وثيقة سياسات ومعايير أمن المعلومات والبيانات

أعداد اللجنة الفرعية لكتابة السياسات والمعايير المشكلة من قبل لجنة (تنسيق وإدارة النشاط الحكومي باتجاه انشاء الحوكمة الالكترونية) – الإصدار ٠,٩ أيار ٢٠١٩

تمهيد

استكمالاً لما تم إنجازه من قبل اللجنة المختصة بـ (تنسيق و إدارة النشاط الحكومي باتجاه انشاء الحوكمة الالكترونية) المؤلفة بموجب الامر الديواني رقم (٤٥) لسنة ٢٠١٦ تم تشكيل اللجنة الفرعية المكلفة بكتابة سياسات ومعايير أمن المعلومات و البيانات وذلك بالأمر المرقم ٤٥١٧٥ الصادر عن الأمانة العامة لمجلس الوزراء / دائرة شؤون مجلس الوزراء و اللجان بتاريخ ٢٠١٨/١٢/٣١ وعليه تم اعداد هذا الوثيقة من قبل اللجنة الفرعية تلبية لالتزاماته المحددة بالأمر اعلاه.

أعضاء اللجنة

رئيس اللجنة	مراد عبد الصمد هادي
مقرر اللجنة	عمر علي عبد الرحيم
النموذج الاولي	ذر كاظم علي
أعضاء اللجنة	مراد عبد الصمد هادي
	ذر كاظم علي
	محمد جمال
	محمد هاشم عمر
	علي محمد علي عرفات
	زياد صباح عابر
	احمد قيس عبد اللطيف
	حيدر قحطان كشاش
	عمر علي عبد الرحيم
	عادل محمود شاكر
	عماد سعدون جابر
	حسن علي حسون
	مصطفى عبد الصمد هادي
	انمار مازن عبد الكريم
	هند رعد جاسم
ألية المصادقة على هذه الوثيقة	
تعرض وتصادق من قبل لجنة تنسيق و إدارة النشاط الحكومي باتجاه انشاء الحوكمة الالكترونية	
تعرض وتصادق من قبل اللجنة الفنية العليا لأمن الاتصالات والمعلومات	
تعرض وتصادق من قبل مجلس الأمن الوطني	
تعرض وتصادق من قبل رئاسة الوزراء	

الهدف

تهدف هذه الوثيقة إلى وضع أطر العمل، و وضع السياسات والمعايير وتحديد الأدوار والمسؤوليات، وبيان الالتزام الأدنى المطلوب من جميع العاملين داخل المؤسسة لضمان أمن وحماية المعلومات التي يتعاملون معها على أي صورة كانت سواءً صور 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، مرورًا بنقلها ومعالجتها وتخزينها، وانتهاءاً بأتلافها بشكل أمن وصحيح.

إن الالتزام الصحيح بالعمل بهذه السياسات و المعايير يؤدي إلى تحقيق المستويات المقبولة من أمن وحماية المعلومات ، مما يعزز الثقة بين المواطنين والحكومة بأن معلوماتهم وتعاملاتهم الإلكترونية وغير الإلكترونية ستكون بأمان ومعزل عن أية مخاطر أو تهديدات قد تؤثر على سلامتها وسريتها وتوافرها قدر الامكان، كما يعزز الثقة المتبادلة بين المؤسسات الحكومية المختلفة والمتعاملين معها في تبادل المعلومات بشكل أمن، ويسهل من تطبيق آليات أمن وحماية المعلومات في الخدمات المشتركة والمتبادلة بينها.

ملخص وثيقة سياسات ومعايير أمن المعلومات والبيانات

تعد سياسات و معايير أمن المعلومات و البيانات وثيقة شاملة أساسيةً توضح أطر العمل، وتحدد الأدوار والمسؤوليات، وتبين الممارسات الفضلى والالتزام الأدنى المطلوب مراعاته والعمل به من قبل العاملين داخل المؤسسة وعلى اختلاف درجاتهم و فئاتهم ومناصبهم من أجل تحقيق أمن وسلامة وتوافرية المعلومات التي يتم تداولها بين المؤسسات الحكومية والمواطنين والمؤسسات الخاصة على حد سواء.

بشكل عام تقسم كل سياسة في هذه الوثيقة إلى ثلاثة أقسام رئيسية:

١. الهدف: يوضح الأهداف الرئيسة التي ترمي كل سياسة إلى تحقيقها.

٢. المجال: يحدد نطاق تطبيق هذه السياسة.

٣. تفاصيل السياسة: توضح الأدوار والواجبات المناطة بكل من المؤسسات الحكومية والمتعاملين معها المشمولين بمجال السياسة.

تنويه

- تحقق هذه السياسات الحدود الدنيا الواجب العمل بها في كافة المؤسسات الحكومية والمؤسسات المتعاملة معها، وللمؤسسة أن تضيف ما تراه ملائمًا حسب طبيعة وظروف عملها و حسب ما تقتضيه مصلحة العمل و وضع التعليمات الخاصة بها لتطبيقها، وتطوير اجراءاتها الداخلية بصورة تكون داعمة لهذه السياسات والمعايير، لتعزيز مستوى أمن وحماية المعلومات داخل المؤسسة إلى أعلى مستوىً ممكن.
- نظرا للتطور الحاصل في عالم تكنولوجيا المعلومات فان هذه الوثيقة عرضة للتحديث والتعديل استجابة للمستجدات الحاصلة . وعليه تم انشاء موقع الكتروني يحتوي على النسخة النهائية المحدثة من هذا الوثيقة ويجب على كل المعنين والمهتمين بمتابعة و تطبيق هذه السياسات في مؤسساتهم التسجيل في قائمة البريد الموجودة في موقع السياسات لتصلهم التحديثات باستمرار.
- تطبق هذه السياسات مع مراعاة القوانين والتشريعات العراقية السارية إضافة الى استراتيجية الأمن السيبراني العراقي.

محتويات الوثيقة

الفصل الأول : التعاريف

ت	المصطلح	التعريف
	المعلومات	هي البيانات التي تم معالجتها و تحويلها من اشكالها الخام المختلفة مثل الاحرف و الارقام والصور...الخ , الى بيانات مبوبة و مرتبة ليتم استخدامها في بعد في مختلف المجالات.
	البيانات	هي مجموعة الحقائق والقياسات والمشاهدات التي تكون على شكل أرقام وحروف ورموز وأشكال خاصّة، تختصّ بفكرة وموضوع معيّن، والبيانات لا يكون لها معنى، ولهذا يتم تجميعها حتى يتم استخدامها.
	نظام المعلومات	نظام يتكون من أشخاص، وسجلات البيانات، وعمليات يدوية وغير يدوية، ويقوم هذا النظام بمعالجة البيانات والمعلومات
	أمن المعلومات	هو العلم الذي يهدف الى حماية المعلومات بكافة اشكالها مستخدما التقنيات والوسائل و الاجراءات اللازمة للحفاظ عليها من المخاطر كالتحريف و الضياع بما يهدد الامن الوطني و القومي للخطر.
	المؤسسة	هي الوزارة او الهيئات المستقلة و اي تشكيل تابع لها و تشمل كذلك الشركات الاهلية المشمولة بهذه السياسة.
	العاملون	هم الموظفون العاملين في المؤسسة بمختلف الاصناف مثل الملاك الدائم و العقود و الاجور اليومية و غيره.
	استراتيجية الأمن السيبراني العراقي	و هي وثيقة الاستراتيجية الوطنية للأمن السيبراني التي تمثل خريطة طريق للمضي قدما نحو تعزيز الأمن السيبراني في العراق وتتلخص رؤية الاستراتيجية في خلق وتعزيز فضاء إلكتروني آمن لحماية المصالح الوطنية لدولة العراق والحفاظ على الحقوق والقيم الأساسية للمجتمع . مجموعة من الاجراءات و الوسائل لحماية البنى التحتية للمعلومات الحيوية الوطنية وتوفير بيئة آمنة لمختلف القطاعات لتقديم خدمات إلكترونية متكاملة وآمنة و لتوفير هيكل حوكمة للتعامل مع قضايا الأمن السيبراني.
	الفريق الوطني للاستجابة للأحداث السيبرانية	و هو فريق من المتخصصين مهامه وقاية و حماية البنى التحتية للمعلومات الحيوية الوطنية و معالجة الخروقات الامنية و توفير الدعم و الاسناد الفني للجهات الحكومية و الاهلية في مجال امن المعلومات
	مدير النظام	هو متخصص في مجال تقنية المعلومات تكون مهامه ادارة نظام تقنيات المعلومات و هو المسؤول عن الإشراف على عمل الإدارة و المشاركة في رسم السياسات العامة ووضع الاستراتيجيات الخاصة بتقنية المعلومات، وتوفير الدعم التقني اللازم لتطوير الاداء المؤسسي
	مدير امن المعلومات	هو موظف مسؤول عن امن المعلومات في كل مؤسسة حكومية و يكون ارتباطه الفني بالفريق الوطني للاستجابة الالكترونية لضمان تطبيق معايير امن المعلومات والالتزام بتطبيق كافة التعليمات التي تضمن حماية بيانات المؤسسة من خطر الضياع و التخريب والتسريب. ويتم تكليفه بعد اجراء المقابلات و استحصال موافقة فريق الاستجابة الالكترونية الوطني واكمال اجراءات التصريح الامني بمستوى (سري للغاية) مع استمرار التدقيق الدوري.
	المخاطر	و هي كل تهديد يستهدف اي مورد من موارد المعلومات

	منسق مشاركة البيانات	و هو الموظف المسؤول عن التنسيق بين جهات مالكة المعلومات و الجهات طالبة المعلومات
	المصدر المفتوح	هي البرمجيات التي تكون فيها شيفرات البرامج متاحة بدون قيود الملكية الفكرية .وهذا يتيح لمستخدمي البرمجيات الحرية الكاملة في الاطلاع على الشيفرة البرمجية للبرامج، وتعديلها أو إضافة مزايا جديدة لها ويمكن تحديثه بشكل مستمر عكس المصادر المغلقة
	مغلقة المصدر	و هي البرمجيات التي لا يمكن الاطلاع على شيفراتها البرمجية الا لأشخاص محددين و اصحاب الترخيص الخاص بها
	حوادث امن المعلومات	حدث أمان المعلومات هو حدث محدد لنظام أو خدمة أو حالة شبكة تشير إلى حدوث خرق محتمل لسياسة أمان المعلومات أو فشل الضمانات أو موقف غير معروف مسبقًا قد يكون ذا صلة بأمن المعلومات. يشار إلى حادثة أمن المعلومات من خلال واحدة أو سلسلة من أحداث أمن المعلومات غير المرغوب فيها أو غير المتوقعة التي لديها احتمال كبير من المساس بالعمليات التجارية أو تهديد أمن المعلومات.
	ضوابط ادارة حوادث أمن المعلومات	تضمن عناصر التحكم في إدارة الحوادث جميع الأنشطة التي تضمن تطبيق نهج متسق وفعال لإدارة حوادث أمن المعلومات.
	الاتلاف	عملية التخلص من المعلومات ومواردها بطريقة فيزيائية او منطقية.
	اصول المعلوماتية	اية معلومات او ملفات (الكترونية او غير الكترونية) او أجهزة او وسائط تخزين او تسهيلات او اشخاص لهم علاقة بعملية تبادل المعلومات ومعالجتها.
	التوافر	التأكد من ان أنظمة المعلومات سوف تبقى متوفرة وان البيانات الضرورية متوفرة او يمكن استرجاعها لاستخدامها عند الحاجة اليها .
	الارشفة	عملية حفظ المعلومات و البيانات بجميع صورها والمرفقات القديمة بشكل منظم على وسائط تخزين في مكان معروف وامن .
	الامتيازات الدنيا او الأقل	مبدا في امن وحماية المعلومات ينص على منح المستخدمين اقل عدد ممكن من الامتيازات والصلاحيات اللازمة لإنجاز العمل المطلوب حسب الوصف الوظيفي
	البريد الالكتروني	الحساب الذي يعطي للمستخدم ضمن نظام البريد الالكتروني لتمكينه من ارسال واستقبال الرسائل والملفات الالكترونية بشكل فريد .
	التحكم بالوصول	القواعد والاليات المستخدمة لتقييد الدخول الى ملكية ما او الوصول الى موارد المعلومات ..... الخ و الاشخاص المخولين فقط .
	التدقيق	هي عملية تقييم تحت ظروف ومعايير خاصة ومدروسة والتي تهدف الى معرفة مدى تقيد عملية او نظام مع معايير او سياسات معينة .
	التشفير	عملية تحويل المعلومات من شكل مقروء صريح الى شكل غير صريح و مبهم لضمان السرية.
	التغيير	أي تعديل يتم اجراءه على الأجهزة او البرمجيات او أي من مكوناتهما او الإجراءات المعمول بها في المؤسسة .
	الجدار الناري	أجهزة امن وحماية بنوعيها البرمجية Software والمادي Hardware تحدد وتقلل من القدرة على اختراق الأنظمة المعلوماتية او الوصول اليها من خلال منع وصول الخدمات غير المعتمدة بين الشبكات المعلوماتية والسماح للخدمات المعتمدة حسب الوصول .
	الخوادم	هو عبارة عن جهاز حاسوب كبقية الأجهزة لكنه ذو مكونات عالية القدرة و الكفاءة ، و تتمثل مهمته الرئيسية في إدارة الموارد المعلوماتية الموجودة على الشبكة مثل أجهزة الحاسوب والآلات الطابعة و الهواتف إلخ. ومتخصص في أداء وظيفة معينة وتلبية الطلبات التي ترده من الموارد المعلوماتية على الشبكة.
	السرية	التأكد من ان المعلومات يتم التعامل معها من قبل الجهات المخولة بذلك فقط .
	السلامة	التحقق من المعلومات التي يتم التعامل معها بانه لم يطرا عليها زيادة او نقص او تغيير بشكل غير مرخص.

	الصلاحيات	هي الاذونات الممنوحة للمستخدمين للدخول و استخدام الموارد المعلوماتية وفقا للحقوق والتراخيص الممنوحة للمستخدم فقط .
	المعلومات المصنفة	أي معلومات شفوية او وثائق مكتوبة او مطبوعة او مختزلة او مخزونة الكترونيا او باي طريقة او المطبوعة على الورق او اشرطة تسجيل او الصور والأفلام او المخططات الو الرسوم والخرائط او ما شابه والمصنفة على انها سرية او وثائق محمية وفق احكام التشريعات النافذة .
	المكتب النظيف	مبدا من مبادى الامن والحماية ينص على عدم ترك اية معلومات او وثائق على المكتب بشكل مكشوف للمحافظة على امنها و سلامتها .
	النسخ الاحتياطي	عملية نسخ المعلومات على وسائط وتخزين من اجل استرجاعها عند التلف او الضياع او الحاجة .
	الوسم	العملية التي تهدف الى بيان مستوى تصنيف المعلومات من اجل التعامل معها بشكل امن وصحيح.
	أمن البيئة المادية	معايير واجراءات الحماية التي تراقب او تحدد الدخول الى اي مرفق او موارد المعلومات مخزونة على وسائط فيزيائية بدون صلاحية او لمنع التماس المباشر مع الموارد المعلوماتية والانظمة مثل المباني وخزائن الملفات والاجهزة المكتبية والخادمة والمحمولة والمعدات
	أنظمة كشف ومنع التطفل والاختراق	أنظمة برمجية تعمل على مراقبة نشاط النظام او الشبكة المعلوماتية باستخدام تقنيات مختلفة تقوم بالكشف عن اية هجمات على الشبكة و منعها.
	برامج مكافحة الفيروسات	برامج صممت خصيصا للكشف عن وجود الفيروسات التي هي نوع من البرامج الخبيثة والقضاء عليها والحجر على الملفات التي تمت اصابتها بفيروسات لحين معالجتها لاحقا .
	بقدر الاستطاعة	مبدا في امن وحماية المعلومات ينص على بذل اقصى الجهود الممكنة في حماية الموارد المعلوماتية في المؤسسة لتطبيق مبدا بقدر الحذر .
	تصنيف المعلومات	عملية ترتيب مستوى الحساسية المناسبة للمعلومات التي يتم انشاؤها او تغييرها او نقلها او تعديلها او حفظها على أي وسائل كانت وبأية تقنيات ممكنة من اجل تحديد المستوى المطلوب لحمايتها والتحكم بالوصول اليها بشكل امن.
	دراسة الجدوى	دراسة الجدوى هي الأساس لأي مشروع وهي تؤسس بمصطلحات التجارة والاعمال – الاحتياجات والتقييم والبدائل المقترحة لتحقيق هدف استراتيجي او هدف متعلق بالعمل .
	سجل الدخول	مصطلح يصف غالبا معلومات المستخدم التي تسمح له بالدخول الى الأنظمة المحوسبة كما يمكن ان يشار اليها أحيانا انها عملية الحصول على حق الوصول من خلال الشبكات الى الطابعات وأنظمة الارشفة وقد يعني أحيانا تطبيق امتيازات خاصة للتحكم بمستوى وصول المستخدم الى موارد النظام بشكل فريد .
	سياسة امن وحماية المعلومات	وثيقة معتمدة تقرها الإدارة العليا للدائرة توضح وتحدد أدوار العاملين فيها في كيفية التعامل مع الموارد المعلوماتية للدائرة بطريقة امنة وصحيحة.
	ضبط التغيير	إدارة وضبط أي تغيير يحدث على الأنظمة المستخدمة ومكوناتها او الأجهزة المختلفة ومكوناتها او الإجراءات والتعليمات المتبعة في المؤسسة .
	عملية ضبط التغيير	الإجراءات والعمليات المتبعة في المؤسسة لطلب الموافقة على اجراء تغيير معين بعد رفع طلب خاص والموافقة عليه ثم مراجعته وارشفته بهدف المحافظة على امان وكفاءة النظام ولضمان حسن إدارة موارد الدوائر المختلفة والمحافظة عليها .
	فك التشفير	عملية استعادة المعلومات من شكل مبهم الى شكل مقروء
	كشف الأعطال	عملية تتبع وإصلاح الأخطاء في البرامج الحاسوبية والأجهزة وتقليلها من خلال إصلاحها أولا بأول حتى لا تؤثر على عمل هذه الأنظمة والأجهزة واستقرارها .
	مدير النظام	الموظف المسؤول عن إدارة الشبكة او النظام او الخدمات الخاصة بالنظام
	مستوى الأداء	حالة من حالات النظام سواء في الوضع الطبيعي او في وقت معين ويقاس بشكل عام عن طريق عمليات إحصائية حسابية متعددة تجري على النظام في لحظة او فترة معينة .

	مسؤول المعلومات او منشى المعلومات	الشخص او المجموعة المسؤولة عن انشاء او حفظ المعلومات ويكون عادة الشخص المسؤول عن المؤسسة التي قامت بإنشاء هذه المعلومات
	ملفات تسجيل الحركات	الملفات التي تقوم الأنظمة الالكترونية فيها بتسجيل احداث معينة مثل عملية قدوم بريد الكتروني (في خادم بريد الكتروني) او عملية التحقق من كلمات الدخول التي تحدث في النظام سواء اكانت جهاز حاسوب او شبكة او قاعدة بيانات - وبشكل الي من اجل المقدرة على التدقيق عبر تتبع الحالات التي تمر بهذه الأنظمة بالإضافة الى عملية التدقيق على عملها وبشكل خارجي .
	مؤتمن المعلومات	الشخص المسؤول عن متابعة وتطبيق وسائل الامن والحماية المناسبة لحماية الممتلكات المعلوماتية في المؤسسة حسب مستوى التصنيف الذي يقره مسؤول المعلومات
	الشبكات الافتراضية	هي شبكة تخلق شبكة خاصة داخل شبكة عمومية، مثل الإنترنت، وتسمح للمستخدم بإرسال واستقبال بيانات ضمن شبكات مشتركة أو عمومية وكأن جهازه متصل بشكل مباشر بتلك الشبكة الخاصة. يعني أنها تخلق جسرا افتراضيا بين المستخدم وبين السيرفر الموجود في مكان ما عبر العالم.
	اللوائح التنظيمية	مجموعة من القوانين والتعليمات التي تنظم العمل في المؤسسات
	كلمة المرور	و هي اداة تحقق تستخدم للتحكم بالدخول الى الموارد المختلفة وهي تتكون من سلسلة سرية من الرموز معروفة في النظام يدخلها المستخدم من اجل اثبات هويته للنظام
	الحوكمة	هي جميع الانظمة والقوانين والتعليمات والتشريعات التي تحكم نظام العمل
	الخدمات الالكترونية	تدير حلول الامن التقني لضمان امن و مرونة الانظمة و الموارد المعلوماتية بما يتفق مع السياسات والاجراءات والاتفاقيات ذات الصلة
	الشبكة اللاسلكية	تعتبر احد انواع الشبكات التي تربط الاجهزة المختلفة لتبادل المعلومات دون الحاجة الى استخدام الاسلاك والتوصيلات وذلك باستخدام امواج الراديو الكهرومغناطيسية كحامل لإشارة هذه المعلومات
	شبكات واسعة النطاق	شبكة معلوماتية تربط مؤسسة او اكثر وتغطي مساحات واسعة جغرافيا

الفصل الثاني : الأدوار والمسؤوليات والواجبات العامة

في هذا الفصل سيتم توضيح بعض الأدوار والمسؤوليات والواجبات العامة لمن تقع على عاتقهم مسؤولية تطبيق هذه الوثيقة.

١.٢ الفريق الوطني للاستجابة للأحداث السيبرانية

يتولى الفريق المهام الاتية:

- الاستجابة الفورية للخروقات الأمنية قبل ان تسبب أضراراً كبيرة، بما في ذلك تقويم الضرر ومستوى الخطورة واحتواء الهجمة وجمع الادلة الالكترونية ومعالجة الخروقات الأمنية، واستعادة البيانات .
- التقويم التكنولوجي والمتابعة الدورية للنظام الأمني للمعلومات المطبق حالياً في القطاعين العام والخاص، وتقويم الاجراءات الأمنية والاحترازية المتبعة كافة ومراجعة الإجراءات المقرة كافة استجابة للأحداث السيبرانية وإصدار التوصيات في حالة الحاجة لتغيير تلك الإجراءات.
- دعم ومساندة الفرق الأمنية المحلية في جميع المؤسسات والدوائر وتقويم إجراءاتها بشكل دوري، والتنسيق لإجراء فحوصات أمنية شاملة للتأكد من تطبيق معايير الأمن السيبراني.
- دعم مديري الأنظمة والبيانات في الوزارات والمؤسسات الحكومية بهدف تحصين شبكاتها وحمايتها من الاختراق والمعالجة عند حدوث طارئ.
- التنسيق مع المنظمات الدولية المتخصصة في مجال الأمن السيبراني والتنسيق مع فرق الاستجابة لدول العالم لتطوير وإنجاز المهام الموكلة اليه.

٢,٢ المؤسسات

- تطبيق وثيقة سياسات ومعايير أمن المعلومات والبيانات التي تعتبر الحدود الدنيا للممارسات المتعلقة بأمن وحماية المعلومات داخل المؤسسة.
- وضع التعليمات والإجراءات المناسبة لتطبيق هذه السياسات.
- تعميم هذه السياسات على العاملين داخل المؤسسة او شخص يتعامل مع المعلومات والبيانات وممكن ان يؤثر عدم اطلاعه على هذه الوثيقة الى ضرر بأمن هذه المعلومات والبيانات وجعلها في متناول أيديهم بشكل مستمر.
- تعيين مدير أمن معلومات وتوفير الدعم اللازم له من اجل تطبيق مهامه و واجباته (سيتم ذكرها لاحقا) .
- التدقيق على مدى الالتزام بهذه السياسات (بالتنسيق مع مدير أمن المعلومات) داخل المؤسسة بهدف تحديد ومعالجة أي قصور أو ثغرات في تطبيق هذه الوثيقة.
- وضع وتوضيح الإجراءات المناسبة لمحاسبة العاملين داخل المؤسسة عن أي خلل أو قصور من شأنه الإخلال بأمن وحماية المعلومات والبيانات داخل المؤسسة طبقًا للأنظمة المعمول بها.

٣.٢ مدير أمن المعلومات

١. التأكد من تطبيق وثيقة سياسات ومعايير أمن المعلومات والبيانات والتعليمات والإجراءات المتعلقة بها داخل المؤسسة.

٢. التعاون مع جميع العاملين داخل المؤسسة من أجل تطبيق هذه السياسات والتعليمات والإجراءات بأعلى مستويات الجودة الممكنة.

٣. القيام بالدور التوعوي المناسب لتدريب ورفع مستوى مهارات العاملين داخل المؤسسة 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 بوثيقة سياسات ومعايير أمن المعلومات والبيانات ، وبيان الآثار السلبية المترتبة على عدم الالتزام بها أو ترك العمل بها.

٤. التدقيق على مدى التزام جميع العاملين داخل المؤسسة بهذه السياسات والتعليمات المتعلقة بها.
٥. مساعدة العاملين داخل المؤسسة لمعالجة أية مشاكل لها علاقة بأمن وحماية المعلومات وبالتنسيق مع مدير النظام .
٦. البحث المتواصل عن ما يستجد في مجال أمن المعلومات لترشيح التقنيات التي يمكن اقتناؤها لتحسين بيئة العمل و الأمن الرقمي.
٧. وضع سياسات التعامل مع المشاكل الأمنية المعلوماتية لحلها في أقصر وقت عند حدوثها.
٨. مراجعة السياسة المتبعة والمتعلقة بأمن المعلومات والبيانات و وضع التصور الخاص بتطويرها.
٩. التنسيق الدائم ورفع التقارير الفنية بصورة دورية الى الفريق الوطني للاستجابة للأحداث السيبرانية المشكل بالأمر الديواني ٦٦س لسنة ٢٠١٧.

٤.٢ مدير النظام

١. تطبيق السياسات والتعليمات والإجراءات على نظام المعلومات الموجود داخل المؤسسة بالتوافق مع هذه الوثيقة.
٢. توفير الدعم الفني الكافي الذي يضمن تطبيق هذه السياسات.
٣. التعاون مع مدير أمن المعلومات للقيام بمهامه بيسر وسهولة.

٥.٢ العاملين داخل المؤسسات (المستخدمين)

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

الفصل الثالث : الأطر والارشادات - خارطة الطريق لتطبيق نظام ادارة أمن المعلومات

كون هذه الوثيقة لا تتطرق للتعليمات والإجراءات والتوجيهات الداخلية لكل مؤسسة فيما يخص الكيفية التي تراها مناسبة لتطبيق هذه السياسات وجدنا من الضروري توضيح بعض الأطر والارشادات وضرورة إعطاء خارطة طريق للمؤسسات لتطبيق نظام إدارة أمن المعلومات وهذا ما سيتم التطرق له في هذا الفصل.

١.٣ حوكمة الأمن الالكتروني

يتعين على المؤسسات القيام بما يلي:

١.١.٣ تخصيص الموازنة الملائمة لتطبيق وادارة برنامج أمن المعلومات

يتعين على المؤسسات ان تثبت التزاماتها بنظام أمن المعلومات من خلال ضمان تخصيص الموارد الملائمة بما في ذلك الموازنة والموظفين لإدارة برنامج أمن المعلومات

قد تؤدي قلة التمويل الى الحيلولة دون تطبيق الضوابط الأمنية المناسبة او تنفيذ برنامج أمن المعلومات. و فيما يتعلق بالموارد، سوف يخفق افضل الانظمة في حالة عدم توافر الموارد الكافية لإدارة عملياته.

٢.١.٣ ضمان قيام الإدارة العليا للمؤسسة بتقديم الدعم من اجل تطوير و تنفيذ عمليات أمن المعلومات والبنية الاساسية لتكنولوجيا المعلومات و الاتصالات و صيانتها بصفة دائمة داخل المؤسسة.

يعد البرنامج الذي يحظى بتمويل ضعيف اسوأ من عدم وجود برنامج في الاساس، حيث يبث شعور الرضا الزائف بين الاطراف الرئيسية. حيث يتمثل العنصر الرئيسي لنجاح اي من برامج أمن المعلومات في الدعم الدائم الذي تقدمه الإدارة العليا من اجل تحقيق الاهداف المرجوة من خلال توفير الموارد الكافية و التمويل للبرنامج.

٢.٣ الالتزام

يجب أن تبدى الإدارة العليا الالتزام الكامل فيما يتعلق بنظام إدارة تأمين المعلومات وتناقل البيانات وذلك من خلال:

١. التحقق من أن سياسات وأهداف أمن المعلومات قد وضعت ومن أنها متوافقة مع التوجه الاستراتيجي للمؤسسة.
٢. التحقق من تكامل / دمج متطلبات نظام إدارة أمن المعلومات في عمليات المؤسسة.
٣. التحقق من اتاحة / توفير الموارد اللازمة لنظام إدارة أمن المعلومات.
٤. التحقق من أن نظام إدارة أمن المعلومات يحقق النتائج المرجوة.
٥. توجيه ودعم الأشخاص للإسهام في فعالية نظام إدارة أمن المعلومات.

٣.٣ الأدوار والمسؤوليات والسلطات التنظيمية

يجب على الإدارة العليا في المؤسسة التأكد من أن المسؤوليات والسلطات المطلوبة للقيام بالأدوار ذات الصلة بأمن المعلومات قد تم تخصيصها وإبلاغها.

٤.٣ تقدير المخاطر

يجب على المؤسسة تقدير المخاطر نتيجة عدم تطبيق نظام أمن المعلومات إضافة الى تحديد وتطبيق عملية لمعالجة مخاطر أمن المعلومات

٥.٣ أهداف أمن المعلومات وخطط تحقيقها

يجب على المؤسسة تحديد أهداف أمن المعلومات في الوظائف والمستويات بالإضافة الى التخطيط لكيفية تحقيق هذه الأهداف وذلك من خلال تحديد ما يلي :

١. ما سيتم القيام به ؟
٢. ما هي الموارد المطلوبة ؟
٣. من الذي سيكون مسؤولا ؟
٤. متى سيتم الانتهاء منه ؟
٥. كيف يتم تقييم النتائج ؟

٦.٣ الدعم والموارد

يجب على المؤسسة تحديد وتوفير الموارد اللازمة لإنشاء وتنفيذ وصيانة وتحسين نظام إدارة أمن المعلومات

٧.٣ الكفاءة

يجب أن تقوم المؤسسة بما يلي:

١. تحديد الكفاءات المطلوبة للأشخاص الذين يقومون بأعمال من شأنها التأثير على أداء أمن المعلومات.
٢. ضمان كفاءة الاشخاص على أساس التعليم والتدريب، أو الخبرات المناسبة.

٣. تحديد الإجراءات الهادفة الى رفع الكفاءة وعلى سبيل المثال: توفير التدريب للأفراد، العمل تحت إشراف زميل أقدم، إعادة تأهيل الموظفين الحاليين، التوظيف أو التعاقد مع أشخاص اكفَّاء.

٧.٣ التوعية

تعد التوعية الأمنية الجزء الاهم لضمان معرفة جميع الاطراف ذات الصلة للمخاطر الممكن وقوعها في حال عدم الالتزام بضوابط أمن المعلومات كما يمكن ان يوفر التدريب و التوعية للمستخدمين و المطورين و أداري أمن المعلومات و اي اطراف ذا صلة المهارات و المعارف اللازمة لتنفيذ التدابير الأمنية.

يعزز برنامج التوعية بأمن المعلومات من فاعلية الضوابط الأمنية التي تم إنشاؤها وتنفيذها مسبقا، ولا شك أن وعي العاملين داخل المؤسسة بالمسئوليات الأمنية الملقاة على عاتقهم يشكل رادعا قويا ضد التهديدات المعروفة والمجهولة على حد سواء. يتألف البرنامج من المراحل الموضحة أدناه:

- التخطيط للتوعية بأمن المعلومات
- المراقبة والتحكم في التوعية بأمن المعلومات
- انتهاء برنامج التوعية بأمن المعلومات وتقييم النتائج

١.٧.٣ التخطيط للتوعية بأمن المعلومات

تمثل هذه المرحلة بداية البرنامج، والهدف الرئيسي منها هو تحديد النطاق والأهداف والقيود، وتحديد الأدوار والمسؤوليات ذات الصلة ببرنامج التوعية بأمن المعلومات، و كما يلي:

١.١.٧.٣ تنظيم برنامج توعوية أمنية و تخصيص الموازنات اللازمة لتنفيذه

و تتضمن مواد التدريب، كحد ادنى مضمون من شانه ان:

- مساعدة الفرد على فهم معنى أمن تكنولوجيا المعلومات و سبب الحاجة اليه و مسؤوليته الشخصية عن الأمن، بالإضافة الى اهمية الالتزام بالسياسات و المعايير الأمنية المحددة للمؤسسات .

- يتضمن او يشير الى القوانين و اللوائح الحكومية المتعلقة بأمن المعلومات و الاتصالات.
- يساعد الفرد على تحقيق فهم افضل لتقنيات اسلوب الهندسة الاجتماعية التي يمكن استخدامها في خداع الشخص من اجل الكشف عن معلومات سرية او خاصة او متميزة بهدف تعريض سرية و سلامة و توافر بيانات و معلومات المؤسسات و مكونات نظم المعلومات للمخاطر.
- مسؤولية الافراد عن الابلاغ عن القضايا ذات الصلة بأمن تكنولوجيا المعلومات و ألية القيام بذلك.
- المتطلبات القانونية لسرية و حماية البيانات.
- ملكية البيانات ووضع العلامات على البيانات (تصنيفها).
- قضايا الاستخدام في غير نطاق العمل.
- متطلبات كلمة المرور الخاصة .
- الحماية من الفيروسات و البرامج المضرة و المدمرة.
- سياسة الاستخدام المقبول لمكونات نظم المعلومات و البريد الالكتروني و استخدام الشبكة الدولية (الانترنت).
- تقنيات الهندسة الاجتماعية الشائع استخدامها في خداع المستخدمين.
- الأمن المادي.
- امكانية تطبيق المتطلبات الأمنية على جميع موارد نظام المعلومات ، بما في ذلك اجهزة تكنولوجيا المعلومات المحمولة، مثل الحاسبة المحمولة و غير ذلك.

كما ينبغي ان يتم توفير مواد التدريب على التوعية الأمنية (الكتيبات و الوثائق و غير ذلك)، بالإضافة الى سياسات و معايير و اجراءات أمن تكنولوجيا المعلومات، سواء بصورة الكترونية او عن طريق النسخ الورقية الى جميع العاملين داخل المؤسسة.

٢.١.٧.٣ يحصل جميع العاملين داخل المؤسسة، على التدريب و التوعية الملائمين فيما يتعلق بسياسات و اجراءات المؤسسات الحكومية حسب الاقتضاء بشان مهامهم الوظيفية و ادوارهم و مسؤولياتهم و مهاراتهم.

- ينبغي ان يحصل العاملين داخل المؤسسة على تدريب أمني قبل ان يحظى بإمكانية الوصول الى انظمة و موارد نظام المعلومات. و قبل الوصول الى تطبيقات البرمجيات المحددة الخاصة بالمؤسسة.
- يتم تعزيز التوعية الأمنية بصفة مستمرة. و ينبغي ان يتم تحديث التدريب على التوعية الأمنية بصورة دورية او بمجرد وقوع حدث محدد، مثل تغيير المسؤوليات الوظيفية او الحالة الوظيفية او غير ذلك.

٣.١.٧.٣ لا يفصح الموظفون بالحكومة (العاملين داخل المؤسسات الحكومية) ، اثناء التدريب مع الموظفين غير الحكوميين (العاملين داخل المؤسسات الغير حكومية)، عن اي معلومات او تفاصيل يمكن ان تعرض أمن المؤسسات الحكومية للخطر.

تهدف هذه التعليمات للتأكيد على مخاطر الهندسة الاجتماعية التي قد تؤدي الى الافصاح عن المعلومات. و غالبا ما تتمثل تلك المخاطر في السلوك البشري للمناقشات القائمة على الخبرات الشخصية. فمن الممكن ان يخوض الموظفون الحكوميون (العاملين داخل المؤسسات الحكومية) اثناء التدريب مناقشات و مداولات حول المعلومات الداخلية للمؤسسات الحكومية (عملية او تقنية). وقد يؤدي ذلك الى الافصاح غير المتعمد عن معلومات حساسة.

٤.١.٧.٣ يتم مراجعة و تحديث مضمون التدريب و التوعية الأمنية بصورة منتظمة كي يعكس التوجهات و المخاطر و التغييرات الجديدة بالبنية الاساسية لتكنولوجيا المعلومات في المؤسسات.

٥.١.٧.٣ يحصل الموظفون (العاملين داخل المؤسسة) الجدد على التدريب و التوعية بأمن المعلومات.

٦.١.٧.٣ يتم تقييم التدريب للتأكد من فاعلية البرنامج. بما في ذلك الحفاظ على سجلات حضور برامج التوعية الأمنية.

ينبغي ان تدرج المؤسسات اليات التقييم و النتائج الرسمية لقياس مدى ملائمة و فاعلية برامج و تقنيات و مواد التوعية الأمنية و التدريب.

ينبغي ان تحتفظ المؤسسات بسجلات حول جهود التوعية بأمن المعلومات. و يجب ان يتم توثيق حضور برامج التدريب على التوعية الأمنية ضمن ملف الموظف بشؤون الموظفين، مع اقرار الموظف بالحصول على التدريب و فهمه له.

٧.١.٧.٣ يتم استخدام الوسائط غير المباشرة مثل الملصقات و الشركات الداخلية و البريد الالكتروني ...الخ بصورة فعالة من اجل دعم برنامج التوعية

تحدد المؤسسات الاساليب الملائمة المستخدمة في التوعية و التعليم، و التي قد تتضمن على سبيل المثال لا الحصر ما يلي:

- الملصقات
- التدريب القائم على الحاسوب
- مواد و موارد الشبكة الداخلية
- افلام الفيديو

- الرسائل الاخبارية
- النشرات
- البيانات الموجزة
- التعليمات الرسمية بالفصل الدراسي
- التدريب اثناء العمل
- المؤتمرات

٢.٧.٣ المراقبة والتحكم في التوعية بأمن المعلومات

يخضع المشروع للمراقبة والتحكم طوال مرحلتي التخطيط والتنفيذ لبرنامج التوعية بأمن المعلومات، لذلك يجب رصد أية مشكلات أو عراقيل قد تخل بالجدول الزمني للبرنامج أو تعيق تحقيق أهدافه، واتخاذ الإجراءات التصحيحية المناسبة. ويجب إخطار المؤسسة في حال رصد أي مشاكل مستعصية. وفيما يلي بيان بعض الأنشطة الرئيسية في المراقبة والتحكم في التوعية بأمن المعلومات

- رصد التقدم في البرنامج مقارنة بقائمة المراحل الرئيسة للخطة.
- رصد العراقيل واتخاذ الإجراءات التصحيحية .
- تسهيل حل النزاعات وإخطار مسؤول البرنامج إذا تطلب الأمر مساعدة إضافية .
- تقديم تقرير عن حالة البرنامج بصفة دورية لجميع الأطراف المعنية .

٣.٧.٣ انتهاء برنامج التوعية بأمن المعلومات وتقييم النتائج

- تتضمن هذه المرحلة الانتهاء من البرنامج وقياس مدى فعاليته مقارنة بالحد الأدنى الذي تحدد أثناء مرحلة التخطيط لبرنامج التوعية الأمنية.
- تتضمن الأنشطة الرئيسية لهذه المرحلة قياس مدى فاعلية التوعية وتحديثها وفقا للدروس المستفادة.

٨.٣ الاتصالات

يجب على المؤسسة تحديد احتياجاتها من الاتصالات الداخلية والخارجية ذات الصلة بنظام إدارة أمن المعلومات بما في ذلك :

١. في أي شأن يتم التواصل ؟
٢. متى يتم التواصل ؟
٣. مع من يتم التواصل ؟
٤. من الذي يقوم بالتواصل ؟
٥. العمليات التي يتأثر بها التواصل ؟

٩.٣ التخطيط للتشغيل والرقابة

١. يجب على المؤسسة تخطيط وتنفيذ ومراقبة العمليات اللازمة للوفاء بمتطلبات تأمين المعلومات، وتنفيذ الإجراءات كما ويتعين على المؤسسة أيضا تنفيذ خطط تحقيق أهداف أمن المعلومات المحددة إضافة الى الاحتفاظ بمعلومات موثقة بالقدر اللازم لإعطاء الثقة في أن العمليات قد نفذت كما هو مخطط لها.
٢. يجب على المؤسسة مراقبة التغييرات المخططة ومراجعة العواقب غير المقصودة للتغييرات، واتخاذ الإجراءات اللازمة لتخفيف أية آثار سلبية، حسب الضرورة.
٣. يجب على المؤسسة ضمان أن العمليات التي تتم بموارد خارجية، محددة ومراقبة.

١٠.٣ تقييم الأداء والتدقيق الداخلي

يجب على المؤسسة تقييم أداء أمن المعلومات وفعالية نظام إدارة أمن المعلومات إضافة الى التدقيق الداخلي وعلى فترات مخططة، لتقديم معلومات بشأن ما إذا كان نظام إدارة أمن المعلومات يتوافق مع متطلبات المؤسسة إضافة الى ألية تنفيذه و صيانته على نحو فعال.

١١.٣ التطوير المستمر

يجب على المؤسسة أن تطور وتحسن باستمرار نظامها لإدارة تأمين المعلومات وقياس مدى ملائمته وفعاليته.

الفصل الرابع : سياسات عامة

السياسة الأولى - سياسة مشاركة البيانات الحكومية

س١.١ المقدمة

- تبين هذه السياسة الضوابط لمشاركة البيانات بين الجهات الحكومية وتدعم تنفيذ أفضل الممارسات والمعايير المذكورة في وثيقة اطار التخاطب البيني للحكومة والتصميم المعماري للمؤسسة الوطنية المقرة من قبل الحكومة العراقية مع مراعاة التحديث المستمر لهذه الوثيقة و وثيقة اطار التخاطب البيني للحكومة بما يتلاءم مع التطورات الحاصلة.
- تقع على الجهات الحكومية المعنية بتقديم خدمات للجمهور مسؤولية ضمان استخدام البيانات الشخصية التي تمتلكها قانونيا، والتحكم بها بشكل صحيح، واحترام حقوق الأشخاص، ويكمن التحدي الأبرز في مشاركة البيانات في إيجاد التوازن المناسب بين الحاجة إلى مشاركة البيانات للمساهمة في تقديم خدمات ذات جودة وضمان حماية سرية البيانات.
- يجب ان يكون تبادل البيانات والمعلومات بشكل سهل، سريع وأمن.
- يجب على الاطراف المتشاركة استخدام نظام تشفير معتمد عالمياً بآخر تحديثاته و متفق عليه يمنع الأشخاص الغير مصرح لهم بالاطلاع على تلك البيانات والمعلومات. ويجب الامتثال لسياسة التشفير المذكورة في هذا الوثيقة.
- التأكد من عدم التلاعب بالبيانات عند الادخال، الخزن والتبادل.
- المعلومات والبيانات المخزنة الكترونيا لها نفس الحجية القانونية لمثيلاتها الورقية.
- الاطراف التي تستخدم نظام تبادل الالكتروني للبيانات يجب ان ترتبط فيما بينها بعقد او اتفاقية لتبادل البيانات الكترونيا وحسب الاستمارات الموجودة في ملاحق هذا الوثيقة.

س١.٢ الهدف

- تحدد هذه السياسة المبادئ والمعايير الواجب الالتزام بها من قبل الجهات الحكومية وتنطبق على جميع أنواع البيانات القابلة للمشاركة، وتحدد السلوكيات والممارسات المتوقعة من قبل موظفيها، وتعزز التزام المؤسسة بمشاركة البيانات من خلال تطبيق أفضل الممارسات.
- تهدف هذه السياسة إلى دعم مشاركة البيانات بين الجهات الحكومية لتسهيل تقديم الخدمات للمواطنين والمستفيدين بشكل أفضل، و تسهيل تنفيذ خطة التحول للحكومة الإلكترونية، وتشمل ما يلي:
  ١. المبادئ العامة لمشاركة البيانات.
  ٢. الأسس القانونية لمشاركة البيانات.
  ٣. الأغراض المشتركة لحفظ ومشاركة البيانات.
  ٤. المسؤوليات المترتبة على الجهات الحكومية المعنية بمشاركة البيانات.
  ٥. معايير البرامج والتطبيقات.
- تحديد إجراءات خاصة لمشاركة البيانات ذات الطابع الخاص بين الجهات الحكومية (البيانات الممكن مشاركته، كيفية مشاركتها وحفظها ولمن يمكن إعطائها، الغرض المحدد لاستخدامها)، حيث ستتكفل الجهات المانحة للبيانات مسؤولية وضع تلك الإجراءات بالتنسيق مع لجنة الحوكمة او من يحل محلها لاحقا.

س١.٣ المجال

تنطبق هذه السياسة على جميع الجهات الحكومية التي تتبادل البيانات والمعلومات فيما بينها إضافة الى الجهات الحكومية التي تتعامل مع (المواطنين، القطاع خاص، القطاع مختلط) ,والتي يتوجب عليها توفير خدمات إلكترونية أساسية.

س١.٤ تفاصيل السياسة

س١.٤.١ ملكية المعلومات الحكومية

- تعود ملكية المعلومات والبيانات الحكومية الى الحكومة العراقية متمثلة بلجنة الحوكمة او من يحل محلها لاحقا.
- تعتبر ملكية المعلومات والبيانات الحكومية ملكية مركزية والمقصود بالملكية المركزية هي ان المؤسسات الحكومية (سواء كانت هي المنشئة او الجامعة للمعلومات والبيانات) لها حق التصرف بالمعلومات والبيانات الالكترونية لتوفير خدماتها لكن ملكية المعلومة وقرار مشاركتها يعود الى لجنة الحوكمة او من يحل محلها لاحقا.

.

س١.٤.٢ ألية مشاركة البيانات والمعلومات

- تشكل لجنة الحوكمة لجنة فرعية دائمة او وحدة ادارية تكون مسؤولة عن مشاركة البيانات والمعلومات .
- تشكل لجان في المؤسسات الحكومية تكون مسؤولة عن مشاركة البيانات والمعلومات ويكون احد افراد هذه اللجنة موظف بعنوان "منسق مشاركة البيانات".
- تكون مهام "منسق مشاركة البيانات" كما مبين ادناه:

١. متابعة التزام مقدم طلب المشاركة بالسياسات والمعايير المذكورة في هذه الوثيقة.
٢. يقوم بتوعية الموظفين بسياسات مشاركة البيانات والمعلومات.
٣. يقوم بتنظيم جدول ومحتوى اجتماعات اللجنة.

- يقوم مقدم طلب مشاركة البيانات وهو جهة حكومية او خاصة بملىء استمارة طلب مشاركة البيانات المرفقة في ملحق هذا الوثيقة.

- تقدم طلبات مشاركة البيانات والمعلومات الحكومية الى لجنة مشاركة البيانات والمعلومات في لجنة الحوكمة او من يحل محلها لاحقا لأجل استحصال الموافقة بمشاركة البيانات المطلوبة بما يضمن تطبيق بنود هذه الوثيقة.

س١.٤.٣ مسؤولية مقدم طلب المشاركة

يجب ان يلتزم مقدم طلب مشاركة البيانات بالنقاط التالية و على "منسق مشاركة البيانات" المتابعة للتأكد من التزامه بها.

- استخدام البيانات للغرض المذكور في استمارة تقديم طلب المشاركة حصرا.
- لا يمكن لمقدم الطلب ان يقوم بإعادة مشاركة البيانات مع أي جهة أخرى لأي سبب كان.
- لا يتم استخدام المعلومات المشاركة لتقديم خدمة تقدمها الجهة الحكومية صاحبة المعلومات أساسا.
- اتاحة الإمكانيات و التسهيلات لـ "منسق مشاركة البيانات" من اجل إتمام مهامه لمتابعة امتثال مقدم الطلب للسياسات المذكورة.

