

أمن وشفافية المعلومات في  
البيئة الرقمية  
اعتبارات وأبعاد وتوجهات أمن  
المعلومات  
Information Security and  
Transparency in the Digital  
Environment  
Considerations, Dimensioned  
and Information Security

إعداد

د. منير عبد الباري عبدالفتاح

Dr. Muneer Abdulbari Abdulfattah

Email: DrMuneer2020@gmail.com

Mobile: 967780780117



الجامعة الإسلامية بمنيوتا  
Islamic University of Minnesota  
المركز الرئيسي IUM



## ملخص البحث:

هدف البحث الى استعراض أمن وشفافية المعلومات في البيئة الرقمية: اعتبارات وأبعاد وتوجهات أمن المعلومات. وتوجهات أمن وشفافية المعلومات في ظل ، التوسع الكبير في استخدام تطبيقات وخدمات نظم المعلومات الإلكترونية المحملة علي كافة أنواع شبكات المعلومات (الشبكات المحلية، شبكات الإنترنت، شبكات الأكسترانت، شبكة المجال العريض وشبكة الإنترنت) التي تعتمد بعضها علي بعض، وقابليتها للتعرض للإضرار المختلفة وحاجتها لبناء الثقة فيها، وقد أدى كل ذلك إلي تعظيم موضوع أمن المعلومات ونظمها في البيئات الرقمية. وحدد مفهوم أمن المعلومات وطبقاته المختلفة، وإطاره، ومكوناته ومحاوره مع ربطه بالتهديدات التي يتعرض لها أمن نظم المعلومات والأضرار التي قد تنجم من قصور إجراءات الأمن، مع تعزيز أمن نظم المعلومات القائمة. وقد تلخصت مشكلة البحث في ضعف توفر أمن وشفافية هذه المعلومات والحفاظ عليها، وللبحث أهمية تعزيز شفافية أمن المعلومات في المؤسسات بهدف تعزيز الثقة في توفير بيئة رقمية آمنة تتوافق مع التحول الرقمي بموجب الاعتبارات والابعاد لتوجه أمن المعلومات. واستخدم المنهج الوصفي التحليلي لتحقيق تلك الأهداف، وقد تم تقسيم البحث الى خمسة فصول اختتمت بأهمية توضيح عمليات التحقق من أمن المعلومات من حيث التعريف، الاعتماد، الإدارة والمراجعة لها، وأساليب استخدام نظم الأمن، وتطوير السياسة الموجهة وإجراءات المحاسبة والتنفيذ المحتاج إليها.

## كلمات مفتاحية:

أمن المعلومات، أمن شبكات الحاسوب، أخلاقيات الحاسوب، الجريمة الالكترونية.

## Abstract

Discussing information security and transparency in the digital environment: considerations, dimensions and trends of information security. The research reviewed the trends of information security and transparency in light of the significant expansion in the use of electronic information systems applications and services loaded on all types of information networks (local networks, intranets, extranet networks, broadband network and the Internet) that depend on each other, and their vulnerability to various harms and their need to build confidence in them, and all of this has led to maximizing the issue of information security and its systems in digital environments. It defined the concept of information security and its different layers, framework, components and axes, linking it to threats to the security of information systems and the damage that may result from deficits of security procedures, while enhancing the security of existing information systems. The research problem was summarized in the weak availability of security and transparency of this information and its preservation, and the research on the importance of enhancing the transparency of information security in institutions in order to enhance confidence in providing a safe digital environment that is compatible with digital transformation under the considerations and dimensions of the information security orientation. The descriptive and analytical approach was used to achieve these goals. The research was divided into five chapters, which concluded with the importance of clarifying



the processes of information security verifications in terms of definition, accreditation, management and review, methods of using security systems, and the development of directed policy and accounting procedures and implementation needed.

**Keywords:**

Information Security, Computer Network Security, Computer Ethics, Cybercrime



## المقدمة

يشكل كل من الحاسب الآلي والبرمجيات والبيانات العناصر الأساسية لنظام المعلومات في البيئة الرقمية. وقد يرتبط الحاسب الآلي بواسطة أجهزة وخدمات الاتصال في شبكة بنهايات طرفية أو حسابات أخرى أو تسهيلات اتصال معينة. وقد تكون شبكة الحاسبات شبكة محلية LAN أو شبكة خاصة ممتدة علي نطاق المصلحة الحكومية أو الوزارة المعنية كشبكة الإنترنت، أو شبكة المجال العريض WAN كشبكة الإكسترنت أو شبكة معلومات دولية كالإنترنت، كما قد تكون وصلة اتصال خارجية مفتوحة لأي فرد مزود بالوسائل التكنولوجية التي تمكنه في الوصول إليها. وتشتمل كثير من شبكات المعلومات علي تجميع من الوصلات الداخلية والخارجية، كما تتضمن شبكات الاتصال علي بيانات اتصال، بالإضافة لتليفون وفاكس موديم. ومن الأجهزة الأخرى قد ترتبط الطابعات بأجهزة الحاسبات والاتصالات. وقد تتضمن برمجيات الحاسبات نظم تشغيل وبرمجيات التطبيقات التي تصمم خصيصاً لعميل معين كمصداة أو جهاز حكومي معين. وقد تركيب البرمجيات في الحاسب الآلي أو تخزين علي أقراص مدمجة CD-ROMs، أو أي وسائل تخزين أخرى متاحة. وتساند الأدلة الورقية والتوثيقية أو المحمولة والمقروءة إلكترونياً تشغيل الأجهزة والبرمجيات واستخدامها وصيانتها.

### مشكلة البحث :

عندما تنشأ بيئة رقمية فان الهيكل نظم وتطبيقات المعلومات في البيئة الرقمية يعمل على تخزين البيانات والمعلومات ومعالجتها واسترجاعها وإرسالها أو نقلها للمستخدم المستهدف. وتجمع كل هذه العناصر المختلفة والعديدة معا لتشكل نظام المعلومات في البيئة الرقمية مما يمثل ديناميكية تكنولوجيا المعلومات والاتصالات المتقدمة في دعم ومساندة البيئة الرقمية وما يرتبط بها من

تطورات وتظهر مشكلة أمن وشفافية هذه المعلومات وفي هذا البحث سيتم دراسة أمن وشفافية المعلومات في بيئة تكنولوجيا المعلومات .

### أهمية البحث :

إن للبيانات والمعلومات المتوافرة في نظم وتطبيقات المعلومات الإلكترونية مزايا إضافية تجعلها مختلفة ومتميزة عن النظم الورقية أو الوثائقية التقليدية، ويحتم ذلك أهمية ضرورة توافر بيئة آمنة شفافة ومتطورة .

### أهداف البحث :

يهدف البحث إلى :

- زيادة استخدام وفعالية قيمة الحاسبات الآلية، وتسهيلات الاتصال، وشبكات الحاسبات والاتصالات، والبيانات والمعلومات التي تخزن وتعالج وتسترجع وترسل بواسطتها متضمنة البرامج والمواصفات والإجراءات في بيئة آمنة ومتطورة.
- نتيجة لزيادة دور نظم وتطبيقات المعلومات المتزايد الأهمية والاعتماد المتنامي عليها في الاقتصاد والتجارة والإدارة والتعلم، أي في كافة أوجه الحياة الاجتماعية والثقافية والسياسية، فقد أدى ذلك إلي بذل جهود خاصة لضمان الثقة والمصداقية لهذه النظم والتطبيقات من حيث أمنها وشفافيتها للمستخدمين.

### فرضيات البحث :

ستقوم هذه الدراسة بوضع حلول على التساؤلات التالية:

- ماهي الطرق الملائمة لزيادة الوعي بالمخاطر المحيطة بنظم وتطبيقات المعلومات.
- ماهي المعايير والأساليب المقننة لحماية أمن وشفافية المعلومات وتطبيقاتها في البيئة الرقمية.

■ ماهي المقاييس والإجراءات التي تعكس المبادئ التي تخص أمن المعلومات الإلكترونية.

## منهجية البحث :

اعتمدت هذه الدراسة على المنهج الوصفي التحليلي القائم على تحليل المعطيات الواقعية ودراسة الظاهرة كما توجد في الواقع .

## تقسيم الدراسة :

### المقدمة

### المدخل

### الفصل الأول

استخدامات تطبيقات وخدمات نظم المعلومات في البيئة الرقمية

- استعراض التطورات في تكنولوجيا المعلومات
- عوامل نظم وتطبيقات شبكة المعلومات الحديثة

### الفصل الثاني

أمن المعلومات ونظمها في البيئة الرقمية

- أمن نظم المعلومات
- مقاييس الأمن الطبيعية
- الأضرار الناجمة من قصور أمن المعلومات
- تعزيز أمن المعلومات

### الفصل الثالث

متطلبات الأمن الطبيعي لنظم المعلومات

- الأمن الطبيعي
- أبعاد نظم أمن المعلومات
- تطوير سياسة أمن المعلومات
- محاسبة إدارة أمن المعلومات
- تنفيذ أدوات ومنتجات الأمن الملائمة



## الفصل الرابع

اعتبارات وأبعاد أمن المعلومات

- الأبعاد الرئيسية لأمن المعلومات
- مكونات أمن المعلومات

## الفصل الخامس

توجيهات أمن وشفافية المعلومات

- الغرض العام من توجيهات ومعايير أمن المعلومات
- مجال التوجيهات والمعايير
- أهداف أمن المعلومات
- المبادئ العامة للتوجيهات ومعايير أمن المعلومات
- تنفيذ أمن المعلومات
- التعليم والتدريب على أمن المعلومات

## الخلاصة

## المصادر والمراجع



## المدخل:

إن تعزيز الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات سوف يعزز إطار الطمأنينة الذي يشمل أمن المعلومات وأمن الشبكات وصون الخصوصية والسرية وحماية المواطن المستخدم مما يعتبر شرطا مسبقا لإنشاء مشروعات تكنولوجيا لتنمية مجتمع المعلومات لبناء الثقة بين مستخدمي تكنولوجيا المعلومات والاتصالات.

ويتضمن هذا البحث عدة محاور ترتبط بالتوسع في استخدامات نظم وتطبيقات وخدمات المعلومات الرقمية التي تتاح علي شبكات المعلومات التي صارت تتسم بالاعتمادية، وقابليتها للتعرض للضرر والخطر، وحاجتها لاكتساب الثقة في التعامل معها من قبل المواطنين، وأمن نظم المعلومات وتطبيقاتها وخدماتها في بيئة المصالح والمنظمات الحكومية الرقمية التي يجب أن تمثل حماية سريتها وسلامتها وتوافرها فيما يتصل بالتهديدات المطلوب مواجهتها والاعتبارات العامة التي تشكل معالم شفافيتها من العمليات والبشر والتكنولوجيا والثقافة المؤسسية المتاحة، ومتطلبات الأمن الطبيعي والمنطقي والفني والسيكولوجي للمعلومات التي تحدد عمليات التحقق من الأمن المستهدفة، وتفهم استخدام أمن نظم المعلومات، ومحاسبة إدارة الأمن وتنفيذ أدوات ومنتجات الأمن، واعتبارات وأبعاد أمن المعلومات؛ وتوجيهات ومعايير أمن نظم المعلومات من حيث غرضها العام ومجالها وتعريفها وأهدافها والمبادئ الخاصة بأمن المعلومات، وتنفيذ نظم أمن وشفافية المعلومات المرتبط بتطوير السياسة الخاصة بنظام الأمن والتعليم والتدريب المصاحب لتطوير النظام وتبادل المعلومات والتعاون في المعلومات الأمنية لنظم المعلومات وتطبيقاتها وخدماتها، ويختتم هذا العمل بالخلاصة التي تتضمن النتائج والتوصيات المتوصل إليها.

## الفصل الأول :

### استخدامات تطبيقات وخدمات نظم المعلومات في البيئة الرقمية

تقبل المجتمع المعاصر أهمية تكنولوجيا الحاسبات والاتصالات اقتصاديا واجتماعيا وسياسيا. وتعتبر هذه التكنولوجيات المتقدمة جوهرية وأساسية لا من أجلها فحسب، ولكن أيضا بما تمثله كقاطرة لكل الأنشطة والمكونات الأخرى التي ترتبط بالمنتجات والخدمات النابعة منها.

وقد شهد المجتمع المعاصر كثيرا من التطورات التي منها:

- انتشار الحاسبات الآلية وتشعبها وانتشارها في كل أوجه حياة المجتمع المعاصر
- تلاحم وتشابك تكنولوجيات المعلومات والاتصالات.
- تواصل أعظم لتكنولوجيا الحاسبات والاتصالات والتشغيل المتداخل لنظمها وتطبيقاتها.
- زيادة لا مركزية وظائف الحاسبات والاتصالات.
- نمو استخدام الحاسبات إلي المدى الذي يعتبر كل فرد مستخدم فعلي أو متوقع لشبكات المعلومات والاتصالات وخاصة في الدول المتقدمة تكنولوجيا.

إن العالم المعاصر يتجه بخطى حثيثة ومثابرة نحو مجتمع المعلومات الذي عقدت له الأمم المتحدة بالتعاون مع الاتحاد الدولي للاتصالات ITU الجولة الأولى لمؤتمر القمة العالمي لمجتمع المعلومات، جنيف: ديسمبر ٢٠٠٣، وسوف تعقد الجولة الثانية لهذا المؤتمر في تونس عام ٢٠٠٥. ويتسم مجتمع المعلومات بأنه مجتمع لا حدود له غير متأثر بالمسافة أو الوقت، كما تعتبر اقتصاديات وسياسات ومجتمعات اليوم مبنية أقل علي البنية الأساسية الجغرافية والطبيعية عما كانت عليه

في الماضي، وصارت حالياً تعتمد بزيادة مطردة علي البنية الأساسية لنظم وتطبيقات المعلومات في البيئة الرقمية التي أصبحت تفيد الحكومات والمنظمات والمنشآت والأفراد علي حد سواء. وقد صارت هذه النظم والتطبيقات المعلوماتية تمثل جزءاً مكملاً وأساسياً لأنشطة الأمن والإدارة والتجارة والتمويل القومية والدولية، كما أصبحت تستخدم بتوسع. وعلي هذا الأساس صارت هذه النظم والتطبيقات الرقمية تستخدم في أداء كثير من الخدمات والأنشطة الحكومية من خلال الحكومات الإلكترونية E-Government، التعلم الإلكتروني E-Learning، الخ. وتقدم استخدامات تطبيقات وخدمات ونظم المعلومات مدى واسع وممتد من الإمكانيات في الوصول الأعظم للموارد والخبرة والتعلم والمشاركة في الحياة المدنية والثقافية للمواطن العادي.

## ■ عوامل نظم وتطبيقات شبكة المعلومات الحديثة :

### أولاً: الاعتمادية Dependency

يتأثر كل شخص، منشأة أو مصلحة حكومية مباشرة بتطبيقات ونظم المعلومات الرقمية، ويصبح معتمداً علي وظائفها المختلفة التي تلائم استخداماته المتنوعة. علي سبيل المثال لا الحصر، إن استخدام نظم المعلومات المتزايد قد ساهم في تعميق التغييرات الأساسية التي تحدث في الإجراءات التنظيمية الداخلية في أي منظمة مما أدى إلي تبديل وتغيير الطريقة التي تتفاعل بها مع جمهور المتعاملين معها. أما في حالة فشل أي نظام معلومات، يصبح من المستحيل الاستمرار في الإجراءات الحالية بدون هذه النظم، كما يصبح من الصعب العودة مرة أخرى إلي الطرق والإجراءات القديمة التقليدية. وأصبح غير كاف تواجد سجلات ورقية، أو الاعتماد فقط علي مهارات العاملين اليدوية، أو حتى توافر عدد كبير من القوي العاملة لكي يسمح للمنظمة أو المؤسسة المعنية من الاستمرار في أداء وظائفها بمعدلات إنتاجية



عالية وجودة أحسن بنفس المدى الذي قد تعمل به مع تواجد نظم وتطبيقات المعلومات الرقمية الحديثة حتى يمكن من مواجهة المنافسين في عالم مفتوح يتسم بالعولمة. فعلى سبيل المثال أيضا، في الإمكان ملاحظة تأثير فشل نظام المعلومات الإلكتروني على الأداء وفعالية الخدمات وانتظام حركة المعاملات على شركات خطوط الطيران والبنوك وغيرها من المؤسسات التي لا تستطيع الاستغناء على التطبيقات والخدمات والنظم الإلكترونية المتقدمة. مما سبق يمكن استنباط مدى نمو الاعتماد على نظم وخدمات المعلومات الرقمية بمعدلات كبيرة غير مسبوقه. وقد صاحب هذا الاعتماد المتنامي بزوغ الحاجة الملحة لتوفير الثقة والشفافية لهذه النظم المستمرة في التطوير والتواجد في المستقبل.

### ثانيا: قابلية تعرض النظم والتطبيقات للضرر Vulnerability

كما أن استخدام تطبيقات وخدمات ونظم المعلومات الرقمية قد زاد بطريقة هائلة مما أدى إلى بزوغ فوائد ومزايا كبيرة عادت بالنفع على المنظمات والأفراد المستخدمين لها، إلا أنها أدت إلى تواجد فجوة كبيرة بين الحاجة لحماية هذه النظم والتطبيقات ودرجة الأمن الموفرة والموظفة لها بالفعل. فقد أصبح مجتمع المعلومات الحديث المتضمن الأعمال والخدمات العامة والأفراد معتمدا بصفة كبيرة على تكنولوجيات المعلومات والاتصالات الغير موثوق منها لحد كبير. وتعتبر كل استخدامات نظم المعلومات وتطبيقاتها الرقمية المحملة على شبكات الحاسبات معرضة للهجمات الضارة أو للفشل فيما يتصل بإفشاء سرية معلوماتها أو عدم حفظ خصوصية بيانات الهيئات والمتعاملين معها أو التأخر في توافرها في الوقت الملائم لمن يحتاج إليها بسرعة، أي توجد مخاطر جمة من الوصول غير المعتمد والاستخدام غير الملائم وغير المخصص أو فشل النظم ذاتها بأسباب عرضية جانبية، مع العلم بأن كثير من نظم وتطبيقات المعلومات سوء كانت عامة أو خاصة كتلك المستخدمة في الأغراض





الحربية والأمنية والبنوك والمستشفيات وغيرها تمثل أرضية خصبة للإرهاب المعلوماتي المتنامي اليوم. وفي إطار التطورات المتلاحقة المتمثلة في تزايد الحاسبات الآلية، زيادة قدرة وقوة الحاسبات، التواصلية المتداخلة، اللامركزية، نمو الشبكات وعدد مستخدميها المتنامي، تعزيز نفعية نظم المعلومات مع زيادة قابليتها للتعرض للضرر والخطر، كل ذلك جعل من الصعوبة تحديد موقع المشكلات التي يتعرض لها النظام وتحديد أسبابها للعمل علي تصحيحها بطريقة متوازنة مع وظائف ومتطلبات النظام الأخرى حتى يمكن منع تكرار حدوثها أو ارتدادها. وكما تصبح نظم المعلومات وتطبيقاتها لامركزية وتنمو بطريقة متناهية، فمن المهم مراعاة اعتماد مكوناتها وملحقاتها وتداخلها مع الموارد والمباعة من قبل موردين وبائعين ومن مصادر مختلفة ومتعددة. إضافة لما تقدم، فإن نمو تواصلية نظم شبكات المعلومات واستخدامات الشبكات الخارجية أدى إلي مضاعفة أوجه الفشل والقصور الممكنة. وتقع هذه المظاهر الخارجية خارج نطاق رقابة عمليات وحقوق ومهام الأطراف المتضمنة والمتعاملة مباشرة مع النظم، وخاصة في حالة حدوث أي هجمات وتجاوزات غير مسموح بها. وفي نفس الوقت، يكون التغيير الفني غير متوازي مع تطوير النظم، ويتخطى بعض الميادين، بينما يتأخر حدوثه في البعض الآخر. كما أن عدم القدرة في التكيف واستيعاب التطورات التكنولوجية بنفس المعدل الذي تحدث فيه التي تحدث مثلاً في حالة الفشل الملائم لاختيار أو تنسيق متغيرات النظام، قد يؤدي إلي حدوث مشكلات علي النظام. وقد تنجز التطورات التكنولوجية قبل تشعبها ونتائجها ومواقعها تجاه التكنولوجيات القائمة بالفعل مما يعتبر شيئاً مألوفاً ومفهوماً. وقد يغطي توزيع قدرات النظام بطريقة غير متساوية غير متساوية في الرقابة والوصول لنظم المعلومات بدلا مما هو مطلوب أو متوقع. كما أن زيادة عدد المستخدمين في الوصول لنظم المعلومات مع تقليل الرقابة المباشرة عليهم من قبل الشركات الموردّة أو المنظمات المستخدمة قد يؤدي إلي خسارة مالية مباشرة

كالخسارة في طلبات العملاء إلي جانب الخسارة غير المباشرة التي قد تتمثل في إفشاء خصوصية المعلومات الشخصية أو المعلومات السرية المهمة أو تلك المعلومات ذات الطابع التنافسي أو الحساسية لتواجد المنظمة ذاتها. ومن الملاحظ أيضا أن تطور الأوجه القانونية والتشريعية قد لا تكون دائما بخطى موازية مع التقدم التكنولوجي، ففي بعض الأحيان يعتبر ذلك غير كافي علي المستوى القومي إلي جانب من تواجده عدد من الحالات غير المطورة حتى الآن علي المستوى الدولي. إن تناسق وانسجام القوانين والتشريعات المرتبطة بنظم المعلومات يعتبر من الأهداف الهامة التي يجب مراعاتها والعمل علي سنها بصفة مستمرة.

### ثالثا: بناء الثقة Building Confidence

يجب أن يثق مستخدمي نظم المعلومات وتطبيقاتها في البيئة الرقمية للمنظمة المعنية في أنها تشغل وفقا لما هو مقرر لها بدون أي أعطال، أخطاء، فشل أو مشكلات غير متوقعة. وفيما عدى ذلك، فإن النظم والتكنولوجيات المرتبطة بها قد لا تكتشف في المدى الممكن لاكتشافها كما أن النمو والإبداع اللذان قد يجب علي ذلك، فإن الوصول لتأمين الشبكات وإعداد توجيهات ومعايير أمن حاکمة قد تتبع نتيجة لمتطلبات المستخدمين ذاتهم، وأن فقد الثقة في النظام والتطبيق القائم عليه قد ينبع من سوء الاستخدام، من عدم تلبية التوقعات، أو عدم التأكد الذي قد يتوصل إليه. وعلي ذلك، تحتاج نظم المعلومات الرقمية إلي توفير وبناء إجراءات وقواعد مقبولة لكل الأطراف المتعاملة معها حتى تقدم أوضاعا تزيد من الثقة والمصداقية في هذه النظم. ويجب ملاحظة أن مسؤولية الفشل في تطوير وتشغيل واستخدام النظم تقع علي كاهل مطوريها ومشغليها ومستخدميها في المقام الأول. وعلي هذا الأساس، يجب تحديد مسؤولياتهم والتزاماتهم وحقوقهم تجاه هذه النظم من خلال وضع قواعد واضحة وموحدة لتسهيل وتشجيع نمو واستغلال

النظم. ويمثل أمن المعلومات ونظمها والقدرة علي تطويرها وتشغيلها واستخدامها قضية عالمية لأن نظم المعلومات غالبا ما تتعدى الحدود القومية أو الوطنية المحدودة، فهي مشكلة تتطلب تعاونا دوليا مكثفا للتغلب عليها. وفي الواقع، بافتراض تجاهل نظم المعلومات للحدود الجغرافية والتشريعية فإنها تعتبر من المعاهدات والاتفاقات الأحسن قبولا ودعما علي المستوي العالمي. وتتضمن الخبرات المكتسبة في القطاعات الأخرى أن التكنولوجيات المتقدمة الجديدة التي قد تتضمن أخطارا وأضرار معينة تجابه تحديات ثلاثة تتمثل في:

- تطوير التكنولوجيا وتطبيقها
  - تجنب ومجابهة فشل التكنولوجيا
  - كسب المساندة العامة والموافقة علي استخدام التكنولوجيا.
- وفي هذا الإطار، يمكن اعتبار أن صناعة الطيران ناجحة في تنفيذ أساليب ومتطلبات السلامة الملاحية الجوية، حيث أنها تسهل الأداء السلس الآمن للنقل الجوي وتبعث علي إضفاء الثقة لدي الجمهور المتعامل معها. وبصفة مشابهة للمثال السابق، تستخدم صناعة السفن نظم اعتماد وسلامة لبناء السفن بنجاح. من هذا المنطلق، يجب أن يكو الهدف من صناعة المعلومات والاتصالات شبيها للمثالين السابقين يرتبط بتجنب أي قصور أو فشل يرتبط بها وتجنبه بقدر الإمكان بدرجة كبيرة من الموثوقية تختص بمنع التطفل والوصول غير المعتمد لنظم المعلومات في البيئة الرقمية.



## الفصل الثاني:

### أمن المعلومات ونظمها في البيئة الرقمية

يمثل أمن المعلومات ونظمها في البيئة الرقمية حماية المعلومات من حيث توافرها وإضفاء الثقة فيها وتأكيد سلامتها. ويعبر توافر Availability المعلومات علي خاصية من خصائص نظم المعلومات الممكن الوصول إليها واستخدامها علي أساس فوري في إطار نمط محدد ومطلوب، كما يصبح في الإمكان الوصول إلي النظام عندما يطلب بطريقة معتمدة ووفقا لمواصفات ملائمة لهذا للنظام؛ وتعتبر السرية Confidentiality خاصية ترتبط بعدم تغيير البيانات والمعلومات أو فقدها أو إهدارها وإتاحتها فقط لأشخاص وكيانات معتمدة ومصرح لها فقط باستخدامها، وتتضمن العمليات التي تستخدم أساليب التشفير والحجب لمحتويات البيانات والمعلومات أو السماح بها في أوقات وفي طرق معتمدة. أما السلامة Integrity فهي خاصية البيانات والمعلومات الدقيقة والكاملة التي تحفظ بدرجة كبيرة من الدقة والاكتمال. وتتنوع الأولوية والأهمية النسبية لتوافر المعلومات وسريتها وسلامتها طبقا لنظام المعلومات المتاح. وفيما يلي نوضح معالم أمن نظام المعلومات وإطار الأمن ومكوناته أو معالمه والتهديدات المختلفة التي يتعرض لها نظام المعلومات:

### أمن نظام المعلومات:

يمثل الهدف من أي برنامج أمن يعد لنظام المعلومات حماية معلومات المنظمة أو المنشأة المعنية بتقليل المخاطر التي قد تؤثر علي توافر المعلومات وسريتها وسلامتها بمستوي مقبول ومحدد. ويتضمن برنامج أمن المعلومات الجيد توافر عنصرين رئيسيين، يتمثلان في تحليل المخاطرة وإدارة المخاطرة. وفي مرحلة تحليل المخاطرة يراعي مستودع البيانات والمعلومات



لكل النظم المتوافرة في المنظمة. وينشأ كل نظام من نظم المعلومات قيمة خاصة للمنظمة والدرجة التي تقرر لتعرض المنظمة للمخاطرة. أما إدارة المخاطرة فهي من جهة أخرى تتضمن أساليب الرقابة ومقاييس الأمن التي تقلل تعرض المنظمة لمستوي مقبول ومسموح به من المخاطرة. ولكي يكون أمن نظام المعلومات فعالاً وكفاءً ويعكس الإحساس المشترك، يجب أن تعمل إدارة المخاطرة مع إطار الأمن، حيث تكمل مقاييس أمن المعلومات من خلال القوي العاملة المهنية في تكنولوجيا المعلومات والاتصالات والإدارة إلى جانب مقاييس الأمن الطبيعية كما يلي:

### ١ طبقات أمن المعلومات المتممة بعضها ببعض

يتضح أن إدارة أمن المعلومات هي قضية إدارية في المقام الأول، حيث يتوصل فيها إلى توازن بين قيمة المعلومات للمنظمة من جهة وتكلفة الأفراد والمقاييس الإدارية والتكنولوجية من جهة أخرى. وتضع مقاييس الأمن الحاجة في التوصل إلى أقل تكلفة من المخاطر أو الأضرار التي قد تسبب فقد سرية المعلومات وتحد من سلامتها وتوافرها.

وتتطلب كثير من المناهج المتبعة في تحليل المخاطرة الرسمية خبرة فنية عالية في مجال تكنولوجيا المعلومات وأساليب رقابة متوافقة وتوافر تكرار أحداث الخطر المحتملة التي قد تكون خارج نطاق عمليات المراجعة التقليدية المتبعة. ويتمثل الهدف من تحليل المخاطرة بناء خبرات وموارد مكتسبة بمرور الوقت.

### إطار أمن المعلومات:

يمثل أمن المعلومات أحد عناصر البنية الأساسية التي يجب أن تتاح لأمن نظام المعلومات، وعلي ذلك يجب ألا يفحص من فراغ، كما يجب وجود إطار سياسات أمن يختص بكل أوجه الأمن الطبيعي وأمن الأفراد وأمن المعلومات، بالإضافة إلى وجود أدوار ومسئوليات واضحة



للمستخدمين وأفراد الأمن وأعضاء لجنة إدارة نظم المعلومات. ويشتمل برنامج أمن المعلومات علي كل الأوجه الحساسة لمعلومات المنظمة التي تتضمن سريتها وسلامتها وتوافرها. كما يجب أن يحدد أيضا برنامج أمن المعلومات برنامجا للتوعية يوضع سبل التنفيذ ويذكر كل العاملين بالمنظمة المعنية بالمخاطر والهجمات الممكنة ومسئولياتهم في حفظ معلومات المنظمة. وإلي جانب الإشارة السابقة يمثل أمن المعلومات مجموعة من المقاييس المختلفة علي كافة المستويات الطبيعية وتلك المتعلقة بالأفراد والمقاييس الإدارية لمستويات نظام المعلومات المتكاملة معا، ويمثل أمن المعلومات مقاييس الرقابة الإدارية الجيدة. وعند وجود أي قصور في أحد المستويات يمكن أن يحدد كل المستويات الأخرى. علي سبيل المثال، إذا كانت سياسات أمن الأفراد غير متضمنة وبالتالي غير منفذة يصبح أمن المعلومات باهظ التكلفة أو علي الأقل غير ممكن مسانده. ومن جهة أخرى، يجب أن تؤكد المقاييس المخططة لكل المستويات حدا أدنى من حماية المعلومات علي أن تكون مخاطرة الأمن محسوبة ومقبولة من قبل الإدارة المعنية.

وتوجد بعض الأوضاع المعنية التي يمكن لمقاييس الأمن في أحد مستويات نظام المعلومات أن تعوض ضعف الأمن في مستويات أخرى. علي سبيل المثال، تضيف عملية التشفير Encryption حتى في الحالات التي تكون فيها مقاييس الأمن الطبيعية أو تلك المتعلقة بالأفراد أو المقاييس الإدارية ضعيفة، يصبح التشفير أحد معالم الدفاع الأخيرة للمساعدة في حماية أي أخطار تواجه سرية المعلومات.

وعند التخطيط لأمن المعلومات، يجب توازن قيمة المعلومات لإدارة المنظمة مع الحجم النسبي لأنواع المعلومات الأخرى في مواجهة حد الأمن المتوسط في الأساس. وفي كثير من المصالح والأجهزة الحكومية، يجب توافر متطلبات أمن صارمة لمعالجة وتخزين واسترجاع المعلومات ونقلها بطريقة تحمي سريتها وسلامتها في مستودعاتها المقروءة آليا.

وفيما يتصل بإطار المعلومات، يمكن ملاحظة تواجد مدخلا يتضمن طبقتين لمراجعة أمن المعلومات. ويرتكز هذا المدخل علي توظيف الإدراك المشترك والسليم في توازن تكلفة الأمن المبنية في نظام لقيمة المعلومات المتدفقة في نظام المعلومات.

### ب) مدخل الطبقتين لتحليل وإدارة مخاطرة الأمن

وتشتمل الطبقة الأولى من هذا المدخل الخاصة بتحليل المخاطرة علي المراجعة من أعلي لأسفل، وتحديد التكاليف الصافية المحتاج إليها، والخبرة والموارد المتوافرة، والتحليل المفصل. أما الطبقة الثانية المرتبطة بإدارة المخاطرة فتتضمن توصيا الأمن العام والمقاييس المعينة، والتحليل الإضافي الكمي، ومرحلة التنفيذ المتعلقة بالمقاييس المفصلة المتضمنة تكلفة الصيانة.

### مكونات ومحاور أمن المعلومات:

تنفيذ وتشغيل نظام أمن المعلومات يمثل طريقة حياة تعتمد علي أربع مكونات أساسية كل منها كل منها مهم ولا يمكن التعامل معه بصفة فردية مستقلة.

### ت) مكونات نظام أمن المعلومات

- **العمليات: Possesses** تعتبر العمليات لا غني عنها لأي نظام أمن، فهي جوهرية وذات طبيعة مستمرة. ويحكم أداة عمليات أمن المعلومات مجموعة من المعايير كتلك التي قررتها المنظمة الدولية للتوحيد القياسي ISO التي تعتبر ذات قيمة كبيرة لأي نظام أمن معلومات. وتطبق العمليات بطريقة منظمة كما تراجع باستمرار في إطار الخبرة المتراكمة بغية استبعاد الأخطاء والمخاطر.
- **بشر: People** الذين يمثلون العاملين، المستشارين، المتعاقدين، والفنيين وينجزون كل العمليات والخدمات، ويحتاج إلي تواجدهم



بأعداد وتخصصات ملائمة وبمهارات وخبرات ودافعية مناسبة

- **التكنولوجيا: Technology** تعتبر متوافرة وجاهزة، ولمنتجاتها دورات حياة قصيرة نسبيا. وتعتبر سوق التكنولوجيا ذات طبعة تنافسية، يتوافر لها عدد كبير من المنتجين و الموردين والبائعين والموزعين الذين يأتون ويذهبون ، وقد يندمجون في شركات أكبر أو قد يخسرون ويخرجون من سوق الأعمال. ويجعل ذلك من الصعب تقييم التكنولوجيا عما كانت عليه في الماضي.

- **الثقافة: Culture** ترتبط بتفسير بيئة الأعمال وتتعلق بأخلاقيات المنظمة تجاه المجتمع، حيث يكون لإدارة المنظمة دورا رئيسيا تؤديه في حفظ ثقافة المنظمة المتوافقة مع ثقافة مجتمعها. ومن أمثلة الثقافات الناجحة في إدارة أمن المعلومات التي يمكن تتبعها في مجالين رئيسيين:

- الاستخبارات، الأمن والدفاع
- الصرافة، التبادل الخارجي والتأمين

## تهديدات أمن نظم المعلومات: Threats to Information Systems

توجد كثير من التحديات تؤثر علي الأداء السليم لوظائف نظم المعلومات، التي منها: التطورات التكنولوجية المتسارعة، المشكلات الفنية المتزايدة، الأحداث البيئية المتغيرة، الضعف البشري، وعدم ملائمة المؤسسات الاجتماعية والسياسية والاقتصادية الراهنة للمتغيرات المتلاحقة، الخ. وتتبع التهديدات والمخاطر التي تواجه نظم المعلومات من الأفعال والتصرفات المقصودة وغير المقصودة علي السواء التي قد ترد من مصادر داخلية أو خارجية، كما أنها تتراوح من أحداث مفاجئة أو أحداث ثانوية تؤدي إلي عدم الكفاءة اليومية المتوقعة. علي سبيل المثال، قد تنتج الأعطال من أعطال كبيرة تؤدي إلي توقف العمل، أو إبطاء العمل بصفة دائمة، أو تقلل قيمة النظام وتفسخ خدماته. وفي هذه الحالة يجب مراعاة توقيتات الأعطال



والتشويش الذي يتعرض له النظام عند التخطيط لأمن المعلومات من البداية. والعوامل الفنية التي تؤدي لفشل نظم المعلومات عديدة ومتنوعة، كما قد تعتبر غير مفهومة في بعض الأحيان، أو تتغير على الدوام.

وقد تتبع أخطاء النظام من سوء استخدام الأجهزة والبرمجيات، الأخطاء الكامنة Bugs، التحميل الزائد أو المشكلات التشغيلية وغير ذلك. وقد تظهر الصعوبة في مكون النظام الداخلي كما في حالة أجهزة وملحقات النظام المتعلقة بوحدة الذاكرة، تجميع نظام الحسابات الشبكي أو النظام الموزع؛ أو في برمجيات نظم التشغيل والتطبيقات مثل المحرر Editor، الجامع Compiler، شبكة الكمبيوتر المحلية LAN. وقد تكون الصعوبة نابعة من مكون النظام الخارجي كما في حالة دوائر الاتصالات عن بعد أو الأقمار الصناعية، أو نتيجة لتواصل وترابط مكونات النظام المختلفة معا.

وقد تتسبب المشكلات الفنية نتيجة للهجمات المختلفة التي يتعرض لها النظام. فغالباً تدخل الفيروسات Viruses في النظام من خلال البرمجيات المصابة Infected، المتطفلين Parasites، أبواب الشراك Trap Doors، الديدان Worms، أو القنابل المنطقية Logic Bombs، الخ. التي تمثل بعض الوسائل الفنية المستخدمة لتعطيل النظام وتشويهه، إتلاف أو تحريف بياناته ووظائفه المختلفة.

والصعوبة في صيانة وحماية أمن المعلومات والنظم والشبكات قد تتبع من تواجد بيئات متعددة من الأطراف المرتبطة بها كالمتعهدين، الموردين، البائعين، الخ. علي سبيل المثال، توجد مشكلة جوهرية تتعلق بعدم توافر برمجيات تحكم ورقابة علي الوصول المعتمد التي يتفق عليها كل الأطراف المعنية. ومن مقاييس الأمن الشائعة ضرورة توافر البرمجيات في بيئة الموردين المتعددة. وحتى يمكن التوصل لذلك، يصبح من الضروري موافقة منظمات التوحيد القياسي، الموردين، والمنظمات ومستخدمي نظم المعلومات علي المعايير والتوجيهات الحاكمة لقياسات الأمن ذات الطابع الدولي.



وتقع التهديدات الطبيعية لنظم المعلومات في مجموعتين عريضتين: الأحداث البيئية الجسيمة، وأوضاع التجهيزات الطبيعية المعكوسة. وتشتمل الأحداث البيئية الجسيمة علي الحرائق، الزلازل، الفيضانات، العواصف الكهربائية، الموجات الحرارية المرتفعة، والرطوبة الزائدة وما شابه ذلك. وقد يقع نظام المعلومات يضم الحاسبات الآلية وخطوط الاتصال، حيث قد يكرس له حجرات للحاسبات الآلية وحجرات تخزين البيانات لها ارتباطات وتجهيزات للطاقة الكهربائية والاتصالات تتعرض كلها للأحداث البيئية الجسيمة عند حدوثها. أما أوضاع التجهيزات الطبيعية المعكوسة فقد تظهر من خلال اختراق مقاييس الأمن الطبيعية في حالات انقطاع التيار الكهربائي، سوء استخدام أجهزة التكييف، تسرب المياه، أو بسبب الغبار والأتربة، الخ. وقد يتأثر نظام المعلومات من الإهمال المباشر في الأماكن المخصصة له، أو غير المباشر في نقاط الربط الجوهرية خارج المنظمة كما في إمداد الكهرباء أو قنوات الاتصال عن بعد. كما يساهم البشر وما ينشأونه من مؤسسات مختلفة اقتصادية، سياسية أو اجتماعية في قصور قيمتها وأدائها مما ينجم عنه مشكلات أمنية أيضا. وقد يؤدي التنوع الكبير لمستخدمي نظام المعلومات والمتعاملين معه (العاملون، المستشارون، العملاء، المنافسون والجمهور العام) فيما يتعلق بتوعيتهم وتدريبهم واهتماماتهم المختلفة والمتفرقة في ظهور صعوبات خاصة بأمن المعلومات ونظمها.

إن نقص التدريب والتوعية الملائمة عن أمن المعلومات وأهميته تسهم في الجهل باستخدام نظم المعلومات المناسبة. وبدون تنظيم دورات تدريب ملائمة، قد يجهل كثير من العاملين والمستخدمين بأعراض الأضرار النابعة من سوء استخدام نظم المعلومات، كما قد لا يستخدمون أي مقاييس أمن حتى البدائية منها، مما قد يؤدي إلي مزاوالات تعود بالإساءة لأمن المعلومات. ويقدم اختيار كلمة المرور Password الذي يمثل نشاط المستخدم في كل أنحاء العالم بل يمثل النشاط الرئيسي لأي نظام معلومات مثلا واضحا لأمن المعلومات.

فعلي الرغم من أن كلمات المرور تطبق عادة علي رقابة الوصول إلي معظم نظم المعلومات، لا زال عدد قليل جدا من المستخدمين يعلم بأهمية الحاجة لأمن كلمة المرور بالطريقة التي تتمثل في تحديد أو إنشاء كلمة المرور ومن العواقب التي تتمثل في سوء استخدام النظام.

علي أنه بدون تدريب أو توجيه، يستطيع كثير من المستخدمين اختيار كلمات مرور واضحة يسهل تذكرها والتحقق منها مثل أسماء العائلة، الأسماء القصيرة، أو الكلمات المرتبطة بالمهام، الخ. وبعد الدخول أو الولوج في النظام، قد يترك المستخدمون غير المدربين كلمات المرور الخاصة بهم معروضة وغير مستخدمة علي النهايات الطرفية النشطة المرتبطة بنظم الشبكة، كما يفشلون في إنشاء ملفات بيانات إضافية مساندة، ويشتركون في رموز التعريف وكلمات المرور، ويتركون منافذ الرقابة والوصول مفتوحة في مواقع الأمن مما يعرضها للاختراق. وكل ذلك يمثل مشكلات الأمن التي تظهر من الدخول علي ملفات الحاسب لآلي، التحويل علي الحاسبات أو النهايات الطرفية وامتلاك كلمات المرور وسوء استخدامها.

وقد تحدث الأخطاء والاختراقات في تجميع البيانات والمعلومات ومعالجتها وتخزينها وإرسالها وحذفها. كما أن فشل عمل نسخ بديلة ومساندة للملفات والبرمجيات ذات الطبيعة الحرجة يضاعف من آثار الأخطاء والاختراقات ذات الطابع السلبي. وعندما لا توجد سياسة أمن للمنظمة المعينة تتصل بإعداد وحفظ نسخ إضافية مساندة لملفات المعلومات والبرمجيات التي تمتلكها، فإنها سوف تتحمل نفقات وخسائر واضحة ترتبط بالوقت والجهد والمال الذي ينفق في إعادة إنشائها من جديد.

إن سوء الاستخدام المقصود للنظام والوصول غير المعتمد له بغرض التطفل والنزوع للأذى وتعهد التخريب والتدمير والاحتيال أو السرقة تعتبر مخاطر وتهديدات خطيرة تؤثر سلبيا علي قابلية نمو حياة النظام والمنظمة المالكة له بل تؤثر أيضا علي القابلية للبقاء والتواجد. علي





سبيل المثال، استتساخ البرمجيات غير المعتمد المنتشر علي نطاق واسع قد يؤدي إلي خسائر كبيرة علي النظم والمنظمات. ومن المؤلفون أن جزءاً أعظم من التهديدات التي تواجه نظم المعلومات يأتي غالباً من المصادر الخارجية. كما أنه علي النقيض من ذلك، فإن الأشخاص الذين منحوا حق الوصول المعتمد للنظام قد يعرضون تهديدات أعظم تواجه نظم المعلومات أيضاً. فعلي الرغم من أنهم قد يكونوا مؤتمنين أو عاملين من ذوي النوايا الحسنة فإنهم بسبب التعب أو الإرهاق أو التدريب غير الملائم قد يقترفون أفعالاً غير متعمدة قد تسهم في حذف كميات كبيرة من البيانات الهامة للمنظمة التي يعملون بها. وفي حالة كون الأشخاص غير مؤتمنين فإنهم سيئون استخدام نظم المعلومات أو يتعمدون الوصول المعتمد علي العبث والتلاعب في النظام بطرق متعمدة بغية الاستغلال أو الثراء الذاتي للإضرار بالمنظمة التي يعملون بها.

وبرامج الحاسبات التي تمثل عنصراً مهماً من عناصر نظام المعلومات، من المحتمل أن تكون مجالاً خصباً للتهديدات التي يتعرض لها النظام، حيث قد تشتمل هذه البرامج علي فيروسات الحاسبات الالوجبة في النظام مما قد يعرض سرية بياناته وخصوصيتها وتوافرها للخطر المتزايد. بالإضافة لذلك فإن التحميل المتزايد للبيانات والمعلومات في النظام، أو تحويلها وتغييرها، وانتهاكات اتفاقيات الترخيص الممنوحة قد تعرض أمن نظام المعلومات للخطر الإضافي. علي سبيل المثال، فإن تبديل البرنامج المرخص به بطريقة غير معتمدة، قد يؤدي إلي قصور الأداء عند تفاعل البرمجيات المعدلة والمراجعة مع أجزاء النظام الأخرى. كما أن إفشاء البيانات الضمنية قد يضر بالوضع التنافسي للمنظمة مما يؤدي إلي خسارتها بل وبقائها. (Alziyyadi H, Obaid.S.Hanan, almusawi AMohammed,AL-Jama, 2023).

من هذا المنطلق، يجب أن تمتد إجراءات الأمن الملائمة لما بعد النهايات الطرفية وخطوط الاتصال إلي مجال نظم المعلومات بالكامل. فعلي سبيل المثال، عدم ملاءمة تداول وسائل تخزين البيانات والمعلومات



(سواء كانت ورقية، ممغنطة، ضوئية، الخ)، بالإضافة إلى عدم ملائمة طريقة التلخيص أو تدمير التقارير التي تمثل مخرجات النظام تؤدي إلى ثغرات أمنية مكلفة. فمثلا قد تشتمل مخرجات الحاسبات الورقية علي معلومات ضمنية أو تنافسية أو مفاتيح تخص الوصول للنظام وأصوله، كما أن كثيرا من الشركات أو المؤسسات المختلفة لا يتوافر لها سياسات واضحة للتلخيص أو استبعاد أصولها المعلوماتية مما يجعل أمن المعلومات سهلا في الاختراق.

وقد يؤدي عدم وجود سياسات واضحة لاستخدام نظام المعلومات إلى مشكلات أمن ضخمة يتعرض لها النظام، كما في حالة أعمال الصيانة والسلامة عند نقص الأفراد المؤهلين، أو بسبب تغيير ودوران العمالة، أو إدخال تكنولوجيات متقدمة تتطلب مهارات جديدة، أو إبطاء العمل أو توقفه التي يجب مراعاتها من بدء التخطيط لنظم الأمن والشفافية المطلوبة.

ومن الملاحظ أن كثيرا من المؤسسات أو المنظمات السياسية والاقتصادية والاجتماعية القائمة حاليا وخاصة في المجتمعات النامية لم تجاري حتى الآن التطور والنمو التكنولوجي المرتبط باستخدام نظم المعلومات وتأمينها، فلا يزال يوجد قصور واضح ونقص كبير في التقنين والتوحيد لعدم الأخذ بالمعايير الدولية والتشفير الخاص بالمزاولة الأحسن، إلى جانب قصور الإرشاد والتوعية والحقوق والالتزامات القانونية، مما يزيد في النفقات ويسبب تأخير الأعمال وعدم تكامل البيانات. إن السماح باستمرار الوضع الراهن يحد من النمو المستقبلي ويؤخر اللحاق بعصر المعلومات والمعرفة المستهدف.

### الأضرار الناجمة من قصور أمن المعلومات:

الأضرار التي تنجم عن قصور وفشل إجراءات الأمن تؤدي إلى خسارة مباشرة تعود بالضرر علي المنظمة المعنية. علي سبيل المثال، تتمثل الخسارة المباشرة في المصالح أو الأجهزة الحكومية علي المعالجات، محطات العمل، الطابعات، الأقراص والأشرطة وأجهزة الاتصالات؛

البرامج المتضمنة في نظم التشغيل وبرمجيات التطبيقات؛ التوثيق المتضمن المواصفات وأدلة المستخدم وإجراءات التشغيل؛ والقوي العاملة المشتملة علي المشغلين والعاملين الفنيين والمساندين للنظام والمستخدمين؛ إلي جانب البيئة الطبيعية المتضمنة حجرات الحاسبات والاتصالات وأجهزة التكييف وإمداد الطاقة الكهربائية. وعلي الرغم من أن الخسارة المباشرة قد تشكل نسبة صغيرة من الخسارة الكلية النابعة من فشل إجراءات الأمن، إلا أن الاستثمار الكامل من تطوير وتشكيل النظام يعتبر جوهريا في العادة. ويتطلب نظام المعلومات حماية تختص بحقوقه من أصول المعلومات المخزنة في أوعيته وقنواته المختلفة والمتعددة. وتتصل الحاجة لحماية النظام والطريقة التي يعمل بها بالأسلوب المرتبط بحماية البيانات والمعلومات التي يقوم النظام بتخزينها ومعالجتها ونقلها لكي يحافظ علي توافرها وسريتها وخصوصيتها، وبما يمنع تبديل أوعيتها أو قنواتها التي يدخل من خلالها البيانات والمعلومات أو تصبح عرضة للفيروسات ذات التأثير الضار والمدمر علي تشغيل واستخدام النظام. وقد تحدث الخسارة الناجمة عن ذلك، من فشل نظام المعلومات في تحقيق الأهداف المتوقعة وأداء الأنشطة والمهام والخدمات المطلوبة منه. وتشتمل الخسارة النابعة من فشل إجراءات أمن النظام علي التالي:

- خسارة السلع، الأصول الملموسة الأخرى، الاعتمادات أو الملكية الفكرية؛ خسارة معلومات قيمة.
- خسارة الرغبة في العمل الكفاء المتسم بالجودة العالية للعملاء أو الموردين.
- خسارة المطالبة بالعقوبات من الانتهاكات الضارة وعدم الالتزام بالاتفاقات والتشريعات القانونية المنظمة.
- الخسارة والأضرار النابعة من ارتباك الأعمال وعدم مصداقيتها أمام الرأي العام والأجهزة الرقابية المسئولة.

في ضوء كل ذلك تصبح مهمة حماية وتأمين البيانات والمعلومات لها الأولوية القصوى والمطلقة في تخطيط وعمل نظم المعلومات علي كافة أنواعها وتوجهاتها.

### تعزيز أمن النظم:

يجب موازنة أغراض السرية والسلامة والتوافر في مواجهة الأولويات التنظيمية الأخرى مثل فعالية التكلفة ضد انتهاكات الأمن السلبية ويجب ألا تتعدى التكلفة العائد المتوقع. وعلي ذلك يجب أن تكون أساليب الرقابة علي الأمن كافية لمنع المتطفلين والمخربين الذين يحاولون دخول نظم المعلومات لرؤية المعلومات غير المصرح بها أو الحصول عليها أو تداولها، حيث أن استخراج أو استخلاص التكاليف وكمية الوقت المطلوب تعتبر أعظم من القيمة التي الممكنة التي تكسب من الاقتحام غير المعتمد.

وتساعد المقاييس الملائمة لأمن نظم المعلومات في تأكيد دقة وسلاسة الأداء الوظيفي لنظم المعلومات. إلي جانب ذلك فيما يتصل بالعوائد التي تعود بالنفع علي نظم المعلومات التجارية، فإن أمن نظم المعلومات قد يساعد في حماية البيانات والخصوصية الشخصية والملكية الفكرية لهذه النظم التي قد تخدم أيضا في تعزيز إجراءات الأمن المستهدفة. كما أنه من جهة أخرى، أدي استخدام نظم المعلومات التجارية في جمع البيانات الشخصية وتخزينها وإحالتها أو الاتجار فيها إلي بزوغ الحاجة الملحة لحماية تلك النظم من الوصول إليها والاستخدام غير المعتمد لها. وتشتمل طرق حماية نظم المعلومات علي ضرورة التحقق من المستخدم لإضفاء الشرعية والصلاحية له، الرقابة علي الوصول لملفات البيانات والتحكم في النهايات الطرفية ومراجعة شبكة المعلومات. وفي العادة تساهم تلك المقاييس علي أمن نظم المعلومات وحماية البيانات والخصوصية الشخصية.

ومن الممكن أن يساء استخدام بعض المقاييس المطبقة والمكيفة لأمن المعلومات فيما يتصل بانتهاك الخصوصية الشخصية. علي



سبيل المثال، من المحتمل أن الشخص المستخدم لنظام المعلومات رصد بياناته لغرض غير مرتبط بالأمن للحصول علي معلومات عنه قد ترتبط ببياناته المالية والوظيفية والطبية وغيرها من البيانات الشخصية. وتعطي المبادئ والتوجيهات والمعايير التي تحدد لأمن وحماية خصوصية المعلومات الشخصية وتدفعها عبر حدود النظم بل والأمم توجيهات محددة في تحقيق واقع متوافق مع أهداف أمن نظم المعلومات وحماية خصوصية البيانات الشخصية، كما سوف يتعرض له في هذا العمل لاحقا.

وكما سبق بيانه، تتضمن نظم المعلومات الأجهزة، برامج الحاسب، قواعد البيانات، تصميمات ترتيب شرائح أشباه المعالجات Semiconductors ، البيانات والمعلومات، إلي جانب العناصر التي تحمي بواسطة قوانين الملكية الفكرية والصناعية. وتعتبر الملكية الفكرية في نظم المعلومات غير محسوسة وتتخطى الحدود الافتراضية غير المدركة وعرضة للهجمات الضارة، كما قد يقوي أمن نظم المعلومات حماية الملكية الفكرية بقصرها علي الوصول المعتمد والمصرح به لمكونات النظام كالبرمجيات أو المعلومات ذات الطابع التنافسي.



## الفصل الثالث:

### متطلبات الأمن الطبيعي لنظم المعلومات

#### الأمن الطبيعي:

كما هو الحال مع مقاييس الأمن الأساسية المستخدمة في الأعمال المنزلية العادية، فإن الأمن الطبيعي لنظم المعلومات يعتبر متطلباً رئيسياً لا بد من توافره لخدمة إنشاء بيئة وثقافة وصول مراقبة وممكنة ومعدة لحماية تعطل أو توقف نظام المعلومات بمكوناته المختلفة. وتتطلب المزاومات الأحسن لنظم أمن المعلومات تعريف التالي:

- الأفراد الذين يدخلون مواقع نظام المعلومات كحجرة الكمبيوتر أو مركز المعلومات سواء كانوا يعملون بها أو مترددين عليها لودهم أو بطريقة جماعية في بعض الوقت أو كله.
  - الشروط والمزاومات المتعلقة باستبعاد أي من مكونات النظام التي لا تستخدم.
  - الشروط المحددة لنقل وتخزين الوسائل أو الوسائط الطبيعية كالشرطة أو الأقراص الممغنطة، الأقراص المدمجة أو أقراص الفيديو الرقمية، الخ.
- إضافة لما تقدم يجب تقديم المتطلبات الفورية للنظم مثل:
- معدات الرقابة علي الوصول أو كروت التعريف والهوية.
  - أبواب ونقاط وصول أخرى مؤمنة.
  - مكتشفات الحرائق والمياه والدخان والإضاءة والدوائر التليفزيونية المغلقة.
  - إمدادات الطاقة المؤمنة والمساندة الملائمة.
  - لدواليب المغلقة وأدراج الكابلات وغير ذلك من المزاومات الهندسية المناسبة الأخرى.

وتعتبر هذه الأمور مهمة بصفة معينة عند توافر خدمات الحاسبات الآلية أو مراكز المعلومات من مصادر خارجية تختص بظاهرة «التعهيد Outsourcing». وعلي أي حال فإن مراقبة أو مراجعة مقدم أو مورد الخدمة تصبح من المتطلبات والشروط الهامة التي يجب مراعاتها. وكما سبق ذكره، يجب ألا يتطلب أمن المعلومات السماح للمتطفلين أو المهاجمين من الاتصال الطبيعي مع الحاسب الآلي وملحقاته. ويتحقق الأمن الطبيعي عندما تستخدم آليات إضافية عديدة في نمط فعال. ويمكن تحديد أربع أبعاد رئيسية تستهدفه نظم أمن المعلومات المختلفة التي تتمثل في التالي (٣):

### 1 التعريف: Identification and Authentication

من يسمح له دخول النظام؟ يجب التحقق من ذلك من خلال ثلاث مداخل أساسية وممكنة هي:

■ ضرورة إعلام أو إخبار الحاسب الآلي عن شيء معرف: أسم الشخص أو كلمة المرور Password. وعلي الرغم من أن كلمات المرور سهلة التطبيق والتنفيذ، إلا أنها تشتمل علي بعض القصور، حيث يمكن إعطائها لطرف ثالث. كما يمكن أن تكون موضوعا لقواعد معقدة ترتبط بعدد الحروف والأعداد، وتتغير بصفة كل فترة زمنية، الخ. وفي هذه الحالات يوجد توجه قوي في كتابة كلمات المرور التي يمكنها البقاء وعدم إفشاء محتواها حتى عندما يعثر عليه شخص آخر.

■ تقديم شيء ما مملوك للشخص للدخول في النظام كبطاقة هوية أو تعريف شخصي أو رمز ما، حيث يمكن أن يزداد أمن النظام بأن يطلب إضافة إلي كلمة المرور بعض أنواع المعدات الطبيعية ككارت أو بطاقة هوية أو رمز إلكتروني معين للسماح بالدخول.

■ إعطاء النظام شيء ما خاص بالمستخدم يرتبط بالخواص الشخصية مثل بصمة الإصبع أو نمط ذبذبة الصوت الشخصي التي يطلق عليها القياسات البيولوجية Biometrics حيث يمكن استخدامها في

بيئة مؤمنة. وعلي الرغم من أن التكنولوجيا المرتبطة بذلك معقدة وباهظة التكلفة، إلا أن استخدامها في تزايد مستمر.

## 2 الاعتماد: Authorization

بمجرد معرفة النظام بالمستخدم الحقيقي، فإن السؤال التالي الطبيعي هو ما يسمح به لهذا الشخص؟ وعلي ذلك فإن عملية الاعتماد تعتمد الوصول إلي الموارد لهذا المستخدم. علي سبيل المثال، تحديد المعاملات أو البيانات التي يسمح له بها، وتلك التي يمكن للمستخدم تعديلها أو إضافتها. وتبني مزايا الوصول المعتمد علي تحديد دور المستخدم ومسئوليته وحقوقه قبل النظام. وفي حالة مقدمي الخدمات المعلوماتية كالمكتبات، شركات التجارة الإلكترونية، الخ تقرر هذه المزايا بمعايير محددة تحدها العقود، الاتفاقات، الاشتراكات، أو حقوق الائتمان، الخ.

## 3 الإدارة: Administration

تمثل الإدارة عملية حفظ سمات المستخدمين ، بالإضافة إلي تعريف أمن مورد معين. ويشتمل ذلك علي أنشطة مثل استبعاد مزايا وصول مستخدم أو موظف ترك الخدمة، تغيير السمات، تحديد قائمة النظام لما يسمح به لمستخدم معين بعد الترقية أو النقل، الخ.

## 4 المراجعة: Audit

تمثل عملية المراجعة التأكد من أن مقاييس الأمن مقبولة في نظام عمل محدد. وفي هذا الصدد، لا توجد طريقة معينة لمعرفة مدى تجاوز المستخدم الاعتماد أو الاعتراف الممنوح له بدون تلك المراجعات، كما لا توجد طريقة أخرى أيضا توضح أن مقاييس الأمن يجب أن تحدد وتقوى بدون معرفة أولية لنواحي القصور التي قد تتواجد فيها، وبذلك تعتبر عملية المراجعة تكملة أساسية لكل مقاييس الأمن. وفي نفس الوقت، لن تكون أي من المقاييس فعالة بدون توافر

عدد من الخصائص ذات التوجه البشري التي تتمثل في التالي:

- مساند الإدارة والإدارة العليا بصفة خاصة لسياسات ومقاييس وعمليات أمن المعلومات، ويجب عليهم الإلزام الكامل بها قبل إعداد الأمن وإدارته.
- ضرورة إلمام كل العاملين في كل مستويات الإدارة بالمخاطر المرتبطة بأمن المعلومات وبأهميتها لمنظمتهم.
- أهمية توافق وترابط كل برامج التدريب والتوