم وإنهاء عقود الموظفين، والتي هي من مهام قسم الموارد البشرية بالتنسيق مع ضابط أمن المعلومات في الدائرة.

ب- على جميع الموظفين الالتزام بالسياسات الوطنية لأمن وحماية المعلومات عامة، وميثاق السلوك الخاص بأمن المعلومات وسياسة الاستعمال المقبول وسياسة كلمات المرور بشكل خاص.

ج- على جميع الموظفين الالتزام بالتعليمات الخاصة بالتعامل مع الزوار، مثل عدم تركهم لوحدهم، وعدم القدوم إلاّ بموعد، والتحقق من هوياتهم بشكل آمن وصحيح بالتوافق مع سياسة الأمن المادي.

٢ واجبات الدائرة (قسم الموارد البشرية)

أ- استخدام الموارد المشروعة والمتاحة للتحقق من الأشخاص الذين يراد تعيينهم في الدائرة والتأكد من مؤهلات كل منهم بقدر الاستطاعة.

ب- وضع وتحديد المهام المناطة بالموظفين آخذين بعين الاعتبار مبدأ "الفصل بين الوظائف" ومبدأ "المعرفة على قدر الحاجة"، وتحديد الواجبات التي يجب على الموظف أداؤها والمتعلقة بأمن وحماية المعلومات، وذلك بالتنسيق مع ضابط أمن المعلومات في الدائرة.

ج- إصدار بطاقات التعريف والمرور الخاصة بالعاملين في الدائرة، مبيناً عليها الاسم والصورة والوظيفة.

د- تجهيز تعهد "عدم الإفصاح عن المعلومات" للموظفين الجدد من أجل قراءتها والتوقيع عليها.

ه- توفير الوثائق المتعلقة بسياسات أمن وحماية المعلومات والتعليمات الخاصة بها للموظفين، ووضع نموذج تعهد من الموظفين بالالتزام بها.

و- وضع الإجراءات الإدارية المناسبة لبيان الآثار المترتبة على مخالفة كل من سياسات أمن وحماية المعلومات والتعليمات المعمول بها لأمن وحماية المعلومات في الدائرة.

ز- تطوير وتنفيذ ومراقبة برامج أمن وحماية الأشخاص في الدائرة.

٣ واجبات ضابط أمن المعلومات

أ- التوصية بمنح وحجب الصلاحيات المناسبة للوصول إلى الموارد المعلوماتية واستعمالها لكل وصف وظيفي على حدة اعتماداً على المهام والمسؤوليات الموكولة إلى الموظف.

ب- تقييم الموظفين في مدى تطبيقهم لسياسات أمن وحماية المعلومات والتعليمات الخاصة بها في الدائرة.

ج- تصميم وتطوير ووضع التوصيات الخاصة بضوابط الدخول الخاصة بأمن الموظفين والعاملين في الدائرة.

٤ واجبات الموظف

أ- توقيع تعهد "عدم الإفصاح عن المعلومات بشكل غير مرخص " عند التعيين.

ب- توقيع تعهد بأن الموظف قد قرأ وفهم سياسات أمن وحماية المعلومات المتبعة في الدائرة وأنه سيلتزم بها، وأنه يعي تماماً الآثار المترتبة على مخالفة وانتهاك سياسات أمن وحماية المعلومات.

ج- عدم تخطي الصلاحيات الممنوحة له في التعامل مع الموارد المعلوماتية في الدائرة.

د- عدم استغلال الموارد المعلوماتية في الدائرة لمنفعة أي جهة خارجية لغير غايات العمل الرسمي.

ه- عدم انتحال هويّات الموظفين الآخرين – عن طريق استعمال بطاقات مرورهم مثلاً – من أجل المنفعة الشخصية أو محاولة التسبب بإيذاء جهة ما أو منفعة جهة أخرى بشكل غير قانوني.

و- المحافظة على الموارد المعلوماتية في الدائرة من سوء الاستعمال أو أية تهديدات أو مخاطر محتملة، بقدر الاستطاعة والحذر، وبالتوافق مع سياسة الاستعمال المقبول.

ز- تعليق بطاقة التعريف التي تعبر عن هويته والصلاحيات المناطة به.

ح- تسليم كل ما بحوزته من بطاقات مرور ومفاتيح وكلمات مرور وأجهزة ووثائق عند إنهاء وظيفته أو سفره (أو مغادرته في إجازة) للجهة المسؤولة عن ذلك في الدائرة.

ط- التوقيع على تعهد للدائرة – عند إنهاء عقده – بأنه لا يحتفظ بأيٍّ من الموارد المعلوماتية المملوكة للدائرة وأنه يتحمل المسؤولية في حال ثبوت غير ذلك.

ي- عدم التعريف عن الوصف الوظيفي لأي جهة خارج الدائرة لغير ضرورة.

السياسة الثامنة: سياسة الحاسوب المكتبي

أولاً: الهدف

ضمان أمن وحماية الحاسوب المكتبي والمعلومات التي يتم التعامل معها أو تخزينها أو معالجتها من خلاله، وتوضيح الطريقة الصحيحة للتعامل معه بشكل آمن.

ثانياً: المجال

تغطي هذه السياسة جميع أجهزة الحاسوب المكتبية داخل الدائرة، وجميع المستخدمين الذين يسمح لهم باستعمالها أو الوصول إليها.

ثالثاً: تفاصيل السياسة

١ واجبات الدائرة

أ- وضع التعليمات المناسبة في التعامل مع أجهزة الحاسوب المكتبية المملوكة للدائرة، وشرائها وإصلاحها ونقلها وإتلافها، بالتوافق مع السياسات الوطنية لأمن وحماية المعلومات عامةً وسياسة حساسية وتصنيف المعلومات خاصةً.

ب- وضع التعليمات والآليات التي يتم بها توزيع أجهزة الحاسوب المكتبية على المستخدمين، وتحديد الصلاحيات المناطة بكل مستخدم على حدة حسب الحالة الوظيفية والوصف الوظيفي ووفق ما تقتضيه طبيعة العمل.

ج- وضع التعليمات الخاصة بتحديد وسائط التخزين التي يسمح باستخدامها، ووضع الضوابط والشروط التي تحدد استعمالها -مثل تشفير الملفات المخزّنة فيها مثلاً-.

د- وضع التعليمات الخاصة بربط أجهزة الحاسوب المكتبية بأية معدات -مثل البلوتوث والـ (واي-فاي) - أو بالشبكة المعلوماتية للدائرة بنوعيها السلكية واللاسلكية بالتوافق مع سياسة أمن الشبكات.

ه- التدقيق على جميع أجهزة الحاسوب المكتبية الموجودة فيها، بما فيها الأجهزة المشمولة باتفاقية التعاقد الخارجي مع أي مزود خارجي له أجهزة حاسوب مكتبية في الدائرة بالتوافق مع سياسة التدقيق الخاص بأمن المعلومات.

٢ واجبات مدير النظام

أ- إعداد أجهزة الحاسوب المكتبية في الدائرة بما يتوافق مع السياسات الوطنية لأمن وحماية المعلومات.

ب- القيام -أو الإيعاز لمن يلزم- بإصلاح أو نقل أو إحداث تغيير على أي جهاز حاسوب مكتبي، من تنصيب أو حذف أو تغيير لأي من القطع أو الإعدادات الخاصة به تبعاً لسياسة ضبط التغيير وسياسة الاستعمال المقبول.

ج- التعامل مع وسائط التخزين، مثل الأقراص الصلبة والمرنة والمضغوطة في حالة تغييرها أو نقلها أو إتلافها بالتوافق مع سياسة حساسية وتصنيف المعلومات.

د- توزيع أجهزة الحاسوب المكتبية داخل الغرف بشكل يحميها من اختلاس النظر بقدر الاستطاعة.

ه- ربط أجهزة الحاسوب المكتبية بالشبكة المعلوماتية في الدائرة وعزلها عنها، اعتماداً على الصلاحيات الممنوحة للمستخدمين.

و- إنشاء وحذف وإدارة سجلات الدخول الإلكترونية لكل جهاز حاسوب مكتبي، سواءً أكان متصلاً بالشبكة المعلوماتية أم لا.

ز- وضع كلمة مرور خاصة لحماية أجهزة الحاسوب المكتبية من دخول الأشخاص غير المخوّلين إلى إعدادات البيوس.

ح- تحديث البرمجيات ونظم التشغيل الموجودة على الأجهزة بشكل دوري، بالتوافق مع السياسات الوطنية لأمن وحماية المعلومات عامة، وسياسة مكافحة الفيروسات والبرامج الخبيثة، وسياسة الاستعمال المقبول خاصة.

ط- تنصيب حافظات شاشة موحدة للحواسيب المكتبية حسب تعليمات الدائرة.

ي- حماية حافظات الشاشة عن طريق استخدام كلمة مرور بعد ترك العمل على الأجهزة لفترة معينة.

ك- استخدام نظام ملفات آمن لحماية ملفات المستخدم، مثل نظام الملفات ***NTFS*** التابع لنظام تشغيل ويندوز.

ل- مراجعة ملفات تسجيل الحركات الخاصة بأمن المعلومات على الأجهزة عند إجراء تدقيق.

٣ واجبات المستخدم

أ- التعامل مع أجهزة الحاسوب المكتبية بشكل يتوافق مع سياسات أمن وحماية المعلومات وتعليمات الدائرة.

ب- المستخدم مسؤول عن حفظ كلمة المرور الخاصة بالدخول إلى حاسوبه المكتبي بالتوافق مع سياسة كلمات المرور.

ج- المستخدم مسؤول عن إبلاغ الدعم الفني بأي مشكلة تصيب حاسوبه المكتبي، وعليه عدم محاولة إصلاحه بنفسه بالتوافق مع سياسة الاستعمال المقبول.

د- عدم ربط أي جهاز أو وسيط تخزين أو معدات لاسلكية -مثل البلوتوث والـ (واي-فاي) - مع الشبكة المعلوماتية للدائرة، أو مع أي من الأجهزة والمعدات الأخرى، أو استخدام المودم، بدون الحصول على موافقة مسبقة ومكتوبة من الإدارة العليا في الدائرة.

ه- عدم إحضار أو ربط أجهزة الحاسوب المكتبية التي يملكها المستخدم بالشبكة المعلوماتية الخاصة بالدائرة.

و- عدم استخدام وسائط التخزين المتنقلة بدون فحصها ببرامج مكافحة الفيروسات.

ز- حفظ المعلومات والملفات على الأجهزة التي يحددها مدير النظام مثل خوادم الملفات بالتوافق مع سياسة أمن الشبكات.

السياسة التاسعة: سياسة الأجهزة المحمولة

أولاً: الهدف

ضمان أمن وحماية المعلومات التي يتم التعامل معها أو تخزينها أو معالجتها من خلال الأجهزة المحمولة أثناء استعمالها أو إصلاحها أو السفر بها.

ثانياً: المجال

تغطي هذه السياسة جميع الأجهزة المحمولة المملوكة للدائرة، مثل أجهزة الحاسوب المحمولة، وأجهزة الاتصال النقالة، والأجهزة المحمولة الأخرى مثل ***PDA*** و ***iPod*** و ***MP3 Player***، كما تغطي كافة الموظفين والعاملين الذين يستعملونها.

ثالثاً: تفاصيل السياسة

١ قواعد عامة

أ- على الدائرة وضع التعليمات الخاصة بمنح وحجب الصلاحيات الخاصة بتوزيع الأجهزة المحمولة على المستخدمين حسب الحالة الوظيفية والوصف الوظيفي ووفقاً لما تقتضيه طبيعة العمل.

ب- على الدائرة وضع التعليمات والآليات الخاصة بإدارة ومراقبة وحماية الأجهزة المحمولة المملوكة لها داخل وخارج الدائرة، وتحديد المعايير التي تحكم سلوك استخدام أجهزة الاتصال النقّالة، وحواسيب الجيب داخل الدائرة.

ج- لا يسمح باستخدام الأجهزة المحمولة الخاصة بالدائرة لمنفعة أي جهة أخرى أو لغير العمل الرسمي.

د- لا يسمح بربط أي جهاز محمول يملكه المستخدم بالشبكة المعلوماتية للدائرة أو أيٍّ من الموارد المعلوماتية للدائرة بدون موافقة مسبقة ومكتوبة من الإدارة العليا في الدائرة.

ه- لا يسمح بتخزين أو إخراج الملفات التي ينص القانون على عدم إخراجها من الدائرة على الأجهزة المحمولة –مثل وثائق العطاءات– حتى وإن كانت مشفّرة.

و- على الدائرة وضع التعليمات الخاصة بالتعامل مع الأجهزة المحمولة وحمايتها عند إخراجها خارج الدائرة.

٢ واجبات مدير النظام

أ- تطبيق معايير أمن وسلامة المعلومات التي يتم التعامل معها أو تخزينها أو معالجتها من خلال الأجهزة المحمولة المملوكة للدائرة بالتوافق مع السياسات الوطنية لأمن وحماية المعلومات عامةً، وكل من سياسة الحاسب المكتبي، وسياسة الاستعمال المقبول، وسياسة مكافحة الفيروسات والبرامج الخبيثة خاصةً.

ب- حماية الأجهزة المحمولة بكلمات مرور لكل من (البيوس) ونظام التشغيل.

ج- منح وحجب الصلاحيات المتعلقة باستخدام الأجهزة المحمولة وتغيير إعداداتها.

د- تشفير الملفات الموجودة على الأجهزة المحمولة المملوكة للدائرة بالتوافق مع سياسة حساسية وتصنيف المعلومات.

ه- إجراء عملية نسخ احتياطي للمعلومات المخزّنة على الأجهزة المحمولة بشكل دوريّ.

٣ واجبات المستخدم

أ- المستخدم مسؤول عن أية أعطال أو ضياع أو تغيير أو الإفصاح عن المعلومات بشكل غير مرخص يمكن أن يحدث للجهاز المحمول المملوك للدائرة سواءً عن طريقه أو عن طريق أي شخص آخر استخدمه بمعرفته أو لإهماله.

ب- حماية الأجهزة المحمولة المملوكة للدائرة والتي له صلاحية استخدامها بقدر الاستطاعة.

ج- عدم إحضار أو ربط الأجهزة المحمولة التي يملكها المستخدم بالشبكة المعلوماتية الخاصة بالدائرة.

السياسة العاشرة: سياسة كلمات المرور

أولاً: الهدف

حماية الموارد المعلوماتية من الدخول غير المشروع إليها عن طريق وضع معايير واضحة لإنشاء كلمات مرور فعّالة، وحمايتها وتغييرها بشكل دوري.

ثانياً: المجال

تغطي هذه السياسة جميع المستخدمين الذين لهم سجلات دخول إلكترونية داخل الدائرة، وآلية تصميم ومراقبة واستخدام كلمات المرور التي تستعمل لإثبات هوية المستخدم للنظام أو الملف أو الخدمة التي يريد الدخول إليها، مثل أجهزة الحاسوب الشخصية والمحمولة والخادمة، وسجلات البريد الإلكتروني، وسجلات الدخول الإلكترونية إلى الأجهزة والشبكات، والبرامج والنظم الإدارية والمالية.

ثالثاً: تفاصيل السياسة

١ قواعد عامة

أ- يجب حماية كلمات المرور وعدم الإفصاح عنها لأي سبب كان و بأي طريقة كانت، مثل كتابتها وتعليقها في مكان ظاهر، أو إعطائها للغير مشافهة أو بشكل مكتوب بطريقة إلكترونية أو غير إلكترونية.

ب- عند حدوث إفصاح لكلمات المرور أو دخول إلى الأنظمة بشكل غير مرخص، فإنه يجب إبلاغ مركز تكنولوجيا المعلومات الوطني للتحقيق في أسباب وآلية الإفصاح عنها أو الدخول إلى الأنظمة.

ج- يجب على الدائرة وضع تعليمات لحفظ نسخة عن كلمات المرور الخاصة بإدارة الأنظمة المحوسبة في الدائرة في معلّف خاص مغلق في خزنة أحد مسؤولي الإدارة العليا لاستخدامها عند حدوث طارئ بالتوافق مع سياسة النسخ الاحتياطي.

د- يجب أخذ الأمور التالية بعين الاعتبار عند اختيار كلمة المرور:

١. ألا تكون قد استخدمت مسبقاً من فترة قريبة.
٢. ألا تكون سهلة التخمين، مثل اسم الشخص، أو تاريخ ولادته، أو رقم هاتفه، أو اسم سجل الدخول الإلكتروني للمستخدم.
٣. ألا تكون من الكلمات المتداولة في القواميس أو اللغات المعروفة.
٤. ألا تكون مبنية بحيث تشكل في مجملها جملة واحدة كاملة من حروف وأرقام متتابعة ومتسلسلة بشكل منطقي ومعروف للعامة.
٥. أن تكون مركبة من الحروف والأرقام والرموز الخاصة، وبدون تكرار.
٦. أن تكون طويلة بشكل كاف.
٧. ألا تحتوي اختصارات معروفة مثل ***gov, MoJ, Sep***.
٨. أن يتم تغييرها بشكل دوري تحدده تعليمات الدائرة.
٩. عدم استخدامها في أكثر من نظام.

ه- يجب زيادة الالتزام بالتوجيهات السابقة كلما ازدادت حساسية كلمة المرور للدائرة.

و- تعامل كلمات المرور على أنها معلومات مصنفة، وتستمد حساسيتها من حساسية المعلومات للنظام المرتبط بها، وذلك لأغراض شمولها بسياسات أمن المعلومات وبخاصة سياسة النسخ الاحتياطي.

٢ واجبات مدير النظام

أ- حماية الموارد المعلوماتية من الدخول غير المشروع أو غير المخول عن طريق إعداد النظام لاستخدام وقبول كلمات المرور التي تحقق الشروط التي تم ذكرها أعلاه في هذه السياسة، ورفض كلمات المرور الضعيفة.

ب- التأكد من تشفير الملفات التي تحتوي على كلمات المرور.

ج- إعداد النظام لتجميد سجل الدخول الإلكتروني عند استخدام كلمة مرور خاطئة بشكل متتالٍ لعدد معين من المرات.

د- إعطاء كلمات مرور جديدة في حالة فتح سجل دخول إلكتروني لمستخدم جديد، وفي حالة نسيان أو فقدان كلمة المرور التي يستخدمها المستخدم حالياً، بعد التحقق من هوية المستخدم صاحب سجل الدخول الإلكتروني.

ه- حماية كلمات المرور المميزة التي قد يؤدي الإفصاح عنها بشكل غير مرخص إلى ضرر بليغ جدًّا بالدائرة ونظم المعلومات المستخدمة فيها، مثل سجل مدير النظام.

٣ واجبات المستخدم

أ- المستخدم مسؤول عن أي عمليات أو مراسلات تحدث عن طريق سجل الدخول الإلكتروني الخاص به سواءً عن طريقه أو عن طريق أي شخص استخدم كلمة المرور الخاصة بهذا المستخدم.

ب- حماية كلمة المرور من الإفصاح عنها بشكل غير مرخص والضياع.

ج- تغيير كلمة المرور على الفور عند الإفصاح عنها بشكل غير مرخص، سواءً بشكل متعمد أو غير متعمد.

د- تطبيق التوجيهات الخاصة بكتابة كلمات المرور والمذكورة أعلاه في هذه السياسة.

ه- عدم كتابة كلمات المرور أمام أي شخص يشاهد عملية الإدخال على لوحة المفاتيح.

و- عدم استعمال كلمات المرور الخاصة بالدائرة في مواقع الإنترنت التي لا علاقة لها بالعمل الرسمي إلا عندما يكون الاتصال بهذه المواقع آمناً بقدر الاستطاعة والحذر.

السياسة الحادية عشرة: سياسة مكافحة الفيروسات والبرامج الخبيثة

أولاً: الهدف

حماية الموارد المعلوماتية من أية تهديدات ناجمة عن الفيروسات أو البرامج الخبيثة.

ثانياً: المجال

تغطي هذه السياسة مكافحة جميع البرامج الخبيثة - من فيروسات وديدان وأحصنة طروادة والبرامج التجسسية والرسائل المزعجة والقنابل المنطقية وغيرها- والتي يمكن أن تهدد أمن وسلامة وإتاحية وخصوصية المعلومات ومواردها وأنظمة المعلومات المعمول بها في الدائرة.

ثالثاً: تفاصيل السياسة

١ قواعد عامة

أ- يجب تنصيب برامج موثوقة ومرخصة لمكافحة الفيروسات والبرامج الخبيثة على جميع أجهزة الحاسوب المملوكة للدائرة، من خوادم، وأجهزة محمولة، وأجهزة مكتبية، مع متابعة تحديثها بشكل مستمر.

ب- عند ظهور فيروسات لا تستطيع برامج مكافحة الفيروسات الكشف عنها والتخلص منها، فإنه يجب على الدعم الفني للدائرة الاتصال بالدعم الفني للمؤسسة صاحبة المنتج، ومحاولة مكافحة الفيروس بأنفسهم بأسرع وقت ممكن، مع إبلاغ مركز تكنولوجيا المعلومات الوطني بذلك.

ج- يجب مسح ***Scan*** الملفات المنقولة عبر شبكات الحاسوب للدائرة باستخدام برامج مكافحة الفيروسات، من أجل التأكد من خلوها من البرامج الخبيثة.

د- على الدائرة إجراء تقييم بين فترة وأخرى للتأكد من مطابقة برامج مكافحة الفيروسات وإعداداتها للسياسات الوطنية لأمن وحماية المعلومات.

ه- على الدائرة تطبيق الفقرات الخاصة بالتعامل مع البرامج الخبيثة في سياسة البريد الإلكتروني.

٢ واجبات مدير النظام

أ- إذا ترتب على أي إجراء يتعلق بمكافحة البرامج الخبيثة أي تغيير، فإنه لابد أن يخضع لعملية ضبط التغيير بهدف الحصول على الموافقة اللازمة من الإدارة العليا في الدائرة لإجراء هذا التغيير بالتوافق مع سياسة ضبط التغيير.

ب- تحديث برامج مكافحة الفيروسات والبرامج الخبيثة وملفات التعريف بشكل دوري وفقاً لآخر تحديث، تبعاً للتراخيص المرفقة مع هذه البرامج.

ج- عند عدم القدرة على تحديث برامج مكافحة للفيروسات – مثل انقطاع الاتصال بالإنترنت مثلاً - فلا بد من إيجاد حل بديل على الفور، بالتنسيق مع ضابط أمن المعلومات في الدائرة.

د- يجب مراقبة وتوثيق عمليات تحديث ملفات تعريف الفيروسات والبرامج الخبيثة.

ه- إغلاق المنافذ وحجب الخدمات التي لا حاجة للدائرة بها والموجودة على الخوادم، والتي تستخدمها البرامج الخبيثة عادة للتسلل إلى الأنظمة والوسائط، بالتوافق مع سياسة أمن الشبكات.

و- إجراء مسح كامل للأجهزة والأنظمة ببرامج مكافحة الفيروسات بين فترة وأخرى وبطريقة منتظمة حسبما يقره مركز تكنولوجيا المعلومات الوطني، للتأكد من خلو الموارد المعلوماتية المحوسبة من أية تهديدات تتعلق بالبرامج الخبيثة.

ز- عزل الأجهزة المصابة بالبرامج الخبيثة عن الشبكة لحين التأكد –وبشكل موثق- من خلوها من هذه البرامج الخبيثة.

ح- تطبيق سياسة النسخ الاحتياطي في حالة استرداد الملفات التي تم التخلص منها – إذا تعذر العلاج ببرامج مكافحة الفيروسات- والتأكد من خلو وسائط النسخ الاحتياطي من البرامج الخبيثة قبل استخدامها.

ط- حجب صلاحيات إيقاف وإزالة برامج مكافحة الفيروسات عن المستخدمين لضمان استمرارية وجود هذه البرامج وعملها بشكل صحيح وآمن، وعدم إعطاء فرصة للفيروسات والبرامج الخبيثة للدخول إلى الأنظمة وتخريبها.

٣ واجبات المستخدم

أ- العمل بالتوافق مع البند الخاص بالإنترنت في سياسة الاستعمال المقبول والخاص بالطريقة الصحيحة في تنزيل وتنصيب البرامج والملفات.

ب- تبليغ مدير النظام عن أي عمل من شأنه نشر الفيروسات أو المساعدة على نشرها.

ج- عند ظهور تحذير يدل على وجود فيروس أو برنامج خبيث فإنه يجب التوقف عن استخدام الجهاز وتبليغ مدير النظام على الفور.

د- عدم استخدام برامج غير مرخصة أو تجريبية فإنه لابد من الخضوع لعملية ضبط التغيير بهدف الحصول على الموافقة اللازمة من مدير النظام لإجراء هذا التغيير بما يتواءم وسياسة ضبط التغيير، تحسباً لوجود برامج خبيثة فيها.

ه- مراجعة الدعم الفني عند الشك في حدوث مشكلة تسببت بها الفيروسات، مثل ضعف أداء الجهاز، واختفاء وتغيير الملفات، بالتوافق مع البند الخاص بالدعم الفني في سياسة الاستعمال المقبول.

و- عدم استخدام وسائط التخزين إلاّ بعد التأكد من خلوّها من البرامج الخبيثة.

ز- عدم إرسال أو استقبال أو تنزيل أو نقل أية ملفات يُشك في أن تكون مصابة بالفيروسات أو البرامج الخبيثة عبر شبكات الحاسوب للدائرة.

ح- عدم تشغيل وسائط أو برامج يُشك في أنها تحمل في طياتها فيروسات أو برامج خبيثة.

٤ واجبات ضابط أمن المعلومات

أ- مراجعة طلبات التغيير المتعلقة ببرامج مكافحة الفيروسات والبرامج الخبيثة، والتي يتم رفعها ضمن عملية ضبط التغير.

ب- مساعدة الدعم الفني للدائرة في مكافحة الفيروسات والبرامج الخبيثة عند الحاجة.

ج- متابعة مواقع الإنترنت الخاصة بالتعريف عن الفيروسات وآليات عملها بشكل دوري من أجل الحصول على معلومات وافية عن آلية عمل الفيروسات والبرامج الخبيثة الجديدة والتحذير من آليات انتقالها، وتنزيل الأدوات الحديثة التي تم تطويرها للقضاء عليها، بقدر الاستطاعة والحذر.

د- نشر الوعي بين المستخدمين بكيفية انتشار الفيروسات والبرامج الخبيثة وبيان أخطارها والتحذير منها، وبيان الوسائط والأنظمة التي يمكنها أن تنتقل عبرها بسهولة.

السياسة الثانية عشرة: سياسة البريد الإلكتروني

أولاً: الهدف

ضمان أمن وسلامة وإتاحية وخصوصية رسائل البريد الإلكترونية عند الإرسال والاستقبال والحفظ والأرشفة.

ثانياً: المجال

تغطي هذه السياسة جميع الموارد المعلوماتية المشمولة بأنظمة البريد الإلكتروني المعمول بها في الدائرة، والمتعاملين مع هذه الأنظمة الذين لهم حق استعمالها، ولهم سجلات بريد إلكتروني عليها.

ثالثاً: تفاصيل السياسة

١ قضايا عامة

أ- لا يجوز التطفّل على سجل البريد الإلكتروني أو الدخول إليه إلا عن طريق صاحبه، باستثناء التدقيق المقنن في مثل الحالات التالية:

١. وجود أدلة على استخدام غير صحيح للسجل.

٢. احتواء السجل على محتويات تتعارض مع سياسة الاستعمال المقبول.

٣. وجود حكم قضائي.

ب- إن كافة المعلومات التي يتم تبادلها عبر الإنترنت من خلال الأجهزة والتسهيلات الخاصة بالدائرة هي ملك للدائرة وليست للمستخدمين، لذا فإن للدائرة الحق في تدقيق ومراقبة الجهة المستقبلة ومحتوى المراسلات كلما دعت الحاجة، وذلك من أجل حماية مصالح الدائرة.

ج- تشفّر رسائل البريد الإلكتروني باستخدام أي برنامج يوافق على توظيفه مركز تكنولوجيا المعلومات الوطني، بما يتوافق مع سياسة التشفير، والسياسة الوطنية لحساسية وتصنيف المعلومات.

د- لا يسمح باستخدام إعادة الإرسال بشكل آلي في الحالات التي تحمل فيها الرسالة معلومات مشفّرة.

٢ واجبات مدير نظام البريد الإلكتروني (مدير النظام)

أ- حماية نظام البريد الإلكتروني بشكل يضمن أمن الرسائل، بما يتوافق والسياسات الوطنية لأمن وحماية المعلومات عامة، وسياسة مكافحة الفيروسات والبرامج الخبيثة خاصة.

ب- تصميم وتطبيق خطة عمل مناسبة لإدارة نظام البريد الإلكتروني في الدائرة بشكل آمن.

ج- إنشاء وإلغاء سجلات البريد الإلكتروني وتحديد الصلاحيات الخاصة باستخدام نظام البريد الإلكتروني لهذه السجلات اعتماداً على الحالة الوظيفية والوصف الوظيفي.

د- القيام بعملية النسخ الاحتياطي للملفات والرسائل التي تمت أرشفتها من أجل ضمان وجودها عند حدوث طارئ، بما يتلاءم وسياسة النسخ الاحتياطي.

ه- توعية المستخدمين بخدمات البريد الإلكتروني التابعة للدائرة والاستخدام الصحيح والآمن لها.

و- منع إرسال الرسائل التسلسلية بين المستخدمين.

ز- حجب المرفقات الخطرة المتداولة عبر البريد الإلكتروني.

ح- وضع صيغة التنازل ***Disclaimer*** الخاصة بالدائرة في نهاية كل رسالة يتم إرسالها من المستخدمين.

٣ واجبات المستخدم

أ- العمل بالبند الخاص بالبريد الإلكتروني في سياسة الاستعمال المقبول

ب- عدم السماح للآخرين بالدخول إلى سجل البريد الإلكتروني الخاص به أو استخدامه بدون موافقة مدير الدائرة.

ج- التعامل مع الرسائل والملفات المنقولة حسب درجة تصنيفها (سريتها)، بما يتوافق مع سياسة حساسية وتصنيف المعلومات.

د- عدم إرسال معلومات مصنفة على أنها "سرية" أو "سرية للغاية" بدون تشفير.

ه- عدم إرسال أو استقبال أو إعادة إرسال أي بريد إلكتروني فيه محتوىً قد يشكّل خطراً على الأنظمة والموارد المعلوماتية مثل المحتويات الدعائية والبرامج الخبيثة.

و- عدم الرد على أي رسالة غريبة أو مشبوهة أو مجهولة المصدر.

السياسة الثالثة عشرة: سياسة النسخ الاحتياطي

أولاً: الهدف

ضمان أمن وحماية المعلومات عن طريق نسخها بشكل آمن ثم استرجاعها عند التلف أو الحاجة بطريقة آمنة وصحيحة.

ثانياً: المجال

تغطي هذه السياسة جميع الموارد المعلوماتية المشمولة بعملية النسخ الاحتياطي- مثل الوثائق والملفات الإلكترونية وغير الإلكترونية، وقواعد البيانات والبريد الإلكتروني، والبرمجيات والأجهزة ووسائط التخزين المستخدمة في النسخ الاحتياطي.

ثالثاً: تفاصيل السياسة

١ واجبات الدائرة

أ- توظيف البرمجيات والمعدات المناسبة للنسخ الاحتياطي لتعزيز أمن المعلومات المخزّنة واسترجاعها عند الحاجة إليها.

ب- وضع التعليمات وتحديد الآليات والإجراءات المناسبة لعملية النسخ الاحتياطي بما يتفق وهذه السياسة.

ج- عند إعداد تعليمات النسخ الاحتياطي، فعلى الدائرة أخذ التاريخ الزمني العائد للمعلومات المشمولة في النسخ الاحتياطية، والفترة الزمنية اللازمة (المسموح بها) لاسترجاع المعلومات في حالات الفشل والانقطاع وذلك ضمن إطار سياسة خطة استمرارية العمل.

د- وضع آليات آمنة لإتلاف وسائط التخزين أو مسحها عند إعادة استخدامها، بما يتلاءم وسياسة حساسية وتصنيف المعلومات.

ه- على الدائرة مراعاة سياسة التعاقد الخارجي عند توكيل جهات خارجية لحماية وسائط النسخ الاحتياطي.

و- وضع آلية واضحة لتخزين وسائط النسخ الاحتياطي في أماكن خارجية عند الحاجة.

٢ واجبات مدير النظام

أ- منح وحجب الصلاحيات اللازمة لإجراء عملية النسخ الاحتياطي أو استرجاع المعلومات.

ب- متابعة عملية النسخ الاحتياطي وعملية استرجاع المعلومات عند الحاجة للتأكد من أنها تتم بشكل صحيح وآمن.

ج- تشفير المعلومات المخزنة على وسائط النسخ الاحتياطي عندما تكون "سرية" أو "سرية للغاية" حسب سياسة حساسية وتصنيف المعلومات وسياسة التشفير.

د- وسم وسائط التخزين والنسخ الاحتياطي بدرجة حساسية وتصنيف المعلومات المخزنة داخلها وحمايتها في مكان آمن حسب وسمها بالتوافق مع سياسة حساسية وتصنيف المعلومات.

ه- تطبيق الجدولة المتبعة في الدائرة لعملية النسخ الاحتياطي.

و- مراعاة موضوع العدد وموضوع التوزيع الجغرافي المحلي والإقليمي في الحفظ المكاني للنسخ الاحتياطية اعتمادا على حساسية المعلومات المخزّنة.

ز- رفع تقارير دورية إلى الإدارة العليا في الدائرة حسب التعليمات المعمول بها في الدائرة تبين النقاط التالية:

١. تاريخ النسخة الاحتياطية.
٢. الموارد المعلوماتية التي تم نسخها احتياطياً.
٣. أسماء الأشخاص الذين لهم حق الوصول إلى المعلومات المخزّنة في وسائط النسخ الاحتياطي.
٤. أسماء الأشخاص الذين تمت لهم عملية استرجاع الملفات.
٥. تواريخ استخدام النسخ الاحتياطية.
٦. الأسباب التي دعت إلى استخدام النسخ الاحتياطية.

٧. الجهات والأماكن التي يتم حفظ وسائط النسخ الاحتياطي فيها.

٨. تاريخ بدء استخدام وسائط النسخ الاحتياطي وانتهاء صلاحيتها.

ح- يجب التأكد من كفاءة وكفاية العمر الافتراضي لوسائط التخزين قبل أخذ النسخ الاحتياطي للمعلومات عليها.

٣ واجبات ضابط أمن المعلومات

أ- التأكد من إجراء الاختبار والتقييم المناسبين للتأكد من أمن وسلامة المعلومات المخزنة على وسائط التخزين للنسخ الاحتياطية.

٤ واجبات المستخدم

أ- حفظ المعلومات والملفات على الأجهزة التي يحددها مدير النظام مثل خوادم الملفات والتي يتمّ نسخها احتياطياً بشكل دوري، ويُمنع حفظها على أية وسائط غيرها، مثل مواقع الإنترنت أو وسائط تخزين شخصية.

ب- التعامل مع وسائط التخزين والنسخ الاحتياطي التي قد تم وسمها حسب سياسة حساسية وتصنيف المعلومات.

ج- العمل بالتعليمات والإجراءات المتبعة في الدائرة عند طلب نسخ عن المعلومات والملفات المخزّنة على وسائط تخزين خارجية، بعد الحصول على الموافقة اللازمة من الجهة المعنية بذلك.

السياسة الرابعة عشرة: سياسة أمن الشبكات

أولاً: الهدف

تهدف هذه السياسة إلى توضيح كيفية التعامل مع عناصر الشبكة المعلوماتية بشكل آمن، وتحدد الأمور المطلوب توافرها في هذه المكونات لضمان أمن وحماية الأنظمة المربوطة على هذه الشبكات، من أجل الوصول إلى شبكة مستقرة وآمنة قادرة على تلبية متطلبات العمل الخاص بالدائرة.

ثانياً: المجال

تغطي هذه السياسة جميع العناصر والمكونات والموارد المعلوماتية المتعلق عملها بالشبكة المحلية والشبكة واسعة النطاق بنوعيها السلكية واللاسلكية؛ والتي تشكّل البنية التحتية للاتصالات، لتوفير تقنيات الاتصال المختلفة للمستخدمين.

ثالثاً: تفاصيل السياسة

١ واجبات الدائرة

أ- وضع التعليمات المناسبة في التعامل مع عناصر الشبكة المعلوماتية المملوكة للدائرة، وشرائها وإصلاحها ونقلها وإتلافها، بما يتفق مع السياسات الوطنية لأمن وحماية المعلومات عامةً وسياسة حساسية وتصنيف المعلومات وسياسة الاستعمال المقبول خاصةً.

ب- وضع التعليمات والضوابط الخاصة بربط عناصر الشبكة مثل الخوادم بأية معدات أو بالشبكة المعلوماتية للدائرة بنوعيها السلكية واللاسلكية.

ج- وضع التعليمات والآليات الخاصة ببيئة عمل هذه الأنظمة، مثل تشغيلها في أماكن آمنة وبعيدة عن أيدي المستخدمين، وتوفير بيئة مناسبة لها بالتوافق مع سياسة الأمن المادي.

د- وضع الصلاحيات المناسبة للأشخاص المتخصصين بتشغيل وصيانة وإدامة عمل الشبكات اعتماداً على الوصف الوظيفي لكل منهم.

ه- التوثيق الكامل للشبكات المعلوماتية للدائرة يشمل رسومات واضحة ومفهومة للشبكة تحدد عناصرها وطريقة ربطها بعضها ببعض.

و- تخزين الإعدادات الخاصة بأجهزة الشبكة في مكان آمن، من أجل توفير إمكانية إرجاع الإعدادات السابقة وذلك بالتوافق مع سياسة النسخ الاحتياطي.

ز- ترقية (تحديث وتطوير) نظم التشغيل في حال توجب ذلك، مثل حدوث اختراق أو خلل في عناصر الحماية الخاصة.

ح- وضع كلمات مرور سرية للدخول إلى الشبكة تعطى للأشخاص المخولين، وذلك بالتوافق مع سياسة كلمات المرور.

ط- التدقيق على جميع العناصر المكونة لهذه الأنظمة، بما فيها الأجهزة المشمولة باتفاقية التعاقد الخارجي مع أي مزود خارجي له أجهزة حاسوب مكتبية أو أية معدات ملحقة في الدائرة بالتوافق مع سياسة التدقيق الخاص بأمن المعلومات وسياسة التعاقد الخارجي.

ي- توفير الحد الأدنى لسرعة الشبكة واسعة النطاق، بحيث يتم ضمان قدرة هذه السرعة على تلبيّة متطلبات العمل الخاص بهذه الدائرة سواءً أكانت محلية أو واسعة النطاق.

ك- توفير الأجهزة التي تدعم حماية الشبكة الداخليّة مثل أنظمة كشف ومنع التطفل والاختراق، والجدران النارية أو أي جهاز أو تطبيق آخر يمكن أن يساعد على التخفيف من المخاطر التي تواجه الشبكة سواء كانت من الداخل أو من الخارج، ووفقاً لدرجة السريّة ومتطلبات العمل.

ل- في حال تزويد خدمات الربط عن طريق مزود خارجي فإنه يجب توقيع اتفاقية تتوافق مع سياسة التعاقد الخارجي.

م- مراقبة التزام الموظفين والمستخدمين بالسياسات الوطنية لأمن وحماية المعلومات عامة وسياسة الاستعمال المقبول ومدونة السلوك الخاص بأمن المعلومات خاصة في استخدام الشبكة بشكل صحيح وآمن.

ن- حفظ المعدات الاحتياطية للشبكة في مكان آمن لتكون متوافرة عند الحاجة.

٢ واجبات مدير النظام

أ- التأكد من توافق المواصفات المتعلقة بالأجهزة والتطبيقات الخاصة بالشبكات المعلوماتية في الدائرة مع السياسات الوطنية لأمن وحماية المعلومات، وبشكل يضمن إمكانية التوسع، والتحديث على الأجهزة والتطبيقات.

ب- توفير قوائم بعدد أجهزة الحواسيب والخوادم من أجل متابعة عددها، والمشاكل التي يمكن أن تطرأ بناءاً عليها لضمان حسن التنفيذ.

ج- التأكد من فتح المنافذ وتوفر خدمات الشبكات الضرورية فقط وإغلاق ما لا يحتاج إليه منها.

د- المحافظة على مستوى أداء ثابت للشبكة يعبر عن حالتها.

ه- ضبط الإعدادات الخاصة بالأجهزة الموجودة على الشبكات لتعمل بطريقة آمنة.

و- تنصيب وضبط ومتابعة تشغيل الأنظمة الخاصة بحماية الشبكة المعلوماتية للدائرة، مثل الجدران النارية، وأنظمة كشف ومنع التطفل والاختراق، وأنظمة مكافحة الفيروسات والبرامج الخبيثة، بالتوافق مع سياسة مكافحة الفيروسات والبرامج الخبيثة.

ز- إعداد البرامج والأجهزة الخاصة بتقنيات الحماية ضد الجاسوسية وذلك باستخدام بروتوكولات آمنة.

ح- التحكم بالأجهزة القادرة على الربط والوصول إلى أجهزة الدائرة المختلفة، عن طريق قوائم التحكم بالوصول.

ط- القيام -أو الإيعاز لمن يلزم- بإصلاح أو نقل أو إحداث تغيير في الإعدادات على أي جهاز أو تطبيق، من تنصيب أو حذف أو تغيير لأي من القطع أو الإعدادات الخاصة به تبعاً لسياسة ضبط التغيير وسياسة الاستعمال المقبول.

ي- مراقبة أداء الشبكات وأنظمة إدارتها أولاً بأول، ورفع التقارير الخاصة بها للإدارة العليا في الدائرة اعتماداً على سجلات الحركات الخاصة بتدفق المعلومات عبر الشبكات.

ك- متابعة ما يستجد من معلومات حول وجود أي ثغرات ضمن أنظمة التشغيل الخاصة بأجهزة إدارة الشبكة المعلوماتية للدائرة، والعمل على معالجتها وفقاً لكل جهاز وتطبيق، بناءاً على خطة عمل واضحة توافق عليها الإدارة العليا في الدائرة، لتحديد الأدوار، وتحديد التوقيت الملائم لتنفيذها بشكل يضمن عدم حدوث انقطاع للخدمة.

ل- تسهيل عمليات التدقيق على الأنظمة وقواعد البيانات ونظم التشغيل وأجهزة الموظفين والمستخدمين بالتوافق مع سياسة التدقيق الخاص بأمن المعلومات.

م- العزل الفيزيائي للأنظمة الحساسة التي تتطلب سرية كبيرة بشبكة منفصلة عن باقي أجزاء الشبكة المعلوماتية للدائرة، وفي حال وجود متطلبات خاصة لفئة معينة داخل الدائرة دون غيرها، فإنه يجب فصل "المجالات" فعلياً عن بعضها كذلك، بحيث يتم إعطاء صلاحيات لكل مجموعة بناءاً على الخوادم والموارد المسموح لهم بالعمل عليها، وتجهيز قوائم التحكم بالوصول للتأكد من أن تلك المجموعات تستطيع التواصل فيما بينها وفقاً لما يتفق عليه، وطبيعة عمل الدائرة.

ن- رفع تقارير دورية توضح المشاكل الأمنية الخاصة بأمن وحماية المعلومات التي تمت مواجهتها على الشبكة، من خلل أو اختراق أو انتشار للبرامج الخبيثة إلى الإدارة العليا في الدائرة.

٣ واجبات ضابط أمن المعلومات

أ- إجراء عمليات مراجعة وتدقيق بموافقة الإدارة العليا في الدائرة لتقييم مدى توافق النواحي الخاصة بأمن المعلومات على الشبكات مع هذه السياسة ومتابعة الجوانب الأمنية الخاصة بالشبكة المعلوماتية في الدائرة بالتعاون مع مدير النظام.

ب- متابعة التقارير الخاصة بالمشاكل الأمنية التي واجهتها أو تواجهها الشبكة المعلوماتية في الدائرة، والمساعدة في حلها.

٤ واجبات المستخدم

أ- عدم تغيير أو فك أو ربط أي جهاز بالشبكة المعلوماتية للدائرة، بدون الحصول على موافقة مكتوبة ومسبقة من الإدارة العليا في الدائرة، حسب سياسة ضبط التغيير وسياسة الحاسوب المكتبي وسياسة الأجهزة المحمولة.

ب- حفظ المعلومات والملفات على الأجهزة التي يحددها مدير النظام مثل خوادم الملفات.

السياسة الخامسة عشرة: سياسة تطوير وصيانة الأنظمة

أولاً: الهدف

ضمان تحقيق متطلبات الأمن والسلامة للموارد المعلوماتية أثناء دورة حياة تطوير الأنظمة والبرمجيات، والتأكد من أن هذه العملية تتم عن طريق الأشخاص المختصين والمخولين بذلك.

ثانياً: المجال

تغطي هذه السياسة التطبيقات وأنظمة المعلومات والبرمجيات التي يتم تطويرها، سواءً في داخل الدائرة أو عن طريق التعاقد الخارجي، والاعتبارات الواجب اتخاذها من أجل أمن وحماية هذه الأنظمة وسائر المعلومات المتعلقة بها أثناء دورة حياتها.

ثالثاً: تفاصيل السياسة

١ قواعد عامة

أ- تعتبر المخططات والدراسات المتعلقة بتحليل وتصميم أنظمة المعلومات والبرمجيات المراد تطويرها أو صيانتها، والبرمجية المصدرية، وكافة الملفات الخاصة بهذه الأنظمة والبرمجيات معلومات "سرية" ويتم التعامل معها بالاستناد إلى سياسة حساسية وتصنيف المعلومات.

ب- يجب التأكد من أن ضوابط الدخول الخاصة بالدخول والوصول إلى الملفات المتعلقة بالمشاريع كافية وآمنة من أجل المحافظة على سلامة المعلومات والأنظمة.

ج- لا يسمح بإجراء أي تغييرات على أنظمة المعلومات والبرمجيات المستخدمة إلا إذا دعت الحاجة لذلك، على أن يتم توثيق ذلك عن طريق عملية ضبط التغيير المتبعة في الدائرة، بالتوافق مع سياسة ضبط التغيير.

د- أي عملية تطوير للأنظمة يجب أن تكون موجهة بأهداف العمل ومدعّمة بدراسة جدوى متفق عليها، على أن تقع المسؤولية في ذلك على مسؤول العمل.

ه- يسمح بتطوير وشراء البرمجيات المطورة خصيصاً للدائرة عندما يتم ضمانها بدراسة جدوى فعّالة ومدعّمة.

و- يجب اختبار أي تغييرات خاصة بأنظمة المعلومات أو البرمجيات المستخدمة في الدائرة بطريقة صحيحة وآمنة من قبل المختصين في الدائرة قبل إقرارها ثم إطلاقها.

ز- لا يسمح باستخدام البيانات الحقيقية قيد الاستخدام ***Live Data*** عند اختبار الأنظمة قبل وضع ضوابط خاصة لضبط أمن هذه البيانات والمعلومات.

ح- يجب العمل بأنظمة المعلومات والبرمجيات المستخدمة في الدائرة بالتوازي مع الأنظمة والبرمجيات المطورة لحين التأكد من مطابقة الأخيرة لمتطلبات العمل ومتطلبات الأمن والحماية التي تم التطوير من أجلها.

ط- يجب إدارة مكتبات البرنامج المصدرية عن طريق عملية ضبط التغيير، والقيام بعمليات تقصي وتدقيق شاملة تشمل سجلات الحركات. بالتوافق مع سياسة التدقيق الخاص بأمن المعلومات.

ي- يجب التأكد من تطبيق التحديدات التي تعمل على تقليل درجة المخاطرة للأخطاء الناجمة عن المعالجة الداخلية لئلا تؤدي إلى التأثير سلباً على سلامة.

ك- يجب تقييم المخاطر الأمنية من أجل تحديد فيما إذا كانت رسائل التحقق مطلوبة ولتحديد الطريقة الأنسب لتطبيقها.

ل- يجب استخدام أنظمة التشفير لحماية المعلومات في حال احتمال تعرضها للمخاطر، وعند عدم وجود ضوابط دخول قادرة على حمايتها بشكل كاف، وذلك بالتوافق مع سياسة التشفير.

٢ واجبات الدائرة

أ- وضع الضوابط والتعليمات الخاصة بمراحل دورة حياة تطوير أنظمة المعلومات والبرمجيات المستخدمة في الدائرة بالتوافق مع السياسات الوطنية لأمن وحماية المعلومات عامة وسياسة التغيير وسياسة التعاقد الخارجي بشكل خاص.

ب- تحديد متطلبات الأمن والحماية المراد تحقيقها في أنظمة المعلومات والبرمجيات التي يراد استخدامها في الدائرة.

ج- تقييم المخاطر الناجمة عن تطوير أو صيانة أنظمة المعلومات والبرمجيات ودرجة تأثيرها على مستوى أمن وحماية المعلومات التي تعالجها أو تتعامل معها.

د- التأكد –بقدر الاستطاعة- من إغلاق وعدم وجود قنوات سرية أو برمجيات طروادة في أنظمة المعلومات والبرمجيات التي يتم تطويرها، من أجل المحافظة على سلامة وإتاحية المعلومات التي تتم معالجتها عن طريق هذه الأنظمة والبرمجيات.

ه- التأكد من تطبيق مبدأ "الفصل بين المهام" في جميع المجالات المتعلقة بتطوير الأنظمة وإدارتها والعمليات المتعلقة بها.

و- توفير التدريب والتوعية المناسبين للطاقم الفني والمستخدمين العاديين لتخطي المخاطر الناتجة عن استخدام الأنظمة والبرمجيات المطورة.

ز- التأكد من توفر متطلبات أمن وحماية المعلومات الخاصة بتطوير وصيانة الأنظمة والبرمجيات.

ح- اختبار تواجد وفعالية متطلبات أمن وحماية المعلومات المدخلة إلى الأنظمة – مثل التأكد من توافق صيغة المعلومات المدخلة مع الصيغة التي يحتاجها النظام من أجل المعالجة – والمخرجة منها – مثل اختبار صحة القيم المخرجة وصيغتها-.

ط- الموافقة على الانتقال من مرحلة إلى أخرى بعد التأكد من اكتمال المتطلبات والمواصفات الخاصة بأمن المعلومات فيها، واختبارها بشكل مناسب.

ي- التأكد من توثيق جميع الوثائق والدراسات والشيفرات المصدرية وخطط اختبار الأنظمة والبرمجيات بطريقة آمنة وصحيحة.

السياسة السادسة عشرة: سياسة التعاقد الخارجي

أولاً: الهدف

ضمان أمن وحماية المعلومات والموارد المعلوماتية وسلامتها وإتاحيتها وخصوصيتها أثناء الاستعانة بمزود خارجي لتوفير خدمات معينة للدائرة.

ثانياً: المجال

تغطي هذه السياسة أي مزود خارجي يتم التعاقد معه لتوفير خدمات معينة للدائرة، ويشمل ذلك المستشارين و محللي النظم و الباحثين و المبرمجين، و المؤسسات و الشركات الخادمة و المزودة و الداعمة، كما تغطي اعتبارات أمن وحماية المعلومات ومواردها، والإجراءات والعمليات والخدمات والاتصالات التي يتم التعاقد الخارجي من أجلها.

ثالثاً: تفاصيل السياسة

١ قضايا عامة

أ- تكون الاستعانة بمزود خارجي ناتجة عن اتفاقية موقعة مع جهة على درجة عالية من الكفاءة والأمان للقيام بمهمة التعاقد الخارجي بشكل آمن وصحيح وفعّال.

ب- يجب ألا تكون الخدمات المعلوماتية التي يراد الاستعانة بمزود خارجي من أجلها جوهرية وحرجة، إلا بعد موافقة مركز تكنولوجيا المعلومات الوطني.

ج- يجب ألا يؤدي التعاقد الخارجي -بقدر الاستطاعة والحذر- إلى انقطاع أو تأثير في استمرارية الخدمات المقدمة من الدائرة.

د- إذا كانت الخدمة التي سيتم التعاقد الخارجي من أجلها هي التدقيق على أمن المعلومات، فيجب موافقة مركز تكنولوجيا المعلومات الوطني.

٢ واجبات الدائرة

أ- تحديد وتوثيق توصيات جميع الأقسام التي لها علاقة بالخدمات التي سيتم الاستعانة بطرف خارجي من أجلها، وبخاصة قسم أمن وحماية المعلومات.

ب- يجب أن تكون جميع الموارد المعلوماتية المشمولة أو المتعلقة بالتعاقد الخارجي موثقة وخاضعة للتدقيق تبعاً للسياسات الوطنية لأمن وحماية المعلومات المعمول بها، وتبعاً للاتفاقية بين الدائرة والجهة المزودة، من خلال الآلية المتبعة في الدائرة في التدقيق، ورفع التقارير بذلك لمدير الدائرة.

ج- تحديد وتوثيق أسماء الموظفين المسؤولين في الدائرة عن التحضير للاعتبارات الأمنية، ومتابعة الإجراءات المتعلقة بأمن وحماية المعلومات ومواردها، وتقييم المخاطر الخاصة بالاستعانة بطرف خارجي.

د- تحديد وتوثيق آلية إعادة الموارد المعلوماتية ونقلها وإتلافها بطريقة آمنة عند انتهاء اتفاقية الاستعانة بالمزود الخارجي.

ه- تحديد وتوثيق أسماء الموظفين الذين سيباشرون بتزويد الخدمة من الطرف الخارجي وأية معلومات أمنية سابقة تتعلق بهم، والموافقة أمنياً عليهم قبل مباشرة أعمالهم، وأنهم يحققون شروط التوظيف والأمن اللازمة لتعيينهم حسب السياسة المتبعة في الدائرة، وبشكل خاص سياسة أمن الموظفين.

و- تحديد وتوثيق المعايير اللازمة لقياس ومتابعة وتقييم فعالية الإجراءات الأمنية الخاصة بالخدمات التي تم التعاقد الخارجي من أجلها، وخطوات مراقبة الحوادث الأمنية ورفع التقارير بشأنها.

ز- تحديد وتوثيق ضوابط الأمن والحماية اللازمة في إدارة ونقل وإتلاف المعلومات والخدمات وموارد ها ونقل وتبادل الموظفين.

ح- تحديد وتوثيق الشروط الجزائية والغرامات عن أي خلل ينتج عن المزود الخارجي في تقديم خدماته بشكل يخل بأمن المعلومات في الدائرة.

ط- تحديد وتوثيق جميع المؤهلات والمتطلبات والمهام والمسؤوليات اللازم تنفيذها من قبل المزود الخارجي.

ي- التأكد من تطبيق مبدأ "الفصل بين المهام" بين كل من الدائرة والمزود الخارجي.

ك- الدائرة مسؤولة عن أي تجهيزات أو أنظمة أو تعاقدات أو خدمات يزودها الطرف الخارجي، وعليها إنشاء نظام وآلية لإدارة ومتابعة فعالية هذه الخدمات .

ل- التحقق من مطابقة ممارسات وإجراءات الأمن والحماية التي يتبعها المزود الخارجي للسياسات الوطنية لأمن وحماية المعلومات، وتعديل ما يلزم منها لتوافق هذه السياسات.

٣ واجبات المزود الخارجي

أ- توقيع اتفاقية مستوى الخدمة.

ب- توقيع اتفاقية "عدم الإفصاح بشكل غير مرخص عن المعلومات" والمعنيّة بعدم إفصاح المزود الخارجي عن أي معلومات (هي ملك للدائرة) يطّلع عليها بحكم عمله.

ج- توقيع تعهد بأنه لا يحوز أياً من الموارد المعلوماتية المملوكة للدائرة، أو حق الوصول إليها، أو تغييرها، وأنه يتحمل المسؤولية عند أي إفصاح عنها بشكل غير مرخص يصيب هذه الموارد بعد انتهاء اتفاقية التعاقد الخارجي.

د- عدم تشفير أي من الخدمات أو الأنظمة أو المعلومات أو الاتصالات بدون معرفة مسبقة من الدائرة بآلية التشفير وفكه بنفسها، بالتوافق مع سياسة التشفير.

ه- توفير المؤهلات والكوادر والكفاءات والقدرات الكافية بطريقة مثبتة وموثقة للقيام بدور المزود الخارجي، وأن يكون متقدماً في المجال الذي سيتم التعاقد معه من أجله.

و- حماية الموارد المعلوماتية للدائرة بشتى الطرق الفيزيائية أو المنطقية التي تضمن سرية وسلامة وإتاحية وخصوصية المعلومات والخدمات المتعاقد من أجلها، بالتوافق مع السياسات الوطنية لأمن وحماية المعلومات وحسب الملائم، وذلك بقدر الاستطاعة والحذر.

ز- التزام عملية ضبط التغيير المعمول بها في الدائرة.

ح- تطبيق اعتبارات أمن وحماية المعلومات ومواردها أثناء التعامل مع المعلومات ومواردها، وعدم تعريض أمن وسلامة وإتاحية المعلومات ومواردها التي هي ملك للدائرة للخطر.

ط- التعاون مع أي عملية تدقيق تقوم بها الدائرة أو مركز تكنولوجيا المعلومات الوطني بالتوافق مع سياسة التدقيق الخاص بأمن المعلومات.

ي- تزويد الدائرة بخططه المتعلقة باستمرارية الأعمال والاسترداد عند وقوع كارثة تتعلق بالخدمات التي تم التعاقد الخارجي معه لتزويدها.

ك- تطبيق مبدأ "الفصل بين المهام" بين كل من الدائرة والمزود الخارجي.

ل- تحديد آلية اتصال متفق عليها مع الدائرة عند وقوع أي حادث أمني قد يؤثر على أمن وسلامة وإتاحية الخدمات التي تم التعاقد الخارجي من أجلها أو غيرها من الموارد المعلوماتية.

م- رفع وتوثيق تقارير مفصلة للدائرة عن الخدمات التي تم التعاقد الخارجي لتزويدها، على أن تشمل العناصر التالية:

١. إجراءات الأمن والحماية.

٢. الحوادث والخروقات الأمنية، وأية أخطاء قد تصيب الخدمات التي تم التعاقد الخارجي من أجلها أو غيرها من الموارد المعلوماتية، وكيفية معالجتها.

٣. أسماء الموظفين المسؤولين عن حماية هذه الخدمات والموارد المعلوماتية وأي تغييرات تتعلق بتعيينهم أو مسؤولياتهم أو كيفية الاتصال بهم، ومدى الصلاحيات الممنوحة لكل منهم بشكل دوري.

٤. الإجراءات المتبعة في استلام ونقل وإتلاف أية موارد معلوماتية مشمولة أو لها علاقة بالتعاقد الخارجي.

السياسة السابعة عشرة: سياسة التشفير

أولاً: الهدف

حماية المعلومات السرية عن طريق وضع الحدود الدنيا اللازمة لتطبيق خوارزميات التشفير التي تمت مراجعتها وإثبات فاعليتها واعتمادها عالمياً.

ثانياً: المجال

تغطي هذه السياسة إدارة واستخدام برامج ومعدات ومفاتيح التشفير للمعلومات السرية في الدائرة أثناء نقلها وتخزينها.

ثالثاً: تفاصيل السياسة

١ واجبات الدائرة

أ- استخدام خوارزمية تشفير مثبتة ومعتمدة عالمياً من إحدى الخوارزميات التالية: ***RSA, DES, Blowfish, RC5, IDEA***، أو أية خوارزميات يتم الموافقة عليها من قبل الجهة المختصة لاحقاً.

ب- توظيف وتنصيب البرمجيات والبروتوكولات والمعدات المناسبة لتطبيق خوارزميات التشفير المعتمدة في الدائرة.

ج- تشفير جميع وسائط التخزين والاتصالات التي تحتوي معلومات سرية بالتوافق مع سياسة حساسية وتصنيف المعلومات.

د- وضع التعليمات المناسبة التي تضمن إجراء عملية التشفير وفك التشفير بطريقة آمنة وصحيحة.

ه- تحديد وتوثيق أسماء الأشخاص المخولين الذين يجب أن تصرف لهم مفاتيح تشفير وبرامج تشفير حسب متطلبات أعمالهم.

و- وضع التعليمات التي تحدد كيفية التعامل مع الوثائق والملفات التي تم فقدان أو الإفصاح عن مفاتيح تشفيرها أو فك تشفيرها بشكل غير مرخص.

ز- وضع التعليمات الخاصة بإدارة مفاتيح التشفير، على أن تراعى فيها الأمور التالية:

١. حفظ نسخ احتياطية عن مفاتيح التشفير الخاصة بالدائرة في مكان آمن لاستعمالها عند الحاجة.
٢. مواصفات الأنظمة والبرمجيات المستخدمة في إدارة مفاتيح التشفير طوال دورة حياتها.
٣. اعتماد أو إلغاء اعتماد مفاتيح التشفير -عند الإفصاح عنها بشكل غير مرخص أو استقالة الموظف مثلاً- .
٤. الحدود الدنيا لأطوال مفاتيح التشفير.
٥. مدة صلاحية المفاتيح.
٦. إدارة مفاتيح التشفير داخل الدائرة بشكل آمن.

٢ واجبات مدير النظام

أ- تنصيب وضبط وتشغيل وتحديث برامج التشفير المعتمدة في الدائرة والتأكد من أنها تعمل بشكل آمن وصحيح.

ب- التعاون مع ضابط أمن المعلومات في إدارة مفاتيح وبرامج التشفير داخل الدائرة.

٣ واجبات ضابط أمن المعلومات

أ- تدريب الموظفين على كيفية استعمال برامج ومفاتيح التشفير المعتمدة في الدائرة.

ب- التأكد من أن التشفير يتم بشكل بطريقة صحيحة وآمنة اعتماداً على صلاحيات المستخدمين.

ج- التدقيق على الالتزام بعملية التشفير تبعاً لهذه السياسة ورفع التقارير لمسؤولي الدائرة عن أية تجاوزات أو مشاكل تتعلق بالتشفير.

٤ واجبات المستخدم

أ- عدم استخدام برامج تشفير أو فك تشفير أو مفاتيح تشفير لم تصرف له من الدائرة.

ب- تشفير المعلومات المصنفة على أنها "سرية" أو "سرية للغاية" أثناء نقلها وتخزينها بالتوافق مع هذه السياسة وسياسة حساسية وتصنيف المعلومات.

ج- المحافظة على سلامة وسرية مفاتيح التشفير المصروفة له من الدائرة.

د- مراجعة الدعم الفني عند وجود أية مشاكل تتعلق باستخدام برامج أو مفاتيح التشفير المصروفة له من الدائرة.

ه- رفع تقرير إلى ضابط أمن المعلومات ومدير النظام عند الشك في سوء استعمال مفاتيح التشفير أو برامج التشفير.

لقد تمت مناقشة ومراجعة السياسات الوطنية لأمن وحماية المعلومات والموافقة على ما فيها بهذا الشكل من قبل اللجنة الوطنية الفنية لأمن وحماية المعلومات وهم:

الرقم	الجهة	ممثل الجهة	التوقيع
١	وزارة الاتصالات وتكنولوجيا المعلومات	المهندس أيمن غنوم	
		المهندس مازن الخطيب	
٢	وزارة الداخلية	السيد إياد صويص	
٣	وزارة العدل	السيد محمد اللحام	
٤	هيئة الأركان المشتركة	العميد نايل المدادحة	
٥	هيئة تنظيم قطاع الاتصالات	السيد نرت كوف	
٦	مديرية الأمن العام	العقيد بسام روبين عودة	
		الرائد نزيه خليفات	
٧	دائرة المخابرات العامة	العقيد أمين العمد	
٨	المركز الوطني للأمن وإدارة الأزمات	الرائد محمد عبابنة	
٩	مركز تكنولوجيا المعلومات الوطني	المهندس نادر الذنيبات	
١٠	البنك المركزي الأردني	السيد زيد الطراونة	