س١.٤.٤ المسؤولية القانونية لمشاركة البيانات

يجب على جميع الجهات المشاركة للبيانات والمعلومات الامتثال للسياسات و المعايير المذكورة في هذه الوثيقة إضافة الى أي قوانين او لوائح موجودة حاليا او يتم إصدارها مستقبلا تتعلق بمشاركة البيانات و حماية الخصوصية وغيرها من المجالات التي تمس أمن ومشاركة البيانات والمعلومات.

س١.٤.٥ مبادئ مشاركة البيانات

المبادئ المُنظمة لعملية مشاركة البيانات بين الجهات الحكومية والغير حكومية:

- يجب على الجهات كافة مشاركة البيانات لأغراض مشروعة فقط بطريقة لا تتعارض مع هذه الوثيقة و السياسات و اللوائح والقوانين النافذة.
- يجب ان تمنع الجهات الحكومية و الغير حكومية العاملين فيها من الوصول إلى البيانات والمعلومات إلا في نطاق عملهم فقط وبالحد الأدنى الذي يسمح بأداء عملهم ومهامهم ولا يسمح لهم بالإفصاح عن البيانات المتاحة اطلاقا.
- يجب تقييم الفوائد والمخاطر المحتملة على الأفراد أو المجتمع من مشاركة البيانات وعدم مشاركتها.
- يجب الاحتفاظ بسجلات خاصة بالقرارات المعنية بمشاركة البيانات والأسباب ذات الصلة بها – فيما يخص مشاركتها من عدمه. فإذا كان القرار يسمح بمشاركة البيانات، فبالتالي ينبغي توثيق لماذا تمت مشاركة البيانات ومع من ولأي غرض. حسب الاستمارات المرفقة في ملحقات هذا الوثيقة.
- يجب التأكد من أن البيانات التي قامت الجهة بمشاركتها ضرورية للغرض المحدد لها، ومع الأشخاص الذين يحتاجون إليها فقط، وما إذا كانت دقيقة ومحدثة، وما إذا تمت مشاركتها في الوقت المناسب، وبطريقة أمنة.

- لأي طلب له علاقة بمشاركة البيانات، يجب تقييم ما إذا كانت هناك التزامات قانونية مترتبة على ذلك (وجود شرط قانوني أو طلب محكمة، أو ما شابهها من الالتزامات).

س١.٤.٦ التزام الجهات المشاركة للبيانات

- مشاركة البيانات بما يتناسب مع السياسات المذكورة في هذه الوثيقة.
- تكامل ومشاركة البيانات عن طريق الشبكة الحكومية الموحدة.
- التأكد من أن مشاركة البيانات تتم عن طريق وسيط التكامل (لجنة الحوكمة – مركز البيانات الوطني) فقط، وعدم إنشاء أية نقاط مباشرة لمشاركة البيانات.
- إنشاء خدمات تطبيقات خاصة من أجل تسهيل عملية مشاركة البيانات وتقديم الخدمات الحكومية التكاملية.
- الالتزام بشروط الأطر القانونية التي تحكم حماية البيانات.
- الالتزام بوثيقة التخاطب البيني وخطة الحوكمة الالكترونية.
- إعلام المستخدمين متى وكيف تُسجل البيانات الخاصة بهم، وكيف ستستخدم.
- تبني مبدأ المرة الواحدة عند تسجيل البيانات، قدر الإمكان، لضمان عدم مطالبة الجهة الحكومية المواطنين والشركات بالمعلومات نفسها مرتين.
- التأكد من تطبيق الإجراءات التقنية وغير التقنية المناسبة ذات الصلة بأمن المعلومات عند حفظ أو نقل البيانات الشخصية (معايير فريق أمن المعلومات و معايير الجودة العالمية).
- عند مشاركة البيانات مع جهة غير حكومية، يجب على الجهة التي ستقوم بمشاركة البيانات الحصول على ضمانات من الطرف الاخر بالالتزام بهذه الوثيقة وتطبيق كافة بنودها بعد استحصال الموافقات من قبل لجنة الحوكمة.
- تعزيز وعي الموظفين بسياسات وإجراءات مشاركة البيانات.
- تعزيز الوعي بأهمية الحاجة إلى مشاركة البيانات من خلال قنوات الإعلام المناسبة.

س١.٤.٧ المسؤوليات المؤسسية والفردية للجهات الراغبة بمشاركة البيانات

- تقع على جميع الجهات مسؤولية تضمين هذه السياسة ضمن سياساتها المؤسسية الخاصة بمشاركة البيانات.

- يجب على جميع الجهات تعيين الصلاحيات والمسؤوليات ذات الصلة بمشاركة البيانات، وقد يشمل ذلك تحديد الأشخاص من أقسام مختلفة مثل قسم تقنية المعلومات ممن لديهم فهم كافٍ عن السياسات الخاصة بمشاركة البيانات.
- يجب على جميع الجهات عند استلامها للمعلومات والبيانات كجزء من الترتيبات الخاصة بمشاركة البيانات، عدم مشاركتها مع طرف آخر أو جهة أخرى بدون موافقة الجهة المالكة للبيانات والتنسيق مع لجنة الحوكمة.
- يتعين على جميع الجهات الالتزام بإجراءات الحماية لضمان التوازن ما بين الحفاظ على السرية ومشاركة البيانات بشكل صحيح كما موضح بالنقاط التالية:

  - التأكد من أن العاملين داخل المؤسسة واعين وملتزمين بما يلي:

✓ مسؤولياتهم والتزاماتهم فيما يخص سرية المعلومات الشخصية الخاصة بالأشخاص الذين يتواصلون مع الجهة.

✓ معرفة جهة الاتصال التي يمكن الرجوع إليها والإجراءات المتبعة في حال مخالفة سرية البيانات.

✓ التزام جميع الجهات بمشاركة البيانات قانونيا ووفقا للأحكام المتفق عليها فيما يخص الترتيبات الخاصة بمشاركة البيانات.

✓ مسؤولياتهم والتزاماتهم عند مشاركة البيانات مع طرف ثالث.

  - التأكد من أن البيانات المتاحة مسجلة بشكل صحيح من خلال:

✓ وضع إجراءات خاصة بتسجيل تفاصيل البيانات المُشاركة، مزود البيانات، ومُستلِم البيانات.

- ✓ التأكد من أن الأشخاص على علم بمن يمكن التواصل معه عند وجود أية استفسارات.

- أمن البيانات. يجب على جميع الجهات التأكد من وضع إجراءات لحماية سرية وسلامة وإتاحة البيانات خلال جميع المراحل. كما ينبغي عليها الالتزام بإجراءات وسياسات أمن المعلومات
- جودة البيانات. يجب أن تكون البيانات المُشاركة بجودة عالية ويوصى بأن تتبع تلك البيانات إرشادات أساسية مُستخدمة بواسطة الجهة المشاركة للبيانات. وكإرشاد عام: ينبغي تطبيق المبادئ الستة التالية الخاصة بجودة البيانات:

- ✓ الدقة: ينبغي أن تكون البيانات دقيقة بشكل مناسب للأغراض المقصودة لها، مبينة بوضوح وبأدق التفاصيل. كما يجب تسجيل البيانات مرة واحدة فقط، حتى إذا ما كانت ستستخدم في أغراض متعددة.
- ✓ شرعية البيانات: يجب تسجيل واستخدام البيانات وفقا للمتطلبات القانونية ذات الصلة، بما في ذلك التطبيق الصحيح لأية قوانين أو تعريفات.
- ✓ التنسيق: يجب أن تعكس البيانات دقة وتنسيق عملية جمع البيانات خلال جميع نقاط الجمع وخلال فترة زمنية معينة وما إذا كانت الجهات تستخدم الجمع اليدوي أو أنظمة معتمدة على الكمبيوتر أو الطريقتين معا.
- ✓ التوقيت: يجب جمع البيانات بأقصى سرعة ممكنة ، كما يجب إتاحتها للغرض الذي طلبت من أجله خلال فترة زمنية مناسبة. ويجب أن تكون البيانات متاحة بقدر كافٍ من السرعة والانتظام من أجل دعم الحاجات المعلوماتية وللمساهمة في تقديم الخدمات الالكترونية أو عملية اتخاذ القرارات الإدارية.
- ✓ صلة البيانات بالغرض المطلوب: يجب أن تكون البيانات المسجلة ذات صلة بالغرض الذي تستخدم من أجله، وهذا يتطلب مراجعة دورية للمتطلبات من أجل توضيح الاحتياجات اللازمة .

- ✓ التكامل: يجب تحديد متطلبات البيانات بوضوح بناءاً على الاحتياجات المعلوماتية للجهة والإجراءات الخاصة بجمع البيانات ومدى موافقتها لتلك المتطلبات. كما أن مراقبة

النقص، وعدم الاكتمال، أو التسجيل غير الصحيح، قد تعطي مؤشرات على جودة البيانات وقد تشير إلى بعض المشكلات في تسجيل عناصر بيانات محددة.

س١.٤.٨ المراقبة والمراجعة للجهات الراغبة بمشاركة البيانات

- ستقوم (اللجنة الفنية العليا لأمن الاتصالات والمعلومات) بالتعاون مع ممثلي الجهات بمراجعة هذه السياسة سنويا إلا إذا اقتضت تعديلات بعض القوانين والتشريعات مراجعتها قبل ذلك على سبيل المثال حصول طارئ أمني معين يتطلب التعديل.
- ستكون كل جهة مسؤولة عن مراقبة ومراجعة تنفيذ هذه السياسة والإجراءات ذات الصلة بها دوريا وبالتنسيق مع منسق مشاركة البيانات.
- على كل جهة مسؤولية مراقبة ومراجعة الإجراءات الخاصة بمشاركة البيانات الشخصية لديها دوريا وبالتنسيق مع منسق مشاركة البيانات.

س١.٤.٨ المخالفات

- لا بد أن يكون لدى الجهات المشاركة للبيانات إجراءات مناسبة للتحقيق والتعامل مع الوصول أو الاستخدام غير المخول أو غير المسموح به للبيانات والمعلومات سواءً بقصد أو من غير قصد.
- في حال مخالفة الضوابط والإجراءات التي نصت عليها سياسة مشاركة البيانات سواءً عن طريق الخطأ أو عمداً، يجب على الجهة المشاركة للبيانات حال اكتشافها لذلك أن تقوم بما يلي بدون أي تأخير:
- اعلام لجنة الحوكمة بهذا الخرق.
- اتخاذ الإجراءات المناسبة كلما كان ذلك ممكن للتقليل من أي تأثيرات محتملة.
- إبلاغ الجهة التي قامت بتوفير البيانات بكافة التفاصيل.
- التحقيق في الأمر لمعرفة السبب.

- اتخاذ إجراءات تأديبية ضد المسؤول عن المخالفة وحسب القوانين واللوائح التالية بناءاً على المراجع القانونية التالية :
  - ✓ قانون انضباط موظفي الدولة
  - ✓ قانون العقوبات العراقي
  - ✓ قانون جرائم المعلوماتية حال إقراره.
  - ✓ كافة القوانين ذات العلاقة النافذة.

- اتخاذ إجراءات تمنع من حدوث ذلك مستقبلاً.
- عند الإبلاغ عن أية مخالفة، يجب أن تقوم الجهة الموفرة للبيانات والجهة المسؤولة عن المخالفة وأي جهات أخرى إن كان ضروريا القيام بتقييم التأثيرات المحتملة.

س١.٤.٩ الشكاوي

- يجب أن تضع الجهات المشاركة للبيانات إجراءات مناسبة للتعامل مع الشكاوى ذات الصلة بالإفصاح عن المعلومات وبالتنسيق مع لجنة الحوكمة.
- على جميع الجهات المشاركة للبيانات الاتفاق والتعاون على التحقيق في أي شكوى في حال كانت البيانات ذات الصلة بالشكوى مشتركة بينها.

س١.٤.١٠ معايير الأنظمة والتطبيقات

١. تدعم سياسة مشاركة البيانات الحكومية مفهوم المصدر المفتوح (Open Source) في استخدام الأنظمة و التطبيقات.
٢. ان كان من الضرورة استخدام برامج مغلقة المصدر يجب تقديم الأسباب الموجبة لذلك.
٣. اتباع أفضل المعايير العالمية عند بناء التطبيقات لتجنب الثغرات الأمنية والاخطاء البرمجية.

٤. يجب ان يتم فحص كل الأنظمة والتطبيقات أمنيا باستخدام الطرق التقنية المتعارف عليها في اختبارات الاختراق والتحليل الأمني وبالتعاون مع مدير أمن المعلومات والفريق الوطني للاستجابة للأحداث السيبرانية.

٥. عدم استخدام أنظمة او تطبيقات غير مرخصة لمشاركة البيانات الحكومية.

٦. قواعد البيانات العلائقية (Relational Database) يجب ان تكون مهيكلة وفق المعايير العالمية على ان لا تقل عن المستوى الثالث من سلسلة ما يسمى بالنماذج العادية (Database Normalization) من أجل تقليل تكرار البيانات وتحسين تكامل البيانات.

٧. الابتعاد قدر المستطاع عند بناء التطبيقات من استخدام البرمجة الهيكلية (Structural Programming) و اعتماد البرمجية الكيانية (Object Oriented Programming).

٨. الابتعاد عن استخدام لغات برمجية لا تمتلك تحديثات أمنية مستمرة.

٩. استخدام البروتوكولات الخاصة المتفق عليها لتبادل المعلومات والبيانات وكذلك المعاير البرمجية الخاصة بشبكات الانترنت المذكورة في ملحق هذه الوثيقة الخاص بالمعاير. والامتثال للتحديثات الصادرة من لجنة الحوكمة بهذا الخصوص.

١٠. صيغة البيانات والمعلومات التي ستستخدم في التبادل يجب ان تكون متوافقة مع المعاير المذكورة في ملحق هذه الوثيقة والامتثال لتحديثاتها.

١١. البرامج والتطبيقات المستخدمة يجب ان تكون متوافقة مع المعاير المذكورة في ملحق هذه الوثيقة و الامتثال لتحديثاتها.

الفصل الخامس: سياسات عامة

السياسة الثانية: سياسة الاستخدام المقبول

س٢.١ المجال

توضح هذه السياسة الممارسات الفضلى للاستعمالات المقبولة والممنوعة التي يجب على جميع مستخدمي نظام المعلومات داخل المؤسسة أخذها بعين الاعتبار عند التعامل معها.

س٢.٢ الهدف

توفير بيئة نظم معلومات أمنة وموثوقة ومريحة للاستخدام بحيث يتحمل جميع العاملين داخل المؤسسة المسؤولية في الاستعمال الصحيح للمعلومات ومواردها والبنية التحتية لنظام المعلومات داخل المؤسسة.

س٢.٣ تفاصيل السياسة

س٢.٣.١ أجهزة الحاسوب

يوضح هذا البند الاستعمالات المقبولة والممنوعة لأجهزة الحاسوب داخل المؤسسة، بما يتضمنه ذلك من أنظمة التشغيل، وبرامج وملفات ، وبرمجيات، وجميع أنظمة المعلومات داخل المؤسسة.

الممارسات المقبولة

١. تنصيب وتحديث وإعداد البرمجيات المرخصة الخاصة بالعمل عن طريق مدير النظام اعتمادًا على الوصف الوظيفي للمستخدم والمسؤوليات المناطة به.
٢. استخدام البرمجيات المرخصة لتحقيق أهداف المؤسسة والمهام الملقاة على عاتقها.
٣. إنشاء ومعالجة وأرشفة وحذف الملفات حسبما تقتضيه طبيعة ومصلحة العمل.

٤. نسخ البرمجيات او الملفات إلى وسائط تخزين خارجية لأغراض العمل الرسمي بعد استحصال الموافقات الرسمية وحسب السياق المتبع داخل المؤسسة.

الممارسات الممنوعة

١. إزالة أو حذف أي من البرمجيات أو الملفات الضرورية التي يحتاجها المستخدم لأداء واجباته حسب وصفه الوظيفي ومسؤولياته المناطة له.
٢. نسخ البرمجيات أو الملفات إلى وسائط تخزين خارجية لغير أغراض العمل الرسمي او بدون استحصال الموافقات الرسمية.
٣. تنصيب أيّة برمجيات غير مرخصة.
٤. استخدام الحاسوب للهو بالألعاب وبرامج الترفيه.
٥. تنصيب وتشغيل برمجيات أو تطبيقات مشبوهة قد تكون مصابة بالفيروسات أو الديدان أو أحصنة طروادة أو البرامج الإعلانية أو أي نوع من البرمجيات الخبيثة.
٦. استعمال البرمجيات والتطبيقات المرخصة للمنفعة الخاصة أو تطوير برمجيات خبيثة أو استخدمها لغير أغراض العمل الرسمي.

س٢.٣.٢ الإنترنت

يوضح هذا البند الاستعمالات المقبولة والممنوعة لخدمة الإنترنت داخل المؤسسة لتحقيق أهدافها ومصلحة العمل فيها حيث على المؤسسة التعاقد مع مزود خدمة الانترنيت وحسب سياسة التعاقد الخارجي و بالتنسيق المباشر مع مدير أمن المعلومات التابع للمؤسسة.

الممارسات المقبولة

١. البحث عبر الإنترنت لأغراض العمل الرسمي فقط.
٢. الدخول إلى مواقع الإنترنت الموثوقة والمرخصة لتنزيل التحديثات والإصلاحات للبرمجيات المرخصة داخل المؤسسة، ويكون ذلك من قبل مدير النظام، وحسب عملية ضبط التغيير المتبعة داخل المؤسسة استنادًا إلى سياسة إدارة التغيير.

٣. تنزيل أي محتوى له علاقة بطبيعة العمل شريطة تحقق جميع الشروط التالية:

- أن يكون الموقع موثوقًا.
- التأكد أن مادة المحتوى مرخصة للاستعمال او النسخ او التعديل .
- التأكد أن مادة المحتوى خالية من البرامج الخبيثة.
- ألا تؤثر عملية التنزيل سلبًا على الأداء العام للإنترنت داخل المؤسسة.
- أن يتم ذلك بالرجوع إلى مدير النظام داخل المؤسسة.

الممارسات الممنوعة

١- تنزيل بيانات او معلومات او برامج او تطبيقات او أي محتوى غير قانوني أو معادي ليس له علاقة بطبيعة ومصلحة العمل .

٢- تنزيل البرامج من الإنترنت وتشغيلها بدون موافقة مسبقة من قبل مدير النظام داخل المؤسسة.

٣- اللهو بالألعاب واستخدام غرف الدردشة لأغراض شخصية.

٤- المشاركة والمساهمة في المجموعات الإخبارية التي ليس علاقة لها بالعمل الرسمي او بدون استحصال الموفقات الرسمية وحسب الضوابط والتعليمات المتبعة داخل المؤسسة.

٥- تصفح الإنترنت بشكل زائد عن الحد المقبول لغير أغراض العمل الرسمي، ويحدد ذلك مدير النظام اعتمادًا على التعليمات المتبعة داخل المؤسسة.

٦- استخدام اسم المؤسسة في عمليات مالية او إدارية على شبكة الانترنيت بدون موافقة مسبقة واعتمادًا على التعليمات المتبعة داخل المؤسسة.

٧- عدم رفع أي بيانات او معلومات تخص أو تعود ملكيتها للمؤسسة او العاملين داخل المؤسسة إضافة الى عدم الإفصاح عن أي شيء قد يضر بسلامة و أمن و سير العمل داخل المؤسسة او العاملين داخل المؤسسة او تضر الصالح العام على شبكة الانترنيت.

س٢.٣.٣ الشبكات الحكومية

يوضح هذه البند الاستخدامات المقبولة والممنوعة للشبكة الداخلية والخارجية داخل المؤسسة (إضافة الى الشبكات الداخلية والخارجية التابعة لجهات اخرى والتي ترتبط مع الشبكة الخاصة للمؤسسة لأغراض العمل الرسمي) بما يتضمنه ذلك من خوادم وموجهات وجدران نارية وأسلاك وبروتوكولات وغيرها من مكونات الشبكة.

الممارسات المقبولة

١. استخدام أجهزة وعناصر الشبكات والبنية التحتية المعلوماتية لأغراض العمل الرسمي.
٢. اتباع عملية ضبط التغير المتبعة داخل المؤسسة عند تغيير أو إزالة عناصر وأجهزة الشبكات أو تغيير حزم الاتصالات والتمديدات عند الحاجة عن طريق مختصّي الشبكات المخولين بذلك.
٣. تنصيب وتحديث وضبط إعدادات البرمجيات والأجهزة المرخصة لمراقبة وحماية الاتصالات عبر الشبكات، مثل الجدران النارية وأنظمة كشف ومنع التطفل والاختراق بالتوافق مع تعليمات المؤسسة.
٤. إنشاء وإلغاء ومعالجة حسابات المستخدمين على الشبكة، إضافة إلى منح وحجب الصلاحيات حسب الوصف الوظيفي للمستخدمين بما يضمن لهم أداء المهام المناطة لهم و التي تكون محددة مسبقا حسب توجيهات و تعليمات المؤسسة.

الممارسات الممنوعة

١. إتلاف أو فصل أي عنصر أو جهاز تابع للشبكة بدون صلاحية أو موافقة مسبقة ومكتوبة من قبل الجهة المعنية بالأمر بالأمر وذلك حسب اللوائح و التعليمات المتبعة داخل المؤسسة.
٢. استخدام أجهزة الشبك في غير أغراض العمل الرسمي.
٣. تناول الأطعمة والمشروبات أو التدخين في غرف مراكز البيانات أو قرب أجهزة الشبكة.
٤. محاولة التأثير بشكل سلبي على أداء الشبكة بشكل مباشر أو غير مباشر بالقيام بواحد أو أكثر من الأفعال التألية:
- تنزيل أو تحميل كميات ضخمة من الملفات أو البيانات الغير الضرورة.
- التسبب برفع درجة حرارة أجهزة الشبكات أو تخريب أنظمة التكييف والتبريد.
- أي عمل اخر قد يؤثر على أداء الشبكة.

٥. مراقبة Monitoring او اقتناص Capturing تدفق المعلومات عبر الشبكات أو التجسس عليها.
٦. منح وحجب الصلاحيات لحسابات المستخدمين بدون تصريح.

٧. تنصيب أجهزة أو برمجيات على الشبكة بدون موافقة مسبقة ومكتوبة من الجهة المعنية بالأمر داخل المؤسسة وحسب عملية ضبط التغيير .

س٢.٣.٤ أنظمة البريد الالكتروني

يوضح هذا البند الممارسات المقبولة والممنوعة في استخدام أنظمة البريد الإلكتروني .

الممارسات المقبولة

١. فتح وقراءة وإرسال وتخزين البريد الإلكتروني من خلال مالك الحساب حصرا.
٢. استخدام حساب البريد الإلكتروني الرسمي المخصص من قبل المؤسسة حصرا والتي تكون تحت اسم النطاق العلوي العراقي IQ. العائد للمؤسسة وعدم استخدام حسابات البريد التجارية.
٣. إرسال المرفقات ذات المحتوى الرسمي للجهات الرسمية بالتوافق مع سياسة حساسية وتصنيف المعلومات.
٤. تنزيل المرفقات من المصادر الرسمية، بعد فحصها (Scan) باستخدام اجراءات الحماية الملائمة للتأكد من خلوها من أيّة تهديدات تتعلق بالبرامج الخبيثة.
٥. استعمال أنظمة البريد الإلكتروني بشكل مناسب يتوافق مع ميثاق السلوك الخاص بأمن المعلومات.

الممارسات الممنوعة

١. استخدام أنظمة البريد الإلكتروني لغير الأغراض الرسمية أو بطريقة تؤثر سلبًا على سير العمل.
٢. إرسال او وتنزيل المرفقات كبيرة الحجم لغير الاستعمالات الرسمية مثل ملفات الصوت والصورة او أي ملفات أخرى والتي قد تؤثر سلبًا على كفاءة أنظمة المؤسسة.
٣. التجسس على البريد الإلكتروني للمستخدمين الآخرين أو محاولة اختراقه.

س٢.٣.٥ حسابات الدخول الالكترونية للموظفين

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

الممارسات المقبولة

١. منح وحجب وتغيير الصلاحيات لحسابات الدخول الإلكترونية للمستخدمين عن طريق مدراء النظام المخولين بذلك حسب حاجة المؤسسة وحسب الوصف الوظيفي لهؤلاء المستخدمين وطبيعة أعمالهم.
٢. إدارة ملف المستخدم User Profile عن طريق المستخدم صاحب الحساب فقط الا اذا تطلب تدخل مدير النظام و بعد اخذ الموافقات المطلوبة من قبل الجهة المعنية بالأمر داخل المؤسسة او بطلب خطي من صاحب الحساب نفسه.

الممارسات الممنوعة

١. انتهاك واختراق حسابات الدخول الإلكترونية للمستخدمين.
٢. استخدام حسابات الدخول الإلكترونية للمستخدمين بدون ترخيص.
٣. إضافة أو حذف سجلات (Logs) الدخول الإلكترونية للمستخدمين، أو منح أو حجب صلاحيات معينة بدون ترخيص مسبق ومكتوب من قبل الجهة المعنية بالأمر داخل المؤسسة.
٤. جمع المعلومات من حسابات الدخول الإلكترونية للمستخدمين لأي غرض كان بدون ترخيص مسبق ومكتوب من قبل الجهة المعنية بالأمر داخل المؤسسة.
٥. تبادل المعلومات الخاصة بحسابات الدخول الإلكترونية.
٦. الكشف عن كلمة مرور حسابك للآخرين أو السماح للآخرين باستخدام حسابك.

س٢.٣.٦ المعدات

يوضح هذا البند الاستخدامات المقبولة والممنوعة للمعدات داخل المؤسسة، مثل الحواسيب الشخصية للمستخدمين، وأجهزة الاتصالات مثل الهاتف ، والطابعات، وأجهزة التكييف، والمولدات الكهربائية وغيرها من المعدات الأخرى التي تكون ضمن إطار نظام المعلومات و تناقل البيانات.

الممارسات المقبولة

١. تنصيب وتحديث وضبط إعدادات واستخدام المعدات المرخصة التي تعود ملكيتها للمؤسسة بما يتوافق مع عملية ضبط التغيير المعتمدة داخل المؤسسة بالتوافق مع سياسة ضبط التغيير.
٢. إصلاح هذه المعدات عن طريق المختصّين المخولين بذلك عند الحاجة، حسب عملية ضبط التغيير المعتمدة داخل المؤسسة بالتوافق مع سياسة ضبط التغيير.
٣. حفظ ونقل واستقبال وعرض ومعالجة أيّ محتوىً رسمي باستخدام هذه المعدات حسب الصلاحيات الممنوحة للمستخدم.

الممارسات الممنوعة

١. القيام بأي عمل من شأنه تخريب الأجهزة أو أيّة برمجيات تتعلق بها أو إحداث قصور فيها بشكل مباشر أو غير مباشر.
٢. تركيب أو إزالة شيء من المعدات بدون تصريح مكتوب وموافق عليه من قبل الجهة المعنية بالأمر داخل المؤسسة بذلك حسب عملية ضبط التغيير المعتمدة فيها.
٣. استغلال أي من هذه المعدات للمنفعة الشخصية.

س٢.٣.٧ الدعم الفني

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

الممارسات المقبولة

إن فريق الدعم الفني المحدد من قبل المؤسسة مسؤول عن تنصيب وإعداد وتحديث وكشف الأعطال وإصلاحها لأي جهاز أو اعدادات حسب عملية ضبط التغيير.

الممارسات الممنوعة

إصلاح أو محاولة تغيير أي من المعدات من قبل الأشخاص الغير مخولين بذلك.

س٨.٣.٢ ملحوظات مهمة

إن تحديد الاستعمال الشخصي لنظام المعلومات الذي له سبب مقبول متروك للمؤسسة وبموافقة خطية من قبل الجهة المعنية بالأمر شريطة أن تأخذ بعين الاعتبار النقاط التالية:

١. الأداء العام لموارد نظام المعلومات.
٢. القوانين والأنظمة والتعليمات المعمول بها في الدولة.
٣. طبيعة وبيئة العمل.
٤. الوصف الوظيفي للمستخدمين.
٥. السياسات الوطنية لأمن وحماية المعلومات الأخرى.

السياسة الثالثة - سياسة إدارة التغيير

س٣.١ الهدف

ضمان أمن وحماية نظام المعلومات عند القيام بأي تغيير قد يؤثر عليها.

س٣.٢ المجال

تغطي هذه السياسة أي تغيير قد يؤثر على إعدادات أو تنصيب أو إزالة أو إتلاف أي من نظام المعلومات المملوكة للمؤسسة، مثل الملفات والبرمجيات والأجهزة والمعدات والشبكات ووسائط التخزين والوثائق، كما تغطي كذلك الأشخاص المسؤولين عن تقديم طلبات التغيير (مثل مدير النظام) ومراجعتها والموافقة عليها.

س٣.٣ تفاصيل السياسة

س٣.٣.١ قواعد عامة

١. على المؤسسة وضع التعليمات والإجراءات المناسبة لتنظيم عملية ضبط التغيير داخل المؤسسة بالتوافق مع هذه السياسة.
٢. على المؤسسة متابعة عمليات ضبط التغيير والتدقيق على مدى تطبيقها بالتوافق مع هذه السياسة.
٣. لا يسمح بإجراء أي تغيير يتعلق بأيٍّ من نظام المعلومات المملوك للمؤسسة بدون المرور في عملية ضبط التغيير المعمول بها داخل المؤسسة.
٤. تقسم طلبات التغيير إلى نوعين رئيسيين:

- تغييرات مجدولة: وهي التي تحتاج إلى دراسة وموافقة مسبقة من قبل الجهة المعنية بالأمر داخل المؤسسة.

- تغييرات طارئة: وتتعلق عادة بالتغييرات غير المخطط لها، وهنا يرجع فيها إلى مدير النظام ، ومن ّ ثم يتم الإبلاغ عن التغييرات التي تم إجراؤها فيما بعد من أجل توثيقها حسب الأصول.

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

س٣.٣.٢ واجبات مدير النظام

١. تقديم طلبات التغيير من أجل الموافقة عليها من قبل الجهة المعنية بالأمر داخل المؤسسة.
٢. التنسيق مع مدير أمن المعلومات من أجل مراجعة طلبات التغيير المقدمة وإرفاق التوصيات الخاصة بأمن المعلومات بهذه الطلبات.
٣. إجراء التغيير المطلوب بعد موافقة الجهة المعنية بالأمر داخل المؤسسة ، أو الإيعاز بإجرائها لمن يلزم.

س٣.٣.٣ واجبات المستخدم

١. عدم إجراء أي تغيير على نظام المعلومات المملوك للمؤسسة.
٢. إبلاغ مدير النظام عند الحاجة لإجراء أي عملية تغيير تتعلق بعمل المستخدم والقيام بمسؤولياته داخل المؤسسة.

السياسة الرابعة - سياسة أمن العاملين داخل المؤسسة

س٤.١ الهدف

منع و تقليل المخاطر الناتجة عن الخطأ البشري وسوء الاستعمال– مثل الإتلاف والتدمير – عند التعامل مع نظام تكنولوجيا المعلومات.

س٤.٢ المجال

تغطي هذه السياسة جميع بالعاملين داخل المؤسسة او المراد تعينهم او التعاقد معهم.

س٤.٣ تفاصيل السياسة

س٤.٣.١ قواعد عامة

١. هذه السياسة معنيّة بالجوانب الخاصة بأمن المعلومات عند تعيين وتقييم وانهاء عقود العاملين داخل المؤسسة، والتي هي من مهام قسم الموارد البشرية بالتنسيق مع مدير أمن المعلومات داخل المؤسسة.
٢. على جميع العاملين داخل المؤسسة او المراد تعينهم او التعاقد معهم الالتزام بهذه الوثيقة (سياسات ومعايير أمن المعلومات والبيانات) وكافة اللوائح و التعليمات داخل المؤسسة المتعلقة بنظام تكنولوجيا المعلومات.
٣. على جميع العاملين داخل المؤسسة الالتزام بالتعليمات الخاصة بالتعامل مع الزوار، مثل عدم تركهم لوحدهم، وعدم القدوم إلا بموعد، والتحقق من هوياتهم بشكل أمن وصحيح بالتوافق مع سياسة الأمن المادي.

س٤.٣.٢ واجبات المؤسسة (قسم الموارد البشرية او من ينوب عنه)

١. استخدام الموارد المشروعة والمتاحة للتحقق من الأشخاص الذين يراد تعيينهم داخل المؤسسة او التعاقد معهم والتأكد من مؤهلات كل منهم .

٢. وضع وتحديد المهام المناطة بالعاملين داخل المؤسسة او المراد تعينهم او التعاقد معهم آخذين بعين الاعتبار مبدأ "الفصل بين الوظائف" ومبدأ "المعرفة على قدر الحاجة"
٣. تحديد الواجبات التي يجب على العاملين داخل المؤسسة أداؤها والمتعلقة بأمن وحماية المعلومات والبيانات ، وذلك بالتنسيق مع مدير أمن المعلومات داخل المؤسسة.

٤. إصدار بطاقات التعريف والمرور الخاصة بالعاملين داخل المؤسسة، مبينًا عليها الاسم والصورة والوظيفة.
٥. تجهيز تعهد "عدم الإفصاح عن المعلومات" للعاملين داخل المؤسسة الجدد من أجل قراءتها والتوقيع عليها.
٦. توفير الوثائق واللوائح والتعليمات المتعلقة بسياسات أمن وحماية المعلومات للعاملين داخل المؤسسة، ووضع نموذج تعهد بالالتزام بها.
٧. وضع الإجراءات الإدارية المناسبة لبيان الآثار المترتبة على مخالفة الوثائق واللوائح والتعليمات المتعلقة بسياسات أمن وحماية المعلومات.
٨. تطوير وتنفيذ ومراقبة برامج أمن وحماية العاملين داخل المؤسسة.

س٤.٣.٣ واجبات مدير أمن المعلومات

١. التوصية بمنح وحجب الصلاحيات المناسبة للوصول إلى نظام المعلومات وتحديد هذه الصلاحيات اعتمادا على الوصف الوظيفي وبناءاً على المهام والمسؤوليات المناطة إلى العاملين داخل المؤسسة.
٢. تقييم العاملين داخل المؤسسة في مدى تطبيقهم والتزامهم بالوثائق واللوائح والتعليمات المتعلقة بأمن وحماية المعلومات والبيانات
٣. التعاون مع (قسم الأمن والسلامة او من ينوب عنه) بوضع التوصيات والتعليمات الخاصة بضوابط الدخول الى المناطق التي تحتوي على موارد متعلقة بنظام المعلومات والتي يؤثر المساس بها على أمن البيانات والمعلومات.

السياسة الخامسة - سياسة السلوك الخاص بأمن المعلومات

س٥.١ الهدف

تعزيز السلامة العامة وإيجاد بيئة عمل مهنية أمنة يتعامل فيها العاملين داخل المؤسسة بمستوىً عال من الأخلاق والمسؤولية أثناء تعاملهم مع المعلومات والبيانات وجميع مكونات نظم المعلومات وممارسة الطرق الصحيحة لحمايتها.

س٥.٢ المجال

تغطي هذه السياسة جميع بالعاملين داخل المؤسسة.

س٥.٣ تفاصيل السياسة

ميثاق السلوك الخاص بأمن المعلومات هو مجموعة من القواعد والأحكام التي تحدد وترسم مسؤوليات الممارسات الصحيحة للفرد أو المؤسسة ، والتي يجب تطبيقها من أجل توفير بيئة عمل أمنة ومستقرة تساعد في الحفاظ على المعلومات والبيانات وجميع مكونات نظم المعلومات داخل المؤسسة.

س٥.٣.١ قواعد عامة

١. اتباع قوانين الدولة العراقية المتعلقة بأمن المعلومات والبيانات واستراتيجية الأمن السيبراني الوطنية والأنظمة والسياسات والتعليمات الداخلية داخل المؤسسة.

٢. استخدام مكونات نظم المعلومات في استمرارية العمل داخل المؤسسة .
٣. عدم إهدار الوقت والجهد في استخدام المعلومات والبيانات ومكونات نظم المعلومات لخدمة أي مصلحة خارجية ، أو للمصلحة الشخصية ، مثل الأنشطة التجارية (كالأسهم) والأنشطة السياسية، وذلك بالتوافق مع سياسة الاستعمال المقبول.
٤. حسابات الموظفين الإلكترونية ذات خصوصية وسرية، والموظفون غير مخولين بتبادل المعلومات الخاصة بحساباتهم.
٥. على جميع العاملين داخل المؤسسة تطبيق " الوصايا العشر في أخلاقيات الحاسوب" التي أوصى بها معهد أخلاقيات الحاسوب سنة ١٩٩٢ وهي:
   - عدم استخدام الحاسوب لإيذاء الآخرين.
   - عدم التدخل في عمل الآخرين على الحاسوب.
   - عدم التطفل على ملفات الحاسوب للآخرين.
   - عدم استخدام الحاسوب في السرقة.
   - عدم استخدام الحاسوب للإدلاء بشهادة الزور.
   - عدم نسخ أو استعمال برمجية محفوظة الملكية ما لم تكن مدفوعة السعر.
   - عدم استخدام مصادر الحاسوب للآخرين بدون تصريح أو تفويض صحيح.
   - عدم الاستيلاء على النتاجات الفكرية للآخرين.
   - فكر بالنتائج الاجتماعية للبرنامج الذي تكتبه.
   - استخدام الحاسوب بالوسائل التي تضمن الاحترام للآخرين.

س٥.٣.٢ التوظيف والتنقلات

١. تحديد ووضع قائمة بالمهام والمسؤوليات المناطة للعاملين داخل المؤسسة من قبل الجهة المعنية بالأمر بشكل يحقق مبدأ " الفصل بين المهام".

٢. يجب إعطاء جميع العاملين داخل المؤسسة الذين تم تعيينهم الحد الأدنى من الصلاحيات والامتيازات اللازمة لإتمام أعمالهم حسب الوصف الوظيفي لكل منهم، اعتمادًا على مبدأ " المعرفة على قدر الحاجة ".
٣. على العاملين داخل المؤسسة توقيع اتفاقية "عدم الإفصاح عن المعلومات" عند البدء بممارسة أعمالهم.
٤. يجب أن يتم تغيير جميع المهام والصلاحيات المسندة للعاملين داخل المؤسسة عند انتقالهم من منصب او موقع وظيفي الى اخر وحسب مهامهم الجديدة.

س٥.٣.٣ انهاء الخدمات

١. يجب تغيير حساب الدخول الإلكتروني وإلغاء أية صلاحيات أخرى للعاملين داخل المؤسسة في حال انهاء خدماتهم ، بعد التأكد من تسليم جميع المعلومات الخاصة بالعمل إلى المسؤول المباشر .
٢. يجب على العاملين داخل المؤسسة الذين انهيت خدماتهم تسليم كل ما بحوزتهم من مواد او معدات او ملفات او بيانات ترجع ملكيتها للمؤسسة.
٣. على العامل داخل المؤسسة توقيع تعهد أو إقرار مع المؤسسة 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 انهاء الخدمة.
٤. لا يسمح للعامل داخل المؤسسة الذي انهيت خدمته باستخدام الأجهزة والوصول إلى المعلومات المملوكة للمؤسسة.

٥. يجب حفظ نسخة من صندوق البريد الإلكتروني الخاص للعامل داخل المؤسسة المنهي عقده لفترة مناسبة لاستخدامه في حال استدعت الحاجة، وتحويل جميع الرسائل الموجهة إلى بريده الإلكتروني إلى الموظف الذي سينوب عنه وحسب ما يقرره المسؤول المباشر.

س٥.٣.٤ السلامة والأمان

على جميع الموظفين حماية نظام المعلومات والمحافظة عليه من التلف أو التخريب.

س٥.٣.٥ الخصوصية

١. المعلومات التي تخص العاملين داخل المؤسسة ذات خصوصية ويجب حمايتها وعدم الإفصاح عنها بشكل غير مرخص.
٢. للعاملين داخل المؤسسة الحق في استخدام المعلومات المخول لهم باستخدامها والدخول إليها ما دام في نطاق مهامهم.
٣. على العاملين داخل المؤسسة عدم انتهاك خصوصية معلومات أي من العاملين الآخرين.

س٥.٣.٦ قواعد التقارير والتدقيق والمتابعة

١. يجب على العاملين داخل المؤسسة اتباع التسلسل الإداري عند رفع التقارير الخاصة بالعمل.
٢. على المسؤولين داخل المؤسسة تطبيق التعليمات ضد الخروقات والمخالفات من قبل العاملين داخل المؤسسة ضمن القوانين والأنظمة والتعليمات والسياسات المتبعة في الدولة العراقية وداخل المؤسسة.
٣. ليس للعاملين داخل المؤسسة الحق في ممارسة دور " المدقق" أو القيام بتدقيق أو تحقيق بدون تصريح مسبق ومكتوب من قبل الجهة المعنية بالأمر داخل المؤسسة.

٤. على العاملين داخل المؤسسة الالتزام بتعليمات التدقيق الصادرة عن المؤسسة ، بالتوافق مع سياسة التدقيق الخاص بأمن المعلومات.

س٥.٣.٧ التعامل مع المعلومات

١. على العاملين داخل المؤسسة التعامل مع المعلومات وحفظها وإتلافها بشكل موثوق به حسب تصنيف هذه المعلومات، بالتوافق مع سياسة حساسية وتصنيف المعلومات.
٢. لا يسمح للعاملين داخل المؤسسة بالتصريح عن المعلومات السرية أو الإفصاح عنها.
٣. على العاملين داخل المؤسسة تطبيق سياسة " المكتب النظيف".
٤. لا يسمح للعاملين داخل المؤسسة محاولة الدخول إلى المعلومات السرية (الغير متعلقة بعملهم و مهامهم) سواءً بشكل مباشر أو غير مباشر.
٥. على العاملين داخل المؤسسة حماية المعلومات التي تقع ضمن اختصاص عملهم.
٦. لا يجوز للعاملين داخل المؤسسة التعامل مع جميع المعلومات المحفوظة أو المطبوعة أو المنقولة على أجهزة المؤسسة أو وسائطها بصورة غير شرعية وخارج نطاق مهامهم.
٧. عند استعمال الهاتف أو البريد الإلكتروني، فعلى العاملين داخل المؤسسة التأكد من هوية المتحدث أو المصدر قبل الإدلاء او ارسال أي معلومات.

س٥.٣.٨ ميثاق السلوك المهني لمدراء أمن النظام

على مدراء أمن المعلومات الالتزام بميثاق السلوك المهني والموضح بالنقاط ادناه :

١. أن يتحلى بأعلى المستويات الأخلاقية والعقلانية والسلوك السديد.

٢. ألا يكون مرتبطًا أو عضوًا في أي عمل غير قانوني أو غير أخلاقي يمكن أن يؤثر سلبًا على سمعته المهنية أو سمعة وظيفته.
٣. رفع التقارير الى الجهة المعنية بالأمر داخل المؤسسة بخصوص الأعمال الواقعة ضمن تخصصه والتي يعتقد انها غير قانونية وأن يتعاون في حال أدى ذلك إلى إجراء تحقيق بخصوص تلك الأعمال.
٤. دعم الجهود التي تساعد في نشر الوعي الخاص بأمن وحماية المعلومات وتفعيل إجراءات أمن وحماية المعلومات.
٥. تنفيذ الإجراءات الخاصة بأمن المعلومات للعاملين داخل المؤسسة بأعلى مستويات الجودة الممكنة.
٦. تنفيذ المسؤوليات المسندة إليه بطريقة تتوافق مع أعلى مستويات التخصص.
٧. عدم إساءة استخدام المعلومات التي يتعامل معها أثناء أداء واجباته، وعليه المحافظة على سريتها وسرية جميع المعلومات التي تقع تحت حوزته.

السياسة السادسة - سياسة التدقيق الخاص بأمن المعلومات

س٦.١ الهدف

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

س٦.٢ المجال

تغطي هذه السياسة جميع أنظمة تكنولوجيا المعلومات والسجلات وموارد نظام المعلومات المملوكة للمؤسسة (مثل أنظمة الحاسبات والاتصالات) ، والسياسات والإجراءات والتعليمات والسلطات والمسؤوليات وأية أعمال ترتبط بأية وثائق أخرى داخلية أو خارجية، والمعمول بها في هذه المؤسسة.

س٣.٦ تفاصيل السياسة

س١.٣.٦ مقدمة

هناك نوعان من التدقيق لنظام تكنولوجيا المعلومات:

- التدقيق الداخلي: تقوم به المؤسسة من خلال مدير أمن المعلومات لتدقيق نظام المعلومات فيها والإجراءات المعمول بها داخل المؤسسة، ويكون بصورة دورية وفق جدول موضوع من قبل مدير أمن المعلومات وبالتنسيق مع الإدارة العليا داخل المؤسسة .
- التدقيق الخارجي:
  - يقوم به الفريق الوطني للاستجابة للأحداث السيبرانية وبالتنسيق مع مدير أمن المعلومات التابع للمؤسسة.
  - يمكن للمؤسسة أن تقوم بعملية التدقيق بالاستعانة بفريق تدقيق من القطاع الخاص بعد ان يتم التنسيق مع مدير أمن المعلومات التابع للمؤسسة واستحصال الموافقات المطلوبة من الفريق الوطني للاستجابة للأحداث السيبرانية والإدارة العليا داخل المؤسسة.

س٢.٣.٦ الصلاحيات

- لفريق التدقيق (الخارجي) استقلالية مهنية عن الجهة التي يقوم بالتدقيق عليها.
- تحدد صلاحيات فريق التدقيق (الخارجي) من القطاع الخاص من قبل مدير أمن المعلومات و بالتنسيق مع الفريق الوطني للاستجابة للأحداث السيبرانية والإدارة العليا داخل المؤسسة.
- لا يجوز لأي من العاملين داخل المؤسسة إجراء أي عملية تدقيق داخلي بدون الحصول على تصريح مسبق .

- على جميع العاملين داخل المؤسسة التعاون مع المدققين أثناء عملية التدقيق، وتسهيل عملهم، وعدم وضع العوائق التي تحول دون قيامهم بواجبهم الرسمي.
- يجب منح الصلاحيات المناسبة والكافية لطاقم تدقيق أمن المعلومات وذلك حسب مقتضيات العمل ولنجاح 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 المؤسسة، بما يخدم عملية التدقيق.
٣. الوصول إلى مرافق المؤسسة المختلفة، مثل الأرشيف ومراكز البيانات (Data Centers) والخوادم (Servers) ومكاتب العاملين داخل المؤسسة .
٤. مراقبة وتسجيل حركة البيانات عبر الشبكات المعلوماتية.
٥. عدم إعطاء إمكانية الوصول الى مكونات نظم المعلومات التي لا يحتاج لها فريق التدقيق خلال اجراء الفحص.

س٦.٣.٣ واجبات فريق التدقيق

١. تخطيط وجدولة عمليات التدقيق الداخلي او الخارجي واعلام الجهة المعنية بالأمر داخل المؤسسة .
٢. أداء عملية التدقيق بالاستناد إلى المعايير والمقاييس العالمية .
٣. مراجعة العمليات والبرامج للتأكد من أن نظام المعلومات يتم استخدامه بشكل صحيح بالتوافق مع هذه الوثيقة والتعليمات المتبعة داخل المؤسسة.
٤. تقييم الإجراءات والتعليمات الداخلية للتأكد من موافقتها للسياسات والتعليمات المتداولة داخل المؤسسة، مثل مبدأ "الفصل بين الوظائف"، و"المعرفة على قدر الحاجة" و "العمل بقدر الاستطاعة والحذر".
٥. جمع وتقييم الأدلة المناسبة لتقرير وجود أي خلل أو عدم توافق للإجراءات مع السياسات والتعليمات لأمن وحماية المعلومات المعمول بها داخل المؤسسة.

٦. التأكد من ضمان جودة عملية التدقيق والتقارير والوثائق الصادرة عنها.
٧. القيام بعملية التدقيق بشكل دوري للتحقق من مدى التزام المؤسسة بتوصيات فريق التدقيق وإعلام الإدارة العليا داخل المؤسسة والفريق الوطني للاستجابة للأحداث السيبرانية.

س٦.٣.٤ التقارير

١. على فريق التدقيق إصدار تقرير مفصل بجميع نتائج التدقيق من أجل متابعة الإجراءات اللازمة لمعالجة أي استثناءات أو أخطاء في نظام تكنولوجيا المعلومات.
٢. 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- في حالة عدم تنفيذ عملية التدقيق يجب ذكر الأسباب التي أدت الى ذلك بشكل كامل والحصول على استنتاجات صحيحة.
٥- تقرير النتائج التفصيلية والتوصيات.

س٦.٣.٥ التوثيق والادلة

يجب على المؤسسة وبالتنسيق مع مدير أمن المعلومات وضع التعليمات الخاصة بتوثيق عملية التدقيق على أن يشمل التوثيق العناصر التالية:

١. التخطيط والتحضير لمجال وأهداف التدقيق.
٢. الوصف العام والتفصيلي لمجال التدقيق.
٣. برنامج التدقيق.
٤. خطوات التدقيق التي تم إنجازها.

٥. الأدلة التي تم جمعها أثناء التدقيق.
٦. الخدمات التي تم الاستفادة منها من المدققين والخبراء الآخرين.
٧. النتائج والاستنتاجات والتوصيات.

س٦.٣.٦ ميثاق السلوك الخاص بتدقيق أمن المعلومات

الالتزام بميثاق السلوك الأخلاقي الخاص بأمن المعلومات الذي أقرته جمعية التدقيق والرقابة على نظم المعلومات ISACA على مدققي أمن المعلومات والذي تم تلخيصه في النقاط الثمانية التالية:

١. دعم تطبيق السياسات والمعايير والتوجيهات والإجراءات المناسبة لأمن وحماية نظم المعلومات، وتشجيع المؤسسات على القيام بذلك.
٢. أداء الواجبات المناطة للمدقق بشكل هادف وبعناية فائقة ، اعتمادًا على المعايير المهنية المتبعة، ودعم العمل بأفضل الممارسات دون تحيز أو محاباة.
٣. تسهيل إنجاز مصالح المتعاملين مع المؤسسة بشكل قانوني يعكس صورة مهنية عالية لمهنة التدقيق.
٤. 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 بعد اخذ الموافقات الازمة.
٥. لا يجب الشروع بالتدقيق سوى في المجالات التي يكون المدقق فيها مؤهلا مهنيًا بشكل كاف والتي يستطيع من خلالها إثبات كفاءته.
٦. تقديم نتائج دقيقة لعملية التدقيق بأكملها واستخلاص الحقائق الهامة التي تم التوصّل إليها ورفعها إلى الجهات المخولة بذلك.
٧. دعم الجهود التوعوية التي تهدف إلى مساعدة العاملين داخل المؤسسة في تطوير فهمهم لأمن وإدارة نظم المعلومات.

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

الفصل الخامس : سياسات إدارة مكونات نظم المعلومات

السياسة السابعة - سياسة أمن السجلات

س٧.١ الهدف

وضع الضوابط لتحقيق أفضل الممارسات لحماية إنشاء السجلات الحكومية وحفظها والتخلص منها ونقلها وإصدارها والوصول إليها.

س٧.٢ المجال

تطبق هذه السياسة على جميع الوثائق التي تعود ملكيتها الى المؤسسة و كل الوثائق التي ترد الى المؤسسة من الجهات الأخرى.

س٧.٣ تفاصيل السياسة

١. تخضع جميع الوثائق الحكومية الى قانون الحفاظ على الوثائق المرقم (٣٧) لسنة ٢٠١٦.
٢. يجب ان تحتفظ المؤسسة بالسجلات التابعة حتى يتم التعامل معها وفقًا للقانون.
١. لا يجوز للعاملين داخل المؤسسة التخلص من السجلات من أي نوع دون الحصول على إذن مكتوب من الإدارة العليا.

٣. يجب أن يكون لدى كل مؤسسة برنامج إدارة السجلات.
٤. يجب أن يكون لدى كل مؤسسة سجل أصول معلومات يحتوي على تفاصيل جميع أصول المؤسسة.

السياسة الثامنة - سياسة تصنيف المعلومات

س٨.١ 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.

س٨.٢ المجال

تغطي هذه السياسة جميع المعلومات التابعة للمؤسسة ، سواء كانت إلكترونية أو غير إلكترونية.

س٨.٣ تفاصيل السياسة

س٨.٣.١ تعريف المعلومات

١. تتضمن المعلومات المعنيّة في هذه السياسة المعلومات التي يتم حفظها أو تبادلها بشتى الوسائل، سواءً أكانت إلكترونية أو غير إلكترونية، مثل المعلومات المكتوبة، أو تلك التي يتم تبادلها مشافهًة –مثل الهاتف- أو بشكل مرئي - مثل الاجتماعات المرئية والمسموعة وغيرها.
٢. على المؤسسة وضع معايير شاملة للتعامل مع المعلومات وتحديد أهمية هذه المعلومات وحساسيتها، واستخدام خطة التصنيف المتبعة في هذه السياسة.

٣. يجب عزل جميع المعلومات ضمن تصنيفاتها بطريقة فيزيائية أو إلكترونية حسب مستوى حساسيتها.
٤. تقسم دور حياة المعلومة الى:
   أ- الانشاء
   ب- الخزن
   ت- المسح
   ث- المعالجة
   ج- النقل
   ح- النسخ
   خ- الاستعمال
   د- الضياع
   ذ- التلف

س٨.٣.٢ ألية التعامل مع المعلومات

١. يجب تصنيف جميع المعلومات المملوكة للمؤسسة، استنادًا إلى أحكام قانون ضمان حق الحصول على المعلومات رقم ٤٧ لسنة ٢٠٠٧.
٢. ليس لجميع المعلومات القدر نفسه من الحساسية والأهمية، وبالتالي فإن المعلومات تحتاج مستويات مختلفة من الحماية.
٣. يجب أن تتم إدارة المعلومات بشكل صحيح ابتداءً من مرحلة إنشائها، مرورًا بالاستخدام المرخص لها، وانتهاءً بالطريقة الصحيحة لإتلافها.
٤. المؤسسة 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"، استنادًا إلى أحكام قانون حماية أسرار الدولة رقم ٥٠ لسنة ١٩٧١ وأية تعديلات طرأت عليه.

٥. أية معلومات مملوكة للمؤسسة، مثل الوثائق الموجودة منذ أمد بعيد فيها ولم يتم تصنيفها قبل تطبيق هذه السياسة- يجب أن يعاد تصنيفها.

س٨.٣.٣ تصنيف المعلومات

- المستوى الاول: المعلومات العادية

١. المعلومات العادية هي معلومات قليلة الحساسية، لا يؤثر الإفصاح عنها على خصوصية أو أمن المؤسسة أو العاملين فيها، 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.

٢. لا توجد صلاحيات أو تحديدات على هذه النوع من التصنيف.

- المستوى الثاني: المعلومات المحدودة

١. هي معلومات حساسة معدة للاستخدام الرسمي، وإذا ما تم الإفصاح عنها فأنها يمكن أن تعرض خصوصية وأمن المؤسسة أو العاملين فيها للخطر، أو تسبب إيذاءً محدودًا للمصالح السياسية أو الاقتصادية للمؤسسة .

٢. يجب على المؤسسة وضع وإعلان التعليمات المناسبة للكشف عن هذه المعلومات قبل تقديمها لأي جهات خارجية.

٣. يتم تصنيف المعلومات الشخصية على انها "محدودة" ما لم تحدد تعليمات المؤسسة غير ذلك.

- المستوى الثالث: المعلومات السرية

١. معلومات حساسة معدّة للاستخدام الرسمي المحدود، وإذا تم الإفصاح عنها فأنها ستعرض أمن وخصوصية المؤسسة او العاملين فيها للخطر، أو تسبب لهم إيذاءً سياسيًا أو اقتصاديًا، مثل المعلومات التي من المتوقع أن تكون مفيدة للبلاد الأجنبية أو الجهات غير الحكومية.

٢. إن تصنيف المعلومات على انها "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.

- المستوى الرابع: المعلومات السرية للغاية

هي المعلومات التي تعتبر غاية في الحساسية والأهمية للمؤسسة، والتي تعرض أمنها وخصوصيتها والعاملين فيها للخطر الشديد في حالة تعرضها للتلف او الضياع او التسريب، 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 للمؤسسة او العاملين فيها، أو يعرض 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.

س٨.٣.٤ حفظ المعلومات و تداولها واتلافها

١. حفظ المعلومات

- يجب أن تتوافق عملية حفظ المعلومات مع مستويات تصنيفها.
- يجب حفظ جميع وسائط التخزين الثابتة والمتحركة في مكان أمن حسب تصنيف المعلومات المخزنة فيها. فمثلا 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.

٢. تداول المعلومات ونقلها

- يجب تداول المعلومات في المؤسسة بطريقة تضمن حمايتها من الوصول إليها أو الإفصاح عنها أو تغييرها بشكل غير مرخص أو فقدانها، ولهذا، فأنها يجب أن تعالج وتحفظ حسب مستويات تصنيفها في سبيل حماية سريتها ومستوى حساسيتها وسلامتها وتوافرها.
- على المؤسسة 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 وغيرها من السياسات التي تضمن الحفاظ على المعلومات.

٣. إتلاف المعلومات

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

٤. اليات حفظ و تداول واتلاف المعلومات

التصنيف	الحفظ		التداول		الاتلاف	
	غير الكتروني	الكتروني	غير الكتروني	الكتروني	غير الكتروني	الكتروني

المعلومات العادية						
المعلومات المحدودة						

المعلومات السرية						
المعلومات السرية للغاية						

بعض التوجيهات المتعلقة بحفظ المعلومات وتداولها وإتلافها١جدول

س٨.٣.٥ مسؤولية أمن وحماية المعلومات

١. جميع معلومات المؤسسة هي مسؤولية كل من يتعامل معها.
٢. تتحمل الإدارة العليا للمؤسسة المسؤولية النهائية في أمن وحماية المعلومات لذا يجب عليها وضع ومتابعة وتنفيذ التعليمات والضوابط المتعلقة بالحفاظ على المعلومات.

س٨.٣.٦ مسؤولية مدير أمن المعلومات

١. مراقبة أي خروقات لسياسة أمن المعلومات ورفع التقارير بشأنها لمسؤول المعلومات.
٢. التأكد من أن جميع المستخدمين على علم بكيفية تداول وحماية المعلومات بطريقة تتناسب مع تصنيفها.
٣. تطوير إجراءات أمن وحماية المعلومات في المؤسسة.

س٨.٣.٧ وسم المعلومات

١. على المؤسسة وضع التعليمات المناسبة لوسم المعلومات بطريقة توضح المسؤولية عن المعلومات وتصنيفها.
٢. يمَّكن الوسم الصحيح لوسائط تخزين المعلومات العاملين داخل المؤسسة من تداول المعلومات وفقًا للتوجيهات المذكورة في الجدول رقم (١).

س٨.٣.٨ الوعي الخاص بالإفصاح عن المعلومات

١. إن الفهم الصحيح لجميع العاملين داخل المؤسسة بتصنيف المعلومات يساعد على تطبيق التعليمات المناسبة للإفصاح عنها وألية التعامل معها.
٢. على جميع العاملين داخل المؤسسة إدراك التأثيرات المترتبة على الإفصاح عن المعلومات التي من شانها تعريض مصالح المؤسسة والعاملين فيها للخطر، ويجب على المؤسسة وضع تعليمات لضمان تطبيق هذه السياسة.

س٨.٣.٩ العقوبات المترتبة على الإفصاح الغير مرخص عن المعلومات

١. يجب التعميم على جميع العاملين داخل المؤسسة واعلامهم بالإجراءات (العقوبات) المترتبة في حالة الافصاح عن المعلومات بشكل غير مرخص حسب تصنيفها ووسمها بالتوافق مع التشريعات والقوانين النافذة.
٢. يجب أن تغطي هذه الإجراءات (العقوبات) جميع الاحتمالات التي تؤدي الى خرق بأمن المعلومات كسرقة المعلومات وقراءتها والوصول إليها ، ونسخ وطباعة المعلومات بصورة غير مشروعة.
٣. يجب أن تعتمد هذه الإجراءات (العقوبات) على:
   ١- القوانين والأنظمة والسياسات المتبعة داخل الدولة والمؤسسة.
   ٢- تصنيف المعلومات التي تم الإفصاح عنها بشكل غير مرخص.
   ٣- تأثيرات الإفصاح غير المرخص لهذه المعلومات على المؤسسة 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 التاسعة - سياسة سجل أصول نظام المعلومات

س٩.١ الهدف

تحديد وتسجيل جميع أصول نظام المعلومات والاتصالات وحمايتها.

س٩.٢ المجال

جميع أصول نظام المعلومات والاتصالات بما في ذلك الأجهزة والبرامج والخدمات وأصول المعلومات وغيرها.

س٩.٣ تفاصيل السياسة

١. يجب تعيين جميع عناصر نظام المعلومات والاتصالات التي تنشئ أو تخزن أو تعالج أو تنقل المعلومات.
٢. ينبغي تحديد جميع أصول نظام المعلومات والاتصالات (بما في ذلك الأجهزة والبرامج والخدمات) وأصول المعلومات وتوثيقها في سجلات الاصول.
٣. يجب حماية جميع أصول نظام المعلومات والاتصالات من التهديدات الداخلية والخارجية.
٤. . السجل الذي تسجل فيه أصول نظام المعلومات نفسه هو أحد أصول المعلومات التي يجب تصنيفها على أنها سري للغاية.

الفصل السادس : سياسات أمن البيئة المادية

السياسة العاشرة - سياسة حماية البيئة المادية

س١٠.١ الهدف

ضمان أمن وسلامة نظام المعلومات المادية في المؤسسة وتقليل أثر المخاطر والتهديدات البشرية والبيئية وغيرها من المخاطر التي تؤثر على سلامتها وسريتها.

س١٠.٢ المجال

تغطي هذه السياسة موارد نظام المعلومات المادية المملوكة للمؤسسة إضافة الى الأمن المادي للعاملين داخل المؤسسة.

س١٠.٣ تفاصيل السياسة

س١٠.٣.١ قواعد عامة

١. يتم تقسيم المؤسسة من الناحية الأمنية إلى ثلاث مناطق:

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

٢- مناطق محدودة: وهي المناطق الخاصة بالعاملين داخل المؤسسة، ولا يسمح لأي زائر خارجي دخولها بدون صلاحية أو بطاقة أو تخويل مسبق.

٣- مناطق أمنة: وهي المناطق التي لا يسمح فيها لأي شخص بالتواجد فيها، حتى العاملين داخل المؤسسة إلا بصلاحية أو موافقة مسبقة ومكتوبة من الإدارة العليا في المؤسسة.

٢. على جميع العاملين داخل المؤسسة تحمل مسؤولية الالتزام بالتعليمات و الضوابط المتعلقة بالحماية المادية.

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

س١٠.٣.٢ واجبات المؤسسة (واجبات عامة)

١. لكل منطقة من مناطق المؤسسة التي تم ذكرها سابقا (س١٠.٣.١ النقطة ١) ضوابط و تعليمات يجب ان تحدد وتوضع و تنفذ وتتابع من قبل الجهة المعنية بالأمر داخل المؤسسة.

٢. وضع التعليمات الخاصة بالزوار، والصلاحيات الممنوحة لكل منهم في الوصول إلى مرافق المؤسسة ، وكيفية مراقبة سلوك الزوار والإشراف على تحركاتهم داخل المؤسسة.

٣. وضع التعليمات الخاصة بحماية مصادر الطاقة وتوفير مصادر طاقة احتياطية لغرف التحكم والخوادم (Servers) و غيرها من المناطق المهمة وخاصة المناطق الأمنة.

٤. وضع التعليمات الخاصة بأمن التمديدات - لكل من الشبكات والاتصالات والتهوية والمياه والكهرباء وغيرها – وخاصة في المناطق الأمنة.

٥. 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.

٦. توفير واختبار الانظمة الخاصة بإطفاء الحرائق.

٧. إبعاد المواد القابلة للاشتعال أو الانفجار عن المناطق الأمنة.

٨. استخدام وتوظيف ضوابط الأمن والحماية المناسبة للتأكد من خلو الداخلين إلى المؤسسة من أية تهديدات تؤثر على أمنها وسلامة نظام المعلومات داخلها، مثل توظيف حراس الأمن، وأجهزة كشف المعادن، وكاميرات المراقبة، وأجهزة الإنذار وغيرها من مستويات الحماية.

٩. استخدام الإشارات الإرشادية والتحذيرية لبيان الطريقة الصحيحة والأمنة في العمل، مع عدم استخدام أي إشارات أو لافتات تدل على الأماكن الحساسة مثل مراكز البيانات، وغرف المراقبة وغيرها.
١٠. الاحتفاظ بالوسائط والمعدات الاحتياطية في أماكن أمنة تكون في متناول اليد عند الحاجة حسب الآليات التي تحددها المؤسسة.
١١. وضع التعليمات الخاصة بالدخول إلى الأقسام المختلفة في المؤسسة، وتحديد الأشخاص المخولين بالاحتفاظ بالمفاتيح الخاصة بالأقسام والأبواب والغرف، وتمييز الأقسام الحساسة بضوابط دخول مناسبة، مثل بطاقات المرور.
١٢. توظيف وسائل الحماية المناسبة لكل من النوافذ والأبواب والأقسام، مثل شبك الحماية على النوافذ، والأقفال على أبواب الأقسام.
١٣. توفير القاصات والخزائن والغرف القابلة للقفل والمضادة للحريق لحماية مكونات نظم المعلومات الحساسة.
١٤. توظيف مبدأ (الحماية من العمق) في حماية المؤسسة وموارد نظام المعلومات بما يتناسب وأهمية النظام وحساسية المعلومات المتداولة.

س١٠.٣.٣ واجبات المؤسسة (إدارة الأصول)

إدارة الأصول بمعناها العام، تشير إلى أي نظام يقوم بمراقبة الممتلكات القيمة المملوكة للمؤسسة ويحافظ عليها. وهذا التعريف قد ينطبق على الأصول المادية مثل المباني وينطبق على المفاهيم المعنوية مثل البرامج وأنظمة التشغيل وغيرها لذا على المؤسسة الالتزام بالتالي:

١. أن تكون جميع أصول نظام المعلومات والاتصالات موجودة في مناطق أمنة مع وجود آليات للتحكم في الوصول لها لتقييد استخدامها الا للعاملين داخل المؤسسة المصرح لهم فقط.
٢. يجب تنفيذ السياسات والعمليات لرصد وحماية واستخدام وصيانة أصول نظام المعلومات والاتصالات داخل المؤسسة وخارجها.
٣. يجب تنفيذ السياسات والعمليات للتخلص الأمن من أصول نظام المعلومات والاتصالات أو إعادة استخدامها، بما يتناسب مع مستوى تصنيف أمان أصول المعلومات.

٤. بعض الأمور الواجب مراعاتها في إدارة الأصول:

- كيف وأين يتم وضع المعدات الهامة ؟
- ما هي الضمانات الواجب تطبيقها ؟
- ما هي الضمانات المعمول بها لإمدادات الطاقة للمعدات الحيوية؟
- كيف يتم حماية الكابلات ؟
- كيف ومن الذي يسمح له بإجراء الصيانة على المعدات؟
- ما هي السياسة المتعلقة بأمان المعدات المحفوظة خارج الموقع (على سبيل المثال، معدات الاستخدام المنزلي، والمعدات المحمولة)؟
- من يأذن بالتخلص من المعدات وإعادة استخدامها؟

س٤.٣.١٠ واجبات المؤسسة (التعليمات الخاصة بزوار المؤسسة)

تختلف إجراءات الوصول للزوار، اعتمادًا على طبيعة الزيارة ومستوى المخاطرة في كل منطقة عمل.

وعليه:

١. لا يجوز السماح لزوار المناطق التي تحتوي على قدر كبير من المعلومات الحساسة بحرية التنقل بدون مرافق معرف من قبل المؤسسة وموافقة مسبقة من قبل الجهة المعنية بالأمر داخل المؤسسة.
٢. من الموصي به أن يتم إرسال إخطار لمسؤول الدخول عن هوية الزائر وما إذا كان الزائر يحتاج إلى مرافقة داخل المبنى.
٣. يجب على الزائرين عند الوصول إصدار تصريح ومرافقتهم إما إلى غرفة الانتظار أو إلى المسؤول المضيف.
٤. غرفة الانتظار يجب ان تكون مراقبة .
٥. يجب تغطية سجل اسماء الزوار لمنع الزوار من رؤية تفاصيل الزوار الآخرين.
٦. من الموصي به أن يُطلب من الزوار بأنه لن يتم التقاط صور فوتوغرافية أو تسجيلات من أي نوع في أي وقت أثناء الزيارة خاصة في المناطق الأمنة .

٧. من الموصي به أن يُطلب من الزوار إيداع الهواتف والاجهزة المحمولة وغيرها من المعدات في مكتب الاستقبال.
٨. ينبغي ترتيب الوصول والخروج من مناطق الزيارة لتجنب الدخول إلى مناطق العمل حيث قد تكون المواد الحساسة معروضة أو يمكن الوصول إليها.

س١٠.٣.٥ واجبات المؤسسة (العاملين داخل المؤسسة خارج أوقات العمل الرسمي)

١. يجب على المؤسسة تحديد ما إذا كان هناك أي خطر على أمن المعلومات يتعلق بالأفراد الذين يعملون خارج أوقات العمل الرسمي.
٢. كل العاملين داخل المؤسسة الذين يعملون خارج أوقات العمل الرسمي يجب ان تكون لديهم موافقة كتابية من المسؤول المباشر إضافة الى مسؤول أمن المؤسسة ومسؤول أمن المعلومات.
٣. يتم تحديد سياسات المؤسسة وممارساتها المتعلقة بالعاملين داخل المؤسسة الذين يعملون خارج أوقات العمل الرسمي من خلال جميع العوامل ، بما في ذلك قضايا الصحة والسلامة المهنية.
٤. يجب على المؤسسة الاحتفاظ بسجل للعاملين داخل المؤسسة الذين لديهم إمكانية الوصول بعد ساعات العمل (بما في ذلك المغادرة المتأخرة والوصول المبكر).
٥. تطوير الوعي الأمني للعاملين داخل المؤسسة الذين عادة ما يحتاجون إلى الوصول إلى مكان العمل بعد ساعات العمل الغير رسمي.
٦. إذا تبين أن أحد العاملين داخل المؤسسة يمتلك ساعات عمل خارج أوقات الدوام الرسمي بصورة تزيد عن الحد الطبيعي لأداء المهام الموكلة اليه و دون أن تكون الأسباب واضحة ، فمن المستحسن أن يقوم مدير أمن المؤسسة ومدير أمن المعلومات وبالتنسيق مع مدير المؤسسة بإجراء تحقيقات سرية لتحديد السبب.

س١٠.٣.٦ واجبات المؤسسة (المؤتمرات والاجتماعات)

١. قبل بدء الاجتماع ، تأكد من عدم وجود أشخاص غير مصرح بهم في القاعة.

٢. يجب التأكد من عدم وجود مواد ومواضيع لا تتعلق بموضوع الاجتماع أو غير مناسبة للعرض لأنها تمس أمن المعلومات بالخطر.
٣. تقييم المخاطر الأمنية المحتملة الناشئة عن تصميم المكتب وما قد يكون مرئيًا أو مسموعًا أثناء الاجتماعات (من ضمنها الاجتماعات الفديوية او الصوتية) .
٤. النظر في مخاطر السمع / التنصت إذا ما تم بث الكلام من خلال سماعات الصوت داخل قاعة الاجتماع .
٥. لا يتم تسجيل المكالمات الصوتية والمرئية ألا بإذن صريح من جميع المشاركين وحسب مقتضيات مصلحة العمل.
٦. قد توفر الستائر الصافية أو الزجاج المعتم الحماية. عندما تكون الغرفة مضاءة بشكل طبيعي ، ولكن الستائر الصافية لا توفر الحماية دائمًا ، ويوصى باستخدام الستائر الغامقة ويمكن استخدام الستائر المعدنية لتقليل المخاطر إلى الحد الأدنى.
٧. يجب التخطيط لترتيب الجلسة بصورة مناسبة عند حضور اشخاص غير مصرح لهم بالطلاع على معلومات حساسة ، بطريقة تؤدي الى عدم إمكانية مشاهدة الوثائق الرسمية .
٨. قبل مغادرة غرفة الاجتماعات، يوصى بما يلي:
   ١- مسح اللوحات البيضاء.
   ٢- إزالة محركات الأقراص وأجهزة الخزن المحمولة والأجهزة الإلكترونية المحمولة الأخرى.
   ٣- إزالة أي مستندات حساسة والتخلص منها بشكل أمن إضافة الى التأكد من عدم وجود معلومات أو بقايا قصاصات أو نفايات تحتوي معلومات مهمة او حساسة في غرفة الاجتماع.

س١٠.٣.٧ واجبات المؤسسة (العاملين داخل المؤسسة المساعدون او المؤقتين)

١. اجراء التدقيق الأمني على العاملين المساعدون او المؤقتين وهذا لا يعتبر بديل تدابير الأمن المادي.
٢. يجب على المؤسسة التأكد من أن العاملين المساعدون او المؤقتين (الحراس ، عمال النظافة ، الديكور ، عمال الصيانة ، ، إلخ) لا يمكنهم الوصول إلى الوثائق أو المعدات الحساسة او أي شيء من مكونات نظم المعلومات ولا يسمعون المناقشات في المسائل الحساسة.

س١٠.٣.٨ واجبات مدير أمن المعلومات

١. القيام بعملية التوعية الخاصة بالأمن الماديّ داخل المؤسسة.
٢. التنسيق مع الجهات المعنية في المؤسسة (وخارجها) في تطوير وتقييم وإعادة هيكلة إجراءات الأمن المادي لنظام المعلومات في المؤسسة، ورفع التوصيات الخاصة بذلك إلى الإدارة العليا في المؤسسة.
٣. متابعة البلاغات والتقارير الخاصة بوقوع أية مخاطر أو تهديدات تتعلق بالأمن المادي لنظام المعلومات ، والتنسيق مع الجهات المعنية داخل المؤسسة بطريقة تتوافق مع هذه الوثيقة.
٤. التدقيق على مدى توافق الضوابط والإجراءات الخاصة بالأمن المادي لنظام المعلومات في المؤسسة مع هذه الوثيقة وخاصة سياسة الأمن الماديّ، ورفع التقارير الدورية للإدارة العليا في المؤسسة.
٥. الإشراف والتدقيق على تطبيق التعليمات الخاصة بالأمن الماديّ لنظام المعلومات داخل المؤسسة.

س١٠.٣.٩ واجبات العاملين داخل المؤسسة

١. تطبيق مبدأ المكتب النظيف (سياسة تأمين المكتب) وتأمينه عند المغادرة من خلال التأكد من إغلاق النوافذ والخزائن والابواب على سبيل المثال.
٢. الابتعاد عن التدخين والأكل والشرب واستخدام المواد القابلة للاشتعال أو الانفجار داخل المناطق الأمنة خاصة والمناطق التي تحتوي على مواد قابلة للاشتعال.
٣. الابتعاد عن وضع او رفع وقراءة الوثائق ذات المعلومات الحساسة بالقرب من النوافذ وذلك تجنبا لتصويرها من الخارج خصوصا مع وجود التقنيات الحديثة.
٤. عدم التحدث بصوت مرتفع عن معلومات مهمة او حساسة تخص المؤسسة او أي معلومات تخص جهات أخرى مرتبطة بالمؤسسة قد يؤثر افشاءها الى الضرر بأمن و سلامة المعلومات وخصوصا قرب النوافذ او إذا كانت المكاتب الأخرى ملاصقة للمكتب و قريبة من الممرات العامة و السلالم.

السياسة الحادية عشر - سياسة استخدام جهاز الحاسوب

س١١.١ الهدف

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

س١١.٢ المجال

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

س١١.٣ تفاصيل السياسة

س١١.٣.١ واجبات المؤسسة

١. وضع التعليمات المناسبة في التعامل مع أجهزة الحاسوب المكتبية المملوكة للمؤسسة، وشرائها وإصلاحها ونقلها وإتلافها، بالتوافق مع هذه الوثيقة عامّة وسياسة حساسية وتصنيف المعلومات خاصّة.
٢. وضع التعليمات والآليات التي يتم بها توزيع أجهزة الحاسوب المكتبية على العاملين داخل المؤسسة، وتحديد الصلاحيات المناطة حسب الحالة الوظيفية والوصف الوظيفي ووفق ما تقتضيه طبيعة العمل.
٣. وضع التعليمات الخاصة بتحديد وسائط التخزين التي يسمح باستخدامها، ووضع الضوابط والشروط التي تحدد استعمالها - مثل تشفير الملفات المخزّنة

٤. وضع التعليمات الخاصة بربط أجهزة الحاسوب المكتبية بأية معدات - مثل البلوتوث وال (واي-فأي) أو بالشبكة المعلوماتية للمؤسسة بنوعيها السلكية واللاسلكية بالتوافق مع سياسة أمن الشبكات.
٥. التدقيق على جميع أجهزة الحاسوب المكتبية ، بما فيها الأجهزة المشمولة باتفاقية التعاقد الخارجي مع أي مزود خارجي له أجهزة حاسوب مكتبية في المؤسسة بالتوافق مع سياسة التدقيق الخاص بأمن المعلومات.

س١١.٣.٢ واجبات مدير النظام

١. إعداد أجهزة الحاسوب المكتبية في المؤسسة بما يتوافق مع هذه الوثيقة.
٢. 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 تبعًا لسياسة ضبط التغيير وسياسة الاستعمال المقبول.
٣. التعامل مع وسائط التخزين، مثل الأقراص الصلبة والمرنة والمضغوطة في حالة تغييرها أو نقلها أو إتلافها بالتوافق مع سياسة حساسية وتصنيف المعلومات.
٤. توزيع أجهزة الحاسوب المكتبية داخل الغرف بشكل يحميها من اختلاس النظر بقدر الاستطاعة.
٥. ربط أجهزة الحاسوب المكتبية بالشبكة المعلوماتية في المؤسسة وعزلها عنها اذا تطلب الامر، اعتمادًا على الصلاحيات الممنوحة للعاملين داخل المؤسسة.
٦. إنشاء وحذف وإدارة سجلات الدخول الإلكترونية لكل جهاز حاسوب مكتبي، سواءً أكان متصلا بالشبكة المعلوماتية أم لا.
٧. وضع كلمة مرور خاصة لحماية أجهزة الحاسوب المكتبية من دخول الأشخاص غير المخوّلين إلى إعدادات البايوس BIOS إضافة الى نظام التشغيل.
٨. 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.
٩. تنصيب حافظات شاشة Screen Savers موحدة للحواسيب المكتبية حسب تعليمات المؤسسة.

١٠. حماية حافظات الشاشة Screen Savers عن طريق استخدام كلمة مرور بعد ترك العمل على الأجهزة لفترة معينة.

س١١.٣.٣ واجبات العاملين داخل المؤسسة (المستخدمين)

١. التعامل مع أجهزة الحاسوب المكتبية بشكل يتوافق مع هذه الوثيقة وتعليمات المؤسسة.
٢. العامل داخل المؤسسة مسؤول عن حفظ كلمة المرور الخاصة بالدخول إلى حاسوبه المكتبي بالتوافق مع سياسة كلمات المرور.
٣. العامل داخل المؤسسة مسؤول عن إبلاغ الدعم الفني بأي مشكلة تصيب حاسوبه المكتبي، وعليه عدم محاولة إصلاحه بنفسه بالتوافق مع سياسة الاستعمال المقبول.
٤. عدم ربط أي جهاز أو وسيط تحزين أو معدات لاسلكية -مثل البلوتوث وال (واي-فأي) - مع الشبكة المعلوماتية للمؤسسة، أو مع أي من الأجهزة والمعدات الأخرى، بدون الحصول على موافقة مسبقة ومكتوبة من الإدارة العليا في المؤسسة و مدير أمن المعلومات.
٥. عدم إحضار أو ربط أجهزة الحاسوب المكتبية الغير عائدة للمؤسسة بالشبكة المعلوماتية التابعة للمؤسسة.
٦. عدم استخدام وسائط التخزين المتنقلة بدون فحصها ببرامج مكافحة الفيروسات.
٧. حفظ المعلومات والملفات على الأجهزة التي يحددها مدير النظام مثل خوادم الملفات (File Server) بالتوافق مع سياسة أمن الشبكات.
٨. عدم استخدام جهاز الحاسوب التابع للمؤسسة للأغراض الشخصية.

السياسة الثانية عشر - سياسة استخدام جهاز الحاسوب اللوحي

س١٢.١ الهدف

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

س١٢.٢ المجال

تغطي هذه السياسة جميع الأجهزة المحمولة المملوكة للمؤسسة، مثل أجهزة الحاسوب المحمولة، وأجهزة الاتصال النقالة، والأجهزة المحمولة الأخرى كما تغطي كافة العاملين داخل المؤسسة الذين يستخدمون هذه الأجهزة.

س١٢.٣ تفاصيل السياسة

س١٢.٣.١ قواعد عامة

١. على المؤسسة وضع التعليمات الخاصة بمنح و توزيع الأجهزة المحمولة على المستخدمين حسب الحالة الوظيفية والوصف الوظيفي ووفقًا لما تقتضيه طبيعة العمل.

٢. على المؤسسة وضع التعليمات والآليات الخاصة بإدارة ومراقبة وحماية الأجهزة المحمولة المملوكة لها داخل وخارج المؤسسة، وتحديد المعايير التي تحكم سلوك استخدام أجهزة الاتصال النّقالة والأجهزة الذكية المحمولة داخل المؤسسة.
٣. لا يسمح باستخدام الأجهزة المحمولة الخاصة بالمؤسسة لمنفعة أي جهة أخرى أو لغير العمل الرسمي.
٤. لا يسمح بربط أي جهاز محمول يملكه المستخدم بالشبكة المعلوماتية للمؤسسة أو أيٍّ من مكونات نظم المعلومات للمؤسسة بدون موافقة مسبقة ومكتوبة من الإدارة العليا في المؤسسة. ومدير أمن المعلومات.
٥. لا يسمح بتخزين أو إخراج الملفات التي ينص القانون على عدم إخراجها من المؤسسة على الأجهزة المحمولة حتى وإن كانت مشّفرة.

س١٢.٣.٢ واجبات مدير النظام

١. تطبيق معايير أمن وسلامة المعلومات التي يتم التعامل معها أو تخزينها أو معالجتها من خلال الأجهزة المحمولة المملوكة للمؤسسة بالتوافق مع هذه الوثيقة و التعليمات المتبعة في المؤسسة عامة ، وكل من سياسة الحاسب المكتبي، وسياسة الاستعمال المقبول، وسياسة مكافحة الفيروسات والبرامج الخبيثة خاصّة.
٢. حماية الأجهزة المحمولة بكلمات مرور لكل من (البايوس) BIOS ونظام التشغيل.
٣. منح وحجب الصلاحيات المتعلقة باستخدام الأجهزة المحمولة وتغيير إعداداتها.
٤. تشفير الملفات الموجودة على الأجهزة المحمولة المملوكة للمؤسسة بالتوافق مع سياسة حساسية وتصنيف المعلومات.
٥. إجراء عملية نسخ احتياطي للمعلومات المخزّنة على الأجهزة المحمولة بشكل دوريّ.

س١٢.٣.٣ واجبات العاملين داخل المؤسسة (المستخدمين)

١. العامل في المؤسسة (المستخدم) مسؤول عن أية أعطال أو ضياع أو تغيير أو الإفصاح عن المعلومات بشكل غير مرخص يمكن أن يحدث للجهاز المحمول المملوك للمؤسسة سواءً عن طريقه أو عن طريق أي شخص آخر استخدمه بمعرفته أو لإهماله.
٢. حماية الأجهزة المحمولة المملوكة للمؤسسة والتي له صلاحية استخدامها.
٣. عدم إحضار أو ربط الأجهزة المحمولة التي يملكها العامل في المؤسسة (المستخدم) بالشبكة المعلوماتية الخاصة بالمؤسسة.
٤. عدم استخدام الأجهزة المحمولة العائدة للمؤسسة للأغراض الشخصية.

السياسة الثالثة عشر - سياسة تأمين المكتب (المكتب النظيف)

س١٣.١ الهدف

الغرض من هذه السياسة هو تحديد الحد الأدنى من المتطلبات للحفاظ على "مكتب نظيف" - حيث تكون المعلومات وحسب تصنيفها المتبع في المؤسسة أمنة وذلك للتقليل من خطر وقوع حادث أمني والحفاظ على الوثائق الحساسة التي تترك على سطح المكتب من السرقة.

س١٣.٢ المجال

تنطبق هذه السياسة على جميع العاملين داخل المؤسسة.

س١٣.٣ تفاصيل السياسة

١. يجب على جميع العاملين داخل المؤسسة التأكد من أن جميع المعلومات الحساسة أو السرية في شكل ورقي أو إلكتروني أمنة في منطقة عملهم في نهاية اليوم.
٢. خلال أوقات العمل الرسمي يجب ان يحرص العاملين داخل المؤسسة على ان تكون الوثائق المهمة في أظرف او ملفات لمنع الاطلاع عليها او كحد أدني غير قابلة للمشاهدة في حالة العمل عليها بصورة مباشرة.
٣. يجب ان يقوم العاملين داخل المؤسسة بقفل حساباتهم الخاص على جهاز الحاسوب عندما تكون مساحة العمل غير مشغولة.
٤. يجب إطفاء جهاز الحاسوب المكتبي او أجهزة الحاسوب المحمولة والأجهزة اللوحية تمامًا في نهاية يوم العمل الا إذا تم استحصال موافقة خطية من مدير أمن المعلومات و ذلك لدواعي و ضرورة مصلحة العمل.
٥. يجب إزالة أي معلومات سرية أو حساسة من المكتب ووضعها في درج مقفل عندما يكون المكتب غير مأهول وفي نهاية يوم العمل يأخذ نفس الاجراء.
٦. يجب غلق وقفل خزانات الملفات التي تحتوي على معلومات سرية أو حساسة.
٧. يجب ألا تترك المفاتيح المستخدمة للوصول إلى المعلومات السرية أو الحساسة في مكتب غير مراقب او سهل الوصول.
٨. يجب أن تكون أجهزة الحاسوب المحمولة مغلقة إما بكبل قفل أو مغلقة في درج مقفل.
٩. لا يجوز ترك كلمات المرور على الملاحظات اللاصقة المنشورة على جهاز الحاسوب، كما لا يجوز تركها مكتوبة في مكان يسهل الوصول إليه.
١٠. في حالة طباعة الوثائق التي تحتوي على معلومات سرية أو حساسة يجب اخذها على الفور من الطابعة هذا يساعد على ضمان عدم ترك الوثائق الحساسة في ادراج الطابعة ليحملها الشخص الخطأ.
١١. في حالة اتلاف الوثائق التي تحتوي على معلومات مهمة يحب اتلافها في صناديق التقطيع الرسمية.
١٢. يجب محو اللوحات البيضاء التي تحتوي على معلومات سرية أو حساسة.
١٣. تعامل أجهزة التخزين المتنقلة على أنها حساسة ويتم تأمينها في درج مقفل.

١٤. يجب تدقيق جميع الطابعات وأجهزة الفاكس في نهاية اليوم وضمان عدم ترك أي أوراق مهمة فيها.

الفصل السابع : سياسات تكنولوجيا الاتصالات والمعلومات

السياسة الرابعة عشر - سياسة التعاقد الخارجي

س١٤.١ الهدف

ضمان أمن وحماية المعلومات وأنظمة تكنولوجيا المعلومات وسلامتها وتوافرها وخصوصيتها أثناء الاستعانة بمزود خارجي لتوفير خدمات معينة للمؤسسة.

س١٤.٢ المجال

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

س١٤.٣ تفاصيل السياسة

س١٤.٣.١ سياسات عامة

١. تكون الاستعانة بمزود خارجي ناتجة عن اتفاقية موقعة بين المؤسسة و المزود الخارجي على ان يكون الأخير على درجة عالية من الكفاءة والأمان لنجاح مهمة التعاقد الخارجي بشكل أمن وصحيح وفعّال.
٢. يجب ألا تكون الخدمات المعلوماتية التي يراد الاستعانة بمزود خارجي من أجلها جوهرية وحرجة، واذا اضطر الامر لذلك يجب ان يتم التنسيق بين الإدارة العليا ومدير أمن المعلومات في المؤسسة

والفريق الوطني للاستجابة للأحداث السيبرانية وذلك لتحديد وتقييم المخاطر المحتمل وقوعها في حالة الاستعانة بطرف خارجي.

٣. يجب ألا يؤدي التعاقد الخارجي إلى انقطاع أو تأثير في استمرارية الخدمات المقدمة في المؤسسة.
٤. إذا كانت الخدمة التي سيتم التعاقد الخارجي من أجلها هي التدقيق على نظام المعلومات ، فيجب موافقة الفريق الوطني للاستجابة للأحداث السيبرانية .

س١٤.٣.٢ واجبات المؤسسة

١. تحديد وتوثيق توصيات جميع الأقسام التي لها علاقة بالخدمات التي سيتم الاستعانة بطرف خارجي من أجل تقديمها.
٢. يجب أن تكون جميع مكونات نظم المعلومات المشمولة أو المتعلقة بالتعاقد الخارجي موثقة وخاضعة للتدقيق تبعًا لهذه الوثيقة، وتبعًا للاتفاقية بين المؤسسة والجهة المزودة، من خلال الآلية المتبعة في المؤسسة في التدقيق.
٣. تحديد وتوثيق آلية إعادة مكونات نظم المعلومات ونقلها وإتلافها بطريقة أمنة عند انتهاء اتفاقية الاستعانة بالمزود الخارجي.
٤. تحديد وتوثيق أسماء العاملين الذين سيباشرون بتزويد الخدمة من الطرف الخارجي، والموافقة أمنياً عليهم قبل مباشرة أعمالهم، وانهم يحققون شروط العمل والأمن اللازمة لتعيينهم حسب السياسة المتبعة في المؤسسة، وبشكل خاص سياسة أمن العاملين داخل المؤسسة.
٥. تحديد وتوثيق المعايير اللازمة لقياس ومتابعة وتقييم فعالية الخدمات التي تم التعاقد الخارجي من أجلها، وخطوات مراقبة الحوادث الأمنية الممكن حدوثها ورفع التقارير بشأنها.
٦. تحديد وتوثيق الضوابط والحماية اللازمة في إدارة ونقل وإتلاف المعلومات والخدمات ومواردها ونقل وتبادل الموظفين بين المؤسسة والمزود الخارجي.
٧. تحديد وتوثيق الشروط الجزائية والغرامات عن أي خلل ينتج عن المزود الخارجي في تقديم خدماته بشكل يخل بأمن المعلومات في المؤسسة.
٨. تحديد وتوثيق جميع المؤهلات والمتطلبات والمهام والمسؤوليات اللازم تنفيذها من قبل المزود الخارجي.

٩. التأكد من تطبيق مبدأ "الفصل بين المهام" بين كل من المؤسسة والمزود الخارجي.
١٠. التحقق من مطابقة ممارسات وإجراءات الأمن والحماية التي يتبعها المزود الخارجي ، ومدى توافقها مع هذه الوثيقة.

س٣.٣.١٤ واجبات المزود الخارجي

١. تحديد مستوى الخدمة يجب ان يحدد من قبل المستهلك (المؤسسة) لذا يجب ان تحدد المتطلبات ونوع الخدمات وجودتها في "اتفاقية مستوى الخدمة" ويجب على مزود الخدمة ان يلتزم بها .
٢. توقيع اتفاقية "عدم الإفصاح بشكل غير مرخص عن المعلومات" والمعنيّة بعدم إفصاح المزود الخارجي عن أي معلومات (هي ملك للمؤسسة) يتم الاطلاع عليها بحكم عمله ويجب ان تتلاءم هذه الاتفاقية مع وثيقة السياسات والمعايير لأمن المعلومات والاتصالات .
٣. توقيع تعهد بأنه لا يحوز حذف او الوصول او التعديل لأي من مكونات نظم المعلومات المملوكة للمؤسسة الغير متعلقة ببنود الاتفاق او بدون الحصول على اذن مسبق من المؤسسة وذلك لغرض انجاز المهام الموكلة لمزود الخدمة.
٤. عدم تشفير أي من الخدمات أو الأنظمة أو المعلومات أو الاتصالات بدون معرفة مسبقة من المؤسسة بآلية التشفير وفكه بنفسها، بالتوافق مع سياسة التشفير.
٥. توفير المؤهلات والكوادر والكفاءات والقدرات الكافية بطريقة مثبتة وموثقة للقيام بدور المزود الخارجي، وأن يكون متقدمًا في المجال الذي سيتم التعاقد معه من أجله.
٦. حماية مكونات نظم المعلومات التابع للمؤسسة وذلك بضمان سرية وسلامة وتوافرية وخصوصية المعلومات والخدمات المتعاقد من أجلها، بالتوافق مع هذه الوثيقة.
٧. التزام عملية ضبط التغيير المعمول بها في المؤسسة.
٨. التعاون مع أي عملية تدقيق تقوم بها المؤسسة (داخلي او خارجي) بالتوافق مع سياسة التدقيق الخاص بأمن المعلومات.
٩. تزويد المؤسسة بخططه المتعلقة باستمرارية الأعمال والاسترداد عند وقوع كارثة تتعلق بالخدمات المقدمة من قبله.
١٠. تطبيق مبدأ "الفصل بين المهام" بين كل من المؤسسة والمزود الخارجي.

١١. تحديد آلية اتصال متفق عليها مع المؤسسة عند وقوع أي حادث أمني قد يؤثر على أمن وسلامة وتوافرية الخدمات التي تم التعاقد الخارجي من أجلها أو غيرها من مكونات نظم المعلومات.

١٢. رفع وتوثيق تقارير مفصلة للمؤسسة عن الخدمات التي تم التعاقد الخارجي لتزويدها، على أن تشمل العناصر التالية:

- إجراءات الأمن والحماية.
- الحوادث والخروقات الأمنية، وأية أخطاء قد تصيب الخدمات التي تم التعاقد الخارجي من أجلها أو غيرها من مكونات نظم المعلومات، وكيفية معالجتها.
- أسماء العاملين المسؤولين عن حماية هذه الخدمات و مكونات نظم المعلومات وأي تغييرات تتعلق بتعيينهم أو مسؤولياتهم أو كيفية الاتصال بهم، ومدى الصلاحيات الممنوحة لكل منهم.
- الإجراءات المتبعة في استلام ونقل وإتلاف أية موارد لنظام المعلومات مشمولة أو لها علاقة بالتعاقد الخارجي.

السياسة الخامسة عشر - سياسة النسخ الاحتياطي

س١٥.١ الهدف

ضمان أمن وحماية المعلومات عن طريق أخذ نسخة احتياطية وخزنها واسترجاعها عند الحاجة بطريقة أمنة وصحيحة.

س١٥.٢ المجال

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

س١٥.٣ تفاصيل السياسة

س١٥.٣.١ واجبات المؤسسة

١. توظيف البرمجيات والمعدات المناسبة للنسخ الاحتياطي.
٢. وضع التعليمات وتحديد الآليات والإجراءات المناسبة لعملية النسخ الاحتياطي بما يتفق وهذه السياسة.
٣. على المؤسسة مراعاة سياسة التعاقد الخارجي عند توكيل جهات خارجية لحماية وسائط النسخ الاحتياطي.
٤. وضع آلية واضحة لتخزين وسائط النسخ الاحتياطي في أماكن خارجية عند الحاجة.

س١٥.٣.٢ واجبات مدير النظام

١. منح وحجب الصلاحيات اللازمة للمسؤولين عن عملية النسخ الاحتياطي أو استرجاع المعلومات.
٢. متابعة عملية النسخ الاحتياطي وعملية استرجاع المعلومات للتأكد من انها تتم بشكل صحيح وأمن.
٣. تشفير المعلومات المخزنة على وسائط النسخ الاحتياطي حسب سياسة حساسية وتصنيف المعلومات وسياسة التشفير.
٤. وسم وسائط التخزين والنسخ الاحتياطي بدرجة حساسية وتصنيف المعلومات المخزنة داخلها وحمايتها في مكان أمن حسب وسمها بالتوافق مع سياسة حساسية وتصنيف المعلومات.
٥. تطبيق الجدولة المتبعة في المؤسسة لعملية النسخ الاحتياطي.
٦. مراعاة موضوع العدد وموضوع التوزيع الجغرافي المحلي والإقليمي في الحفظ المكاني للنسخ الاحتياطية اعتمادا على حساسية المعلومات المخزّنة.
٧. رفع تقارير دورية إلى الإدارة العليا في المؤسسة حسب التعليمات المعمول بها في المؤسسة تبين النقاط التالية:
   - تاريخ النسخة الاحتياطية.
   - المعلومات التي تم نسخها احتياطياً.
   - أسماء الأشخاص الذين لهم حق الوصول إلى المعلومات المخزّنة في وسائط النسخ الاحتياطي.

- أسماء الأشخاص الذين تمت لهم عملية استرجاع الملفات.
- تواريخ استخدام النسخ الاحتياطية.
- الأسباب التي دعت إلى استخدام النسخ الاحتياطية.
- الجهات والأماكن التي يتم حفظ وسائط النسخ الاحتياطي فيها.
- تاريخ بدء استخدام وسائط النسخ الاحتياطي وانتهاء صلاحيتها.

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

س١٥.٣.٣ واجبات مدير أمن المعلومات

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

س١٥.٣.٣ واجبات العاملين داخل المؤسسة (المستخدمين)

١. حفظ المعلومات والملفات على الأجهزة التي يحددها مدير النظام مثل خوادم الملفات (File Server) والتي يتمّ نسخها احتياطياً بشكل دوري، ويُمنع حفظها على أية وسائط غيرها، مثل مواقع الإنترنت أو وسائط تخزين شخصية.
٢. العمل بالتعليمات والإجراءات المتبعة في المؤسسة عند الحاجة الى استرجاع المعلومات وتقديم طلب الاسترجاع الى مدير النظام بعد موافقة المسؤول المباشر.

السياسة السادسة عشر - سياسة أمن الشبكات

س١٦.١ الهدف

الهدف الرئيسي هو الوصول إلى شبكة مستقرة وأمنة قادرة على تلبية متطلبات العمل الخاص بالمؤسسة وذلك من خلال توضيح ألية التعامل مع عناصر شبكة المعلومات وتحديد الأمور المطلوب توافرها في هذه العناصر لضمان أمن وحماية الأنظمة المرتبطة بالشبكة.

س١٦.٢ المجال

تغطي هذه السياسة جميع العناصر والمكونات المتعلق عملها بشبكة نظام المعلومات التابعة للمؤسسة بنوعيها السلكية واللاسلكية ، أضافة الى كل البنية التحتية للاتصالات.

س١٦.٣ تفاصيل السياسة

س١٦.٣.١ واجبات المؤسسة

١. وضع التعليمات المناسبة في التعامل مع عناصر الشبكة التابعة للمؤسسة ، وشرائها وإصلاحها ونقلها وإتلافها، بما يتفق مع هذه الوثيقة عامًة وسياسة حساسية وتصنيف المعلومات وسياسة الاستعمال المقبول خاصًة.
٢. وضع التعليمات والضوابط الخاصة بربط عناصر الشبكة مثل الخوادم (Servers) والموجهات (Routers) وغيرها من معدات الشبكة.
٣. وضع التعليمات والآليات الخاصة ببيئة عمل هذه الشبكات ، مثل تشغيلها في أماكن أمنة وبعيدة عن أيدي المستخدمين، وتوفير بيئة مناسبة لها بالتوافق مع سياسة الأمن المادي.
٤. وضع الصلاحيات المناسبة للعاملين داخل المؤسسة المتخصصين بتشغيل وصيانة وإدامة عمل الشبكة اعتمادًا على الوصف الوظيفي لكل منهم.

٥. التوثيق الكامل للشبكة يشمل رسومات واضحة ومفهومة للشبكة تحدد عناصرها وطريقة ربطها بعضها ببعض.
٦. تخزين الإعدادات الخاصة بأجهزة الشبكة في مكان أمن، من أجل توفير إمكانية إرجاع الإعدادات السابقة وذلك بالتوافق مع سياسة النسخ الاحتياطي.
٧. ترقية (تحديث وتطوير) نظم التشغيل والبرامج المشغلة للشبكة في حال توجب ذلك، مثل حدوث اختراق أو خلل في عناصر الحماية الخاصة بالشبكة.
٨. وضع كلمات مرور سرية للدخول إلى الشبكة تعطى للعاملين داخل المؤسسة المخولين، وذلك بالتوافق مع سياسة كلمات المرور.
٩. التدقيق على جميع العناصر المكونة لهذه الشبكات، بما فيها الأجهزة المشمولة باتفاقية التعاقد الخارجي وبالتوافق مع سياسة التدقيق الخاص بأمن المعلومات وسياسة التعاقد الخارجي.
١٠. توفير الأجهزة التي تدعم حماية الشبكة مثل أنظمة كشف ومنع التطفل والاختراق، والجدران النارية (Firewall) أو أي جهاز أو تطبيق آخر يمكن أن يساعد على التقليل أو منع المخاطر التي تواجه الشبكة سواء كانت من الداخل أو من الخارج، ووفقًا لدرجة السريّة ومتطلبات العمل.
١١. مراقبة التزام الموظفين والمستخدمين بهذه الوثيقة عامة وسياسة الاستعمال المقبول ومدونة السلوك الخاص بأمن المعلومات خاصة في استخدام الشبكة بشكل صحيح وأمن.
١٢. حفظ المعدات الاحتياطية للشبكة في مكان أمن لتكون متوافرة عند الحاجة.

س١٦.٣.٢ واجبات مدير النظام

١. التأكد من توافق المواصفات المتعلقة بالأجهزة والتطبيقات الخاصة بالشبكة في المؤسسة مع هذه الوثيقة، وبشكل يضمن إمكانية التوسع، والتحديث على الأجهزة والتطبيقات.
٢. توفير قوائم بعدد أجهزة الحواسيب والخوادم وكل الأجهزة الالكترونية المرتبطة بالشبكة.
٣. التأكد من فتح المنافذ (Ports) وتوفر خدمات الشبكات الضرورية فقط وإغلاق ما لا يحتاج إليه منها.
٤. ضبط الإعدادات الخاصة بالأجهزة الموجودة على الشبكات لتعمل بطريقة أمنة.

٥. تنصيب وضبط ومتابعة تشغيل الأنظمة الخاصة بحماية شبكة المؤسسة، مثل الجدران النارية (Firewall)، وأنظمة كشف ومنع التطفل والاختراق، وأنظمة مكافحة الفيروسات والبرامج الخبيثة، بالتوافق مع سياسة مكافحة الفيروسات والبرامج الخبيثة.

٦. التحكم بالأجهزة القادرة على الربط والوصول إلى أجهزة المؤسسة المختلفة، عن طريق قوائم التحكم بالوصول (Access List).

٧. 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 تبعًا لسياسة ضبط التغيير وسياسة الاستعمال المقبول.

٨. مراقبة أداء الشبكات وأنظمة ادارتها، ورفع التقارير الخاصة بها للجهة المسؤولة عن الامر داخل المؤسسة اعتمادًا على سجلات الحركات الخاصة بتدفق المعلومات عبر الشبكات.

٩. متابعة ما يستجد من معلومات حول وجود أي ثغرات ضمن أنظمة التشغيل الخاصة بأجهزة الشبكة ، والعمل على معالجتها وفقًا لكل جهاز وتطبيق، اعتمادا على خطة عمل واضحة وبالتنسيق مع مدير أمن المعلومات ، لتحديد الأدوار، وتحديد التوقيت الملائم لتنفيذها بشكل يضمن عدم حدوث انقطاع للخدمة.

١٠. تسهيل عمليات التدقيق على الأنظمة وقواعد البيانات ونظم التشغيل وأجهزة العاملين داخل المؤسسة بالتوافق مع سياسة التدقيق الخاص بأمن المعلومات.

١١. في حال وجود متطلبات خاصة لفئة معينة داخل المؤسسة دون غيرها في استخدام أنظمة حساسة على الشبكة ، فإنه يجب فصل "المجالات" فعليًا عن بعضها كذلك، بحيث يتم إعطاء صلاحيات لكل مجموعة اعتمادا على الخوادم والموارد المسموح لهم بالعمل عليها، وتجهيز قوائم التحكم بالوصول (Access List) للتأكد من أن تلك المجموعات تستطيع التواصل فيما بينها وفقًا لما يتفق عليه، وطبيعة عمل المؤسسة.

١٢. رفع تقارير دورية توضح المشاكل الأمنية الخاصة بأمن وحماية المعلومات التي تمت مواجهتها على الشبكة، من خلل أو اختراق أو انتشار للبرامج الخبيثة إلى مدير أمن المعلومات.

س١٦.٣.٣ واجبات مدير أمن المعلومات

١. إجراء عمليات مراجعة وتدقيق لتقييم مدى توافق النواحي الخاصة بأمن المعلومات على الشبكات مع هذه السياسة ومتابعة الجوانب الأمنية الخاصة بالشبكة في المؤسسة بالتعاون مع مدير النظام.
٢. متابعة التقارير الخاصة بالمشاكل الأمنية التي واجهتها أو تواجهها الشبكة في المؤسسة، والمساعدة في حلها.

س١٦.٣.٤ واجبات العاملين داخل المؤسسة (المستخدمين)

١. عدم تغيير أو فك أو ربط أي جهاز بالشبكة التابعة للمؤسسة .
٢. حفظ المعلومات والملفات على الأجهزة التي يحددها مدير النظام مثل خوادم الملفات (File Server).

السياسة السابعة عشر - سياسة ألتعامل مع الأجهزة الالكترونية منتهية الخدمة

س١٧.١ الهدف

تحديد الضوابط للتعامل مع الأجهزة الالكترونية بعد انتهاء خدمتها والية التعامل معها.

س١٧.٢ المجال

تغطي هذه السياسة جميع الأجهزة الالكترونية المرتبطة بالشبكة التابعة للمؤسسة او الأجهزة التي كانت تعمل بصورة منفصلة والتي تؤثر على أمن المعلومات وتناقل البيانات داخل المؤسسة او خارجها.

س٣.١٧ تفاصيل السياسة

س١.٣.١٧ تقنيات إزالة المعلومات

هناك ثلاث طرق لإزالة المعلومات من الأجهزة و الوسائط التي كانت تخزن المعلومات، من الأقل فعالية إلى الأكثر فاعلية، هي الحذف، او الكتابة فوق البيانات، او التدمير المادي.

١. حذف المعلومات: وهي طريقة غير فعالة تتلخص بإزالة المؤشرات إلى المعلومات المخزنة على الجهاز مع بقاء المعلومات بدون حذف. لا يجوز الاعتماد على طريقة الحذف المستخدمة بشكل روتيني عند العمل على جهاز الحاسوب وهي نقل ملف إلى سلة المحذوفات، أو اختيار "حذف" حتى إذا تمت عملية إفراغ سلة المهملات، فإن المعلومات لا تزال موجودة ويمكن استرجاعها.
٢. الكتابة فوق البيانات: وهي طريق فعالة تتلخص بوضع البيانات العشوائية في مكان المعلومات الاصلية المخزنة على الجهاز ، والتي لا يمكن استرجاعها لأنه قد تم طمسها ، يوصي بالكتابة على المعلومات اكثر من مرة واحدة وذلك لضمان عدم استرجاع المعلومات الاصلية.
٣. التدمير المادي: هو الطريقة المثلى لمنع الآخرين من استرداد المعلومات و خصوصا إذا كان الجهاز يحتوي سابقا على معلومات قد يؤدي افشاءها الى ضرر كبير بأمن المعلومات.

س٢.٣.١٧ واجبات المؤسسة

١. على المؤسسة ان توضح الطرق و الاليات في التعامل مع الأجهزة الالكترونية المنتهية الخدمة اعتمادا على المقاييس العالمية و يجب ان تكون الإجراءات السابقة مثبتة و موثقة ضمن الية تطبيق نظام أمن المعلومات في تلك المؤسسة واعتمادا على هذه الوثيقة.
٢. اتباع الإجراءات الصحيحة في التعامل مع الأجهزة اللوحية و أجهزة الهاتف النقال المراد إخراجها من الخدمة او اعطاءها الى شخص اخر.
٣. مراعاة الاعتبارات التالية في التعامل مع الأجهزة الالكترونية المنتهية الخدمة:

١- هل سيتم اعادة استخدام هذه الأجهزة في أماكن و مجالات عمل أخرى ؟ على سبيل المثال. محركات الأقراص الصلبة وأشرطة النسخ الاحتياطي.

٢- كيفية و الية نقل وتخزين البيانات الموجودة على الأجهزة المراد اخارجها من الخدمة الى الأجهزة الأخرى ؟

٣- ما هي العملية ومن الذي يأذن بالتخلص من جميع أنواع المعلومات؟ على سبيل المثال. الوثائق الورقية والأقراص و وسائط التخزين وغيرها ؟

السياسة الثامنة عشر – سياسة مكافحة الفيروسات و البرامج الخبيثة

س١٨.١ الهدف

حماية موارد ونظام المعلومات من البرامج الضارة و الفيروسات

س١٨.٢ المجال

تغطي هذه السياسة اليات التعامل والمكافحة من البرامج الخبيثة كالفيروسات والديدان وأحصنة طروادة وبرامج التجسس والرسائل المزعجة وغيرها من البرامج التي يمكن أن تهدد أمن وسلامة وتوافرية وخصوصية المعلومات ومواردها وأنظمة المعلومات المعمول بها في المؤسسة.

س١٨.٣ تفاصيل السياسة

س١٨.٣.١ قواعد عامة

١. يجب تنصيب برامج موثوقة ومرخصة لمكافحة الفيروسات والبرامج الخبيثة على جميع أجهزة الحاسوب المملوكة للمؤسسة ، من خوادم (Severs)، وأجهزة محمولة، وأجهزة مكتبية وغيرها، مع متابعة تحديثها بشكل مستمر.
٢. عند اكتشاف فيروسات لا تستطيع برامج مكافحة الفيروسات الكشف عنها والتخلص منها، فإنه يجب على الدعم الفني للمؤسسة الاتصال بالشركة صاحبة المنتج، مع محاولة التقليل والحد من تأثير الفيروس على الأجهزة المصابة .
٣. يجب القيام بعملية مسح SCAN للملفات المنقولة عبر شبكات الحاسوب للمؤسسة باستخدام برامج مكافحة الفيروسات، من أجل التأكد من خلوها من البرامج الخبيثة.
٤. على المؤسسة إجراء تقييم بين فترة وأخرى للتأكد من مطابقة برامج مكافحة الفيروسات واعداداتها للسياسات الواردة في هذه الوثيقة.
٥. على المؤسسة تطبيق الفقرات الخاصة بالتعامل مع البرامج الخبيثة في سياسة البريد الإلكتروني.

س١٨.٣.٢ واجبات مدير النظام

١. الالتزام بعملية ضبط التغيير في المؤسسة إذا ترتب أي إجراء تغير يتعلق ببرنامج مكافحة الفيروسات والبرامج الخبيثة ، ولابد الحصول على الموافقة اللازمة من مدير أمن المعلومات والإدارة العليا في المؤسسة و بالتوافق مع سياسة ضبط التغيير.
٢. تحديث برامج مكافحة الفيروسات والبرامج الخبيثة بشكل دوري وفقًا لآخر تحديث، تبعًا للتراخيص المرفقة مع هذه البرامج.
٣. عند عدم القدرة على تحديث برامج مكافحة للفيروسات – مثل انقطاع الاتصال بالإنترنت مثلا - فلا بد من إيجاد حل بديل على الفور، بالتنسيق مع مدير أمن المعلومات في المؤسسة.

٤. يجب مراقبة وتوثيق عمليات تحديث ملفات تعريف الفيروسات والبرامج الخبيثة.
٥. إغلاق المنافذ (Ports) وحجب الخدمات التي لا حاجة للمؤسسة بها، والتي تستخدمها البرامج الخبيثة عادة للتسلل إلى الأنظمة والوسائط، بالتوافق مع سياسة أمن الشبكات.
٦. إجراء مسح (Scan) كامل للأجهزة والأنظمة ببرامج مكافحة الفيروسات بين فترة وأخرى وبطريقة منتظمة حسبما يقره مدير النظام وبالتنسيق مع مدير أمن المعلومات ، للتأكد من خلو نظام المعلومات من أية تهديدات تتعلق بالبرامج الخبيثة.
٧. عزل الأجهزة المصابة بالبرامج الخبيثة عن الشبكة لحين التأكد –وبشكل موثق- من خلوها من هذه البرامج الخبيثة.
٨. 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.
٩. حجب صلاحيات إيقاف وإزالة برامج مكافحة الفيروسات عن العاملين داخل المؤسسة لضمان استمرارية هذه البرامج وعملها بشكل صحيح وأمن، وعدم إعطاء فرصة للفيروسات والبرامج الخبيثة بالدخول إلى الأنظمة وتخريبها.

س١٨.٣.٣ واجبات مدير أمن المعلومات

١. مراجعة طلبات التغيير المتعلقة ببرامج مكافحة الفيروسات والبرامج الخبيثة، والتي يتم رفعها ضمن عملية ضبط التغير.
٢. مساعدة الدعم الفني للمؤسسة في مكافحة الفيروسات والبرامج الخبيثة عند الحاجة.
٣. متابعة مواقع الإنترنت الرصينة المختصة بالفيروسات والبرامج الخبيثة وآليات عملها بشكل دوري من أجل الحصول على معلومات وافية عن آلية عمل الفيروسات والبرامج الخبيثة الجديدة والتحذير من كيفية انتقالها، وتنزيل الأدوات الحديثة التي تم تطويرها للقضاء عليها بعد التأكد من كفاءتها.
٤. نشر الوعي بين العاملين داخل المؤسسة عن الية انتشار الفيروسات والبرامج الخبيثة وبيان أخطارها والتحذير منها، وبيان الكيفية والوسائط والأنظمة التي يمكنها أن تنتقل عبرها بسهولة.

س١٨.٣.٤ واجبات العاملين داخل المؤسسة (المستخدمين)

١. العمل بالتوافق مع البند الخاص بالإنترنت في سياسة الاستعمال المقبول والذي يشير الى الطريقة الصحيحة في تنزيل وتنصيب البرامج والملفات تحسبًا لوجود برامج خبيثة فيها.
٢. تبليغ مدير النظام عن أي عمل من شأنه نشر الفيروسات أو المساعدة على نشرها.
٣. عند ظهور تحذير يدل على وجود فيروس أو برنامج خبيث فإنه يجب التوقف عن استخدام الجهاز وتبليغ مدير النظام على الفور.
٤. عدم استخدام برامج غير مرخصة.
٥. عدم تشغيل وسائط أو برامج يُشك في انها ملغمة بالفيروسات أو برامج خبيثة.
٦. 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.
٧. عدم استخدام وسائط التخزين إلا بعد التأكد من خلوّها من البرامج الخبيثة.
٨. عدم إرسال أو استقبال أو تنزيل أو نقل أية ملفات يُشك في أن تكون مصابة بالفيروسات أو البرامج الخبيثة عبر الشبكة التابعة للمؤسسة.

السياسة التاسعة عشر – سياسة الوصول عن بُعد

س١٩.١ الهدف

تحديد قواعد وأليات استخدام تقنية الوصول عن بُعد في الدخول لشبكة المؤسسة وذلك لضمان تقليل الأضرار والمخاطر التي قد تنجم عن الاستخدام الخاطئ والغير مصرح به لهذه التقنية.

س١٩.٢ المجال

تغطي هذه السياسة جميع العناصر والمكونات والموارد المستخدمة في الوصول عن بُعد لشبكة المؤسسة بنوعيها السلكية واللاسلكية.

.

س١٩.٣ تفاصيل السياسة

١. منح وحذف صلاحيات الوصول عن بُعد للعاملين داخل المؤسسة حسب مقتضيات العمل وحسب الأدوار والمهام الموكلة اليهم لإنجاز مهامهم.
٢. يجب على العاملين داخل المؤسسة المصرح لهم باستخدام تقنية الوصول عن بُعد حماية بيانات تسجيل الدخول الخاصة بهم وعدم مشاركتها مع أي شخص لأي سبب من الأسباب.
٣. يجب ان تكون قناة الاتصال عن بُعد مشفرة بأعلى درجات التشفير على سبيل المثال لا الحصر استخدام تقنية الـ IPSec VPN أو الـ SSL VPN وذلك حسب متطلبات العمل و حساسية المعلومات والبيانات المتناقلة اعتمادا على سياسة تصنيف المعلومات أضافة الى استخدام اعلى تقنيات الحماية وكلمات سر قوية اعتمادا على سياسة التشفير وسياسة كلمة المرور مع مراعاة التحديثات الواردة توافرها في المستقبل لتقنية الاتصال عن بُعد .
٤. يجب أن تمر جميع الاتصالات الواردة إلى الشبكات الداخلية للمؤسسة عبر نقطة التحكم في الوصول قبل أن يتمكن المستخدم من الوصول إلى واجهة تسجيل الدخول.
٥. يجب تسجيل الدخول عن بُعد في قاعدة بيانات مركزية أضافة الى مراجعة سجلات الوصول بانتظام للكشف عن الحالات الشاذة.
٦. يجب أن تفي المعدات الشخصية المستخدمة في الاتصال بالشبكة الداخلية بكل متطلبات الأمان وذلك بالتنسيق المباشر مع مدير أمن المعلومات و على سبيل المثال التأكد من تحديث جهاز الحاسوب وتنصيب وتحديث برنامج مكافح الفيروسات و البرامج الضارة.

٧. يجب ان تكون المعدات المستخدمة في الوصول عن بعد موثقة في السجلات و في حالة تغير هذه الأجهزة يجب اخذ الموافقة من مدير أمن المعلومات.
٨. يجب على المستخدمين المصرح لهم باستخدام تقنية الوصول عن بُعد توخي الحذر عند الاتصال بالشبكات في الأماكن العامة مثل المطارات والمقاهي ، وما إلى ذلك ، ويجب عدم الاتصال بالشبكة الداخلية للشركة (حتى عبر القنوات المشفرة) إذا كان ذلك على شبكة عامة غير أمنة.
٩. في حالة استخدام تقنية الاتصال عن بُعد لربط أفرع المؤسسة (Site to Site) يجب استخدام قنوات اتصال مشفرة وأمنة إضافة الى اخذ الإجراءات الازمة لتحديد وقت الاتصال وحسب مقتضيات العمل.

السياسة العشرين – سياسة كلمات المرور

س٢٠.١ الهدف

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

س٢٠.٢ المجال

تنطبق هذه السياسة على جميع كلمات المرور داخل المؤسسة بما في ذلك على سبيل المثال لا الحصر ، الحسابات على مستوى المستخدم ، والحسابات على مستوى النظام ، وحسابات الموقع الالكتروني ، وحسابات البريد الإلكتروني ، وحماية شاشة التوقف ، والبريد الصوتي .

س٣.٢٠ تفاصيل السياسة

س١.٣.٢٠ قواعد عامة

١. 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.
٢. عند حدوث إفصاح لكلمات المرور أو دخول إلى الأنظمة بشكل غير مرخص، فإنه يجب إبلاغ مدير النظام ومدير أمن المعلومات للتحقيق في أسباب وآلية الإفصاح إضافة الى اتخاذ الإجراءات المناسبة كتغيير كلمة المرور واكتشاف أي تغيرات جرت على النظام وبالسرعة الممكنة.
٣. يجب على المؤسسة وضع تعليمات لحفظ نسخة عن كلمات المرور في مغّلف خاص مغلق توضع وتخزن عند الإدارة العليا في المؤسسة لاستعمالها وقت الضرورة.
٤. يجب أخذ الأمور التالية بعين الاعتبار عند اختيار كلمة المرور:

- ألا تكون قد استخدمت مسبقًا من فترة قريبة.
- ألا تكون سهلة التخمين، مثل اسم الشخص، أو تاريخ ولادته، أو رقم هاتفه، أو اسم حساب الدخول الإلكتروني للمستخدم.
- ألا تكون من الكلمات المتداولة في القواميس أو اللغات المعروفة.
- ألا تكون مبنية بحيث تشكل في مجملها جملة واحدة كاملة من حروف وأرقام متتابعة ومتسلسلة بشكل منطقي ومعروف للعامة.
- أن تكون مركبة من الحروف والأرقام والرموز الخاصة، وبدون تكرار.
- أن تكون طويلة بشكل كافٍ.
- ألا تحتوي اختصارات معروفة مثل gov او com.
- أن يتم تغييرها بشكل دوري وحسب ما تحدده تعليمات المؤسسة.
- عدم استخدامها في أكثر من حساب ونظام دخول.

٥. يجب زيادة الالتزام بالتوجيهات السابقة لكلمات المرور كلما ازدادت حساسية المعلومات المتبادلة بين العاملين داخل المؤسسة .
٦. تعامل كلمات المرور على انها معلومات مصنفة "سري للغاية".

س٢٠.٣.٢٠ واجبات مدير النظام

١. حماية مكونات نظم المعلومات من الدخول غير المشروع أو غير المخول به عن طريق إعداد النظام لاستخدام وقبول كلمات المرور التي تحقق الشروط التي تم ذكرها أعلاه في هذه السياسة، ورفض كلمات المرور الضعيفة.
٢. التأكد من تشفير الملفات التي تحتوي على كلمات المرور.
٣. إعداد النظام لإيقاف حساب الدخول الإلكتروني مؤقتا عند استخدام كلمة مرور خاطئة بشكل متتال لِعدد معين من المرات.
٤. إعطاء كلمات مرور جديدة في حالة :
   - فتح حساب دخول إلكتروني لمستخدم جديد على أن يقوم المستخدم بتغير كلمة المرور فور دخوله للمرة الأولى.
   - نسيان أو فقدان كلمة المرور التي يستخدمها المستخدم حاليًا، بعد التحقق من هوية المستخدم صاحب الحساب الإلكتروني.
٥. حماية كلمات المرور المميزة التي قد يؤدي الإفصاح عنها بشكل غير مرخص إلى ضرر بليغ جدا بالمؤسسة ونظم المعلومات المستخدمة فيها، مثل حساب مدير النظام.

س٢٠.٣.٢٠ واجبات العاملين داخل المؤسسة (المستخدمين)

١. المستخدم مسؤول عن أي عمليات أو مراسلات تحدث عن طريق الحساب الإلكتروني الخاص به سواءً عن طريقه أو عن طريق أي شخص استخدم حساب الدخول الالكتروني وكلمة المرور لهذا المستخدم.
٢. حماية كلمة المرور من الإفصاح عنها بشكل غير مرخص والضياع.
٣. تغيير كلمة المرور على الفور عند الإفصاح عنها بشكل غير مرخص، سواءً بشكل متعمد أو غير متعمد.
٤. تطبيق التوجيهات الخاصة بكتابة كلمات المرور والمذكورة أعلاه في هذه السياسة.
٥. عدم كتابة كلمات المرور أمام أي شخص يشاهد عملية الإدخال على لوحة المفاتيح.
٦. عدم استعمال كلمات المرور الخاصة بالمؤسسة في مواقع الإنترنت او أي مواقع أخرى تعود للاستعمال الشخصي للمستخدم.

السياسة الحادية والعشرين – سياسة الشبكات اللاسلكية

س٢١.١ الهدف

تهدف هذه السياسة الى توفير المتطلبات والضوابط الواجب توافرها لحماية شبكات الاتصالات اللاسلكية.

س٢١.٢ المجال

تغطي هذه السياسة شبكات الاتصالات اللاسلكية و شبكات الاتصالات عبر الاقمار الصناعية (Vsat) إضافة الى الشبكات التابعة لجهات اخرى والتي ترتبط مع الشبكة الخاصة للمؤسسة لأغراض العمل الرسمي بما يتضمنه ذلك من خوادم وموجهات وجدران نارية وأسلاك وبروتوكولات وغيرها من مكونات الشبكة.

س٢١.٣ تفاصيل السياسة

١. يوصي بعزل شبكة المؤسسة عن الانترنت في حال ربطها مع الشبكة المؤمنة واذا دعت الحاجة الى ربط شبكة المؤسسة مع الانترنت يجب تامين الشبكة بالأجهزة والبرمجيات اللازمة للحفاظ على الشبكة من التهديدات و الخروقات الناتجة عن الاتصال بالأنترنت.
٢. استخدام اجهزة التشفير بين نقاط الاتصال التابعة للشبكة.
٣. استخدام احدث البروتوكولات الخاصة بالتشفير وحسب حساسية واهمية الشبكة و في حال اصدار بروتوكولات احدث وذات امنية اعلى يجب ان يتم استخدامها.
٤. ضمان عدم تداخل الترددات المستخدمة في الشبكات من خلال استخدام الترددات المرخصة.
٥. تامين البيئة المادية الخاصة بالأبراج التي تستخدم في نقاط توصيل الشبكة من العبث و التخريب.
٦. استخدام احدث بروتوكولات المصادقة وحسب حساسية واهمية الشبكة و في حال اصدار بروتوكولات احدث وذات امنية اعلى يجب ان يتم استخدامها.
٧. استخدام كلمة مرور معقدة وصعبة التخمين .

السياسة الثانية والعشرين – سياسة أمن الخوادم (Servers)

س٢٢.١ الهدف

تهدف هذه السياسة الى فرض الإجراءات و الضوابط لحماية الخوادم والتقليل من خطر الوصول الغير مصرح به لهذه الأجهزة إضافة الى اليات التعامل معها.

س٢٢.٢ المجال

تغطي هذه السياسة جميع الخوادم التي تقدم خدمات معينة الى المؤسسة.

س٢٢.٣ تفاصيل السياسة

س٢٢.٣.١ المتطلبات العامة

١. يجب ان يقوم مدير النظام بتحديد الافراد المسؤولين عن إدارة الخوادم واعطائهم الصلاحيات الكافية لإدارتها بناءً على احتياجات العمل .
٢. يجب تسجيل الخوادم ضمن سجلات جرد الاصول.
٣. يجب ان تكون المعلومات التالية متوفرة و موثقة لكل خادم:
   - نظام التشغيل / الإصدار
   - الوظائف والتطبيقات الرئيسية
   - الجهات التي يقوم هذا الخادم بتقديم الخدمات لها

س٢٢.٣.٢ متطلبات الاعداد

١. يجب أن يكون نظام التشغيل على هذه الخوادم معتمد و مرخص.
٢. يجب تفعيل الخدمات والتطبيقات الضرورية لأداء مهام المؤسسة وتعطيل أي خدمات و تطبيقات أخرى غير ضرورية .
٣. يجب تثبيت تحديثات الأمان على نظام التشغيل وباقي مكونات السيرفر بصورة دورية بعد اجراء عملية الاختبار على بيئة تجريبية لتجنب المشاكل التي قد تحدث اثناء وبعد عملية التحديث .

٤. في حالة الوصول عن بُعد لهذه الخوادم يجب ان تكون هذه القنوات مشفرة وحسب سياسة الوصول عن بُعد.
٥. يجب أن تكون الخوادم موجودة في بيئة يمكن الوصول إليها فقط من العاملين داخل المؤسسة المصرح لهم بذلك وحسب سياسة حماية البيئة المادية.
٦. يجب اخذ النسخ الاحتياطية لهذه الخوادم بشكل دوري وحسب سياسة النسخ الاحتياطي.
٧. المراقبة الدائمة لسجلات الخوادم (Logs) لاستكشاف الأخطاء ان وجدت.

السياسة الثالثة والعشرين – سياسة البريد الالكتروني

س٢٣.١ الهدف

تهدف هذه السياسة الى وضع الضوابط والتعليمات لضمان الاستخدام الصحيح للبريد الالكتروني إضافة الى حمايته.

س٢٣.٢ المجال

تغطي هذه السياسة جميع انظمة البريد الإلكتروني المعمول بها في المؤسسة، والمتعاملين مع هذه الأنظمة ويملكون حسابات بريد إلكتروني.

س٢٣.٣ تفاصيل السياسة

س٢٣.٣.١ قواعد عامة

١. كافة المعلومات التي يتم تبادلها عبر البريد الالكتروني هي ملك للمؤسسة ، لذا فإن للمؤسسة الحق في تدقيق ومراقبة البريد الالكتروني ومحتوى المراسلات كلما دعت الحاجة وذلك من أجل حماية مصالح المؤسسة.

٢. يتم اجراء التدقيق والمراقبة لنظام البريد الالكتروني بعد اخذ الموافقة من الإدارة العليا و بالتنسيق مع مدير أمن المعلومات.

س٢٣.٣.٢ واجبات مدير النظام

١. حماية نظام البريد الإلكتروني باستخدام التقنيات الحديثة وبرامج مكافحة البرامج الضارة وغيرها من التقنيات بشكل يضمن أمن الرسائل المتبادلة .
٢. اتاحة نظام تشفير البريد الالكتروني للعاملين داخل المؤسسة.
٣. تصميم وتطبيق خطة عمل مناسبة لإدارة نظام البريد الإلكتروني في المؤسسة بشكل أمن.
٤. إنشاء وإلغاء حسابات البريد الإلكتروني وتحديد الصلاحيات الخاصة باستخدام نظام البريد الإلكتروني لهذه الحسابات اعتمادًا على الوصف الوظيفي.
٥. القيام بعملية النسخ الاحتياطي للملفات والرسائل التي تمت أرشفتها من أجل ضمان وجودها عند حدوث طارئ، بما يتلاءم وسياسة النسخ الاحتياطي.
٦. توعية المستخدمين بخدمات البريد الإلكتروني التابعة للمؤسسة والاستخدام الصحيح والأمن لها.
٧. وضع صيغة التنازل (Disclaimer) الخاصة بالمؤسسة في نهاية كل رسالة يتم إرسالها من قبل العاملين داخل المؤسسة.

س٢٣.٣.٣ واجبات العاملين داخل المؤسسة

١. العمل بالبند الخاص بالبريد الإلكتروني في سياسة الاستعمال المقبول.
٢. عدم السماح للآخرين بالدخول إلى حساب البريد الإلكتروني الخاص بالمستخدم أو استخدامه الا في الحالات الضرورية و التي تتطلب موافقة الإدارة العليا.

٣. التعامل مع الرسائل والملفات المنقولة حسب درجة تصنيفها (سريتها)، بما يتوافق مع سياسة حساسية وتصنيف المعلومات.
٤. عدم إرسال معلومات مصنفة على انها "سرية" أو "سرية للغاية" بدون تشفير.
٥. عدم إرسال أو استقبال أو إعادة إرسال أي بريد إلكتروني فيه محتوىً قد يشكل خطرًا على الأنظمة وموارد نظام المعلومات مثل المحتويات الدعائية والبرامج الخبيثة.
٦. عدم الرد على أي رسالة غريبة أو مشبوهة أو مجهولة المصدر إضافة الى تبليغ مدير النظام بوصول رسائل من هذا النوع.
٧. التأكد من مصدر الرسالة و التدقيق في عنوان البريد الالكتروني قبل الإجابة على الرسالة او فتحها او الضغط على أي رابط مشبوه داخل الرسالة.

الفصل الثامن : التشفير

السياسة الرابعة والعشرين – سياسة التشفير

س٢٤.١ الهدف

حماية المعلومات عن طريق وضع القواعد اللازمة لتطبيق خوارزميات التشفير التي تمت مراجعتها وأثبات فاعليتها وجدارتها عالميا.

س٢٤.٢ المجال

تغطي هذه السياسة إدارة واستخدام برامج ومعدات ومفاتيح التشفير للمعلومات المراد تشفيرها في المؤسسة .

س٢٤.٣ تفاصيل السياسة

س٢٤.٣.١ واجبات المؤسسة

١. استخدام خوارزمية تشفير معتمدة عالميا (او خوارزمية تشفير محلية معتمدة) بعد الموافقة عليها من قبل الإدارة العليا وبالتنسيق مع مدير أمن المعلومات بشكل يضمن أمن المعلومات.
٢. توظيف وتنصيب البرمجيات والبروتوكولات والمعدات المناسبة لتطبيق خوارزميات التشفير المعتمدة في المؤسسة.
٣. تشفير جميع وسائط التخزين والاتصالات التي تحتوي معلومات سرية وبالتوافق مع سياسة حساسية وتصنيف المعلومات.
٤. وضع التعليمات المناسبة التي تضمن إجراء عملية التشفير وفك التشفير بطريقة أمنة وصحيحة.
٥. تحديد وتوثيق أسماء العاملين داخل المؤسسة المخولين بالتعامل مع برامج التشفير إضافة الى أسماء الافراد الذين يجب أن تصرف لهم مفاتيح التشفير وذلك حسب متطلبات العمل.

٦. وضع التعليمات التي تحدد كيفية التعامل مع الوثائق والملفات التي تم فقدان أو الإفصاح عن مفاتيح التشفير الخاصة بها أو تم فك تشفيرها بشكل غير مرخص.
٧. وضع التعليمات الخاصة بإدارة مفاتيح التشفير، على أن تراعى فيها الأمور التالية:

- حفظ نسخ احتياطية عن مفاتيح التشفير الخاصة بالمؤسسة في مكان أمن لاستعمالها عند الحاجة.
- مواصفات الأنظمة والبرمجيات المستخدمة في إدارة مفاتيح التشفير.
- اعتماد أو إلغاء اعتماد مفاتيح التشفير -عند الإفصاح عنها بشكل غير مرخص أو استقالة المستخدم مثلا.
- الحدود الدنيا لأطوال مفاتيح التشفير.
- مدة صلاحية المفاتيح.

س٢٤.٣.٢ واجبات مدير أمن المعلومات

١. التأكد من أن التشفير يتم بطريقة صحيحة وأمنة اعتمادًا على صلاحيات المستخدمين.
٢. التدقيق على الالتزام بعملية التشفير تبعًا لهذه السياسة ورفع التقارير للإدارة العليا في المؤسسة عن أية تجاوزات أو مشاكل تتعلق بالتشفير.

س٢٤.٣.٣ واجبات مدير النظام

١. تدريب العاملين داخل المؤسسة على كيفية استعمال برامج ومفاتيح التشفير المعتمدة في المؤسسة.
٢. تنصيب وضبط وتشغيل وتحديث برامج التشفير المعتمدة في المؤسسة والتأكد من انها تعمل بشكل أمن وصحيح.
٣. التعاون مع مدير أمن المعلومات في إدارة مفاتيح وبرامج التشفير داخل المؤسسة.

س٤.٣.٢٤ واجبات العاملين داخل المؤسسة

١. عدم استخدام برامج تشفير أو فك تشفير أو مفاتيح تشفير لم تصرف له من المؤسسة.
٢. تشفير المعلومات المصنفة على انها "سرية" أو "سرية للغاية" أثناء نقلها وتخزينها بالتوافق مع هذه السياسة وسياسة حساسية وتصنيف المعلومات.
٣. المحافظة على سلامة وسرية مفاتيح التشفير المصروفة له من المؤسسة.
٤. مراجعة الدعم الفني عند وجود أية مشاكل تتعلق باستخدام برامج أو مفاتيح التشفير المصروفة له من المؤسسة.
٥. تبليغ مدير النظام عند الشك في سوء استعمال مفاتيح التشفير أو برامج التشفير.

الفصل التاسع : إدارة الحوادث

السياسة الخامسة والعشرين – سياسة إدارة الحوادث

س٢٥.١ الهدف

وضع الضوابط والاليات الصحيحة للتعامل مع الحوادث المتعلقة بأمن المعلومات.

س٢٥.٢ المجال

توضح هذه السياسة الممارسات الفضلى في التعامل مع حوادث أمن المعلومات لجميع العاملين داخل المؤسسة إضافة الى الحوادث الأمنية المتعلقة بموارد نظام المعلومات داخل المؤسسة.

س٢٥.٣ تفاصيل السياسة

س٢٥.٣.١ واجبات المؤسسة

١. يجب وضع إجراءات لإدارة حوادث أمن المعلومات داخل المؤسسة لضمان الاستجابة المناسبة في حالة حصول خروقات أو فشل في النظام.
٢. يجب على المؤسسة متابعة وتنفيذ ضوابط إدارة حوادث أمن المعلومات المقرة و المعتمدة داخل المؤسسة.
٣. إنشاء سجل للحوادث المتعلقة بأمن المعلومات وتسجيلها ومتابعة الحوادث المتكررة وإيجاد الحلول لتجنب حدوثها مجددا.

٤. في حالة حدوث انتهاك أو خرق متعمد لسياسة أمن المعلومات داخل المؤسسة ، يجب التحقيق في ذلك واتخاذ الإجراءات المناسبة لتجنب حدوث مثل هذه الاختراقات مجددا.
٥. يجب إبلاغ جميع العاملين داخل المؤسسة بالمسؤوليات والإجراءات المتعلقة بالإبلاغ في الوقت المناسب عن الأحداث والحوادث الأمنية بما في ذلك الخروقات والتهديدات والضعف الأمني.
٦. وضع الإجراءات والقواعد لضمان الاحتفاظ بالأدلة المتعلقة بحوادث أمن المعلومات في شكل مناسب للتحقيق والمقاضاة.
٧. يجب على المؤسسة أيضًا مراعاة ما يلي:
   - ما هي العملية والسياسة الخاصة بالإبلاغ عن الحوادث الأمنية للمؤسسة؟
   - ما نوع الحوادث الأمنية التي يجب الإبلاغ عنها؟
   - كيف يتم جمع المعلومات؟
   - ما هي المعلومات التي يجب الإبلاغ عنها؟
   - من المسؤول عن متابعة تقارير الحوادث الأمنية؟
   - من المسؤول عن متابعة الأعطال وحلها؟
   - ما هي الإجراءات التي يتعين تنفيذها لكل نوع من الحوادث؟

س٢.٣.٢٥ التخطيط لإدارة حوادث أمن المعلومات

١- يجب أن تتضمن خطة إدارة الحوادث الأمنية للمؤسسة أولويات عامة للعمل أثناء وقوع الحادث. قد تتغير الأولويات تبعًا لطبيعة الحادث. ويفضل اتباع التوصيات التالية:

- حماية حياة الإنسان وسلامة العاملين داخل المؤسسة.
- حماية المعلومات الحساسة.
- حماية المعلومات الأخرى.
- اتباع الإجراءات القانونية.
- منع الأضرار قدر الإمكان.
- تقليل تعطل الخدمات.

٢- يجب على المؤسسة تحديد الأدوار والمسؤوليات لضمان إدارة الحوادث بشكل مناسب. لذا يوصى بإعداد قوائم جهات الاتصال التالية:

- العاملين داخل المؤسسة المسؤولون عن كل موقع.
- مدير أمن المعلومات.
- مدير النظام.
- الإدارة العليا للمؤسسة.
- فريق الاستجابة للأحداث السيبرانية.

الفصل العاشر : استمرارية العمل

السياسة السادسة والعشرين – سياسة استمرارية العمل

س٢٦.١ الهدف

وضع الضوابط لضمان استمرارية العمل وعدم انقطاع أو فشل أنظمة المعلومات والاتصالات ، وضمان استئنافها في الوقت المناسب.

س٢٦.٢ المجال

كل أنظمة المعلومات والاتصالات والخدمات المقدمة من قبل المؤسسة أضافة الى الخدمات والاعمال المقدمة من خلال التعاقدات الخارجية .

س٢٦.٣ تفاصيل السياسة

١. يجب على المؤسسة وضع وتنفيذ ومتابعة خطط استمرارية العمل التي تفي بالمتطلبات الواجب توافرها لضمان استمرار العمل.
٢. يجب استخدام افضل الاليات والتقنيات من اجل تقليل المخاطر على نظام المعلومات والاتصالات والخدمات المقدمة اعتمادا على أهمية تلك الأنظمة والخدمات.
٣. يجب متابعة وتطوير واختبار خطط استمرارية العمل لضمان كفاءتها وتوافرها في الوقت المناسب.
٤. توفير مواقع بديلة تقوم بتقديم الخدمات في حالة الحوادث اعتمادا على أهمية المعلومات والخدمات المقدمة.
٥. يجب على المؤسسة أيضًا مراعاة ما يلي:
   - هل هناك دراسة ووعي لتأثير الانقطاعات على المؤسسة ؟
   - هل تم تحديد جميع الأحداث المحتملة ؟
   - هل جميع خطط استمرارية العمل داخل المؤسسة تؤدي الغرض المطلوب من وجودها؟

الفصل الحادي عشر : أنظمة المعلومات

السياسة السابعة والعشرين – سياسة تطوير وصيانة نظام المعلومات

س٢٧.١ الهدف

ضمان تحقيق المتطلبات اللازمة لتطوير وصيانة نظام المعلومات والخدمات المقدمة من قبل المؤسسة او الخدمات المقدمة من خلال التعاقدات الخارجية.

س٢٧.٢ المجال

تغطي هذه السياسة جميع التطبيقات وأنظمة المعلومات والبرمجيات ، سواء في داخل المؤسسة أو عن طريق التعاقد الخارجي، إضافة الى الاعتبارات الواجب اتخاذها من أجل أمن وحماية هذه الأنظمة وسائر المعلومات المتعلقة بها أثناء دورة حياتها.

س٢٧.٣ تفاصيل السياسة

س٢٧.٣.١ قواعد عامة

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

٢. يجب التأكد من أن ضوابط الدخول الخاصة بالوصول إلى الملفات المتعلقة بالمشاريع كافية وأمنة من أجل المحافظة على سلامة المعلومات والأنظمة.
٣. 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 المؤسسة، بالتوافق مع سياسة ضبط التغيير.
٤. أي عملية تطوير للأنظمة يجب أن تكون موجهة بأهداف العمل ومدعّمة بدراسة جدوى.
٥. يجب اختبار أي تغييرات خاصة بأنظمة المعلومات أو البرمجيات المستخدمة في المؤسسة بطريقة صحيحة وأمنة من قبل المختصين في المؤسسة قبل إقرارها ثم إطلاقها.
٦. لا يسمح باستخدام البيانات الحقيقية قيد الاستخدام Live Data عند اختبار الأنظمة.
٧. يجب العمل بأنظمة المعلومات والبرمجيات المستخدمة في المؤسسة بالتوازي مع الأنظمة والبرمجيات المطورة لحين التأكد من مطابقة الأخيرة لمتطلبات العمل ومتطلبات الأمن والحماية التي تم التطوير من أجلها.

س٢.٣.٢٧ واجبات المؤسسة

١. وضع الضوابط والتعليمات الخاصة بمراحل دورة حياة تطوير أنظمة المعلومات والبرمجيات المستخدمة في المؤسسة بالتوافق مع هذه الوثيقة عامة وسياسة التغيير وسياسة التعاقد الخارجي بشكل خاص.
٢. تحديد متطلبات الأمن والحماية المراد تحقيقها في أنظمة المعلومات والبرمجيات التي يراد استخدامها في المؤسسة.
٣. تقييم المخاطر الناجمة عن تطوير أو صيانة أنظمة المعلومات والبرمجيات ودرجة تأثيرها على مستوى أمن وحماية المعلومات التي تعالجها أو تتعامل معها.
٤. التأكد من عدم وجود أي برمجيات خبيثة في أنظمة المعلومات والبرمجيات التي يتم تطويرها، من أجل المحافظة على سلامة وتوافر المعلومات التي تتم معالجتها عن طريق هذه الأنظمة والبرمجيات.

٥. التأكد من تطبيق مبدأ "الفصل بين المهام" في جميع المجالات المتعلقة بتطوير الأنظمة وادارتها والعمليات المتعلقة بها.
٦. توفير التدريب والتوعية المناسبين للطاقم الفني والمستخدمين لتخطي المخاطر الناتجة عن استخدام الأنظمة والبرمجيات المطورة.
٧. التأكد من توفر متطلبات أمن وحماية المعلومات الخاصة بتطوير وصيانة الأنظمة والبرمجيات.
٨. الموافقة على الانتقال من مرحلة إلى أخرى بعد التأكد من اكتمال المتطلبات والمواصفات الخاصة بأمن المعلومات فيها، واختبارها بشكل مناسب.
٩. التأكد من توثيق جميع الوثائق والدراسات وخطط اختبار الأنظمة والبرمجيات بطريقة أمنة وصحيحة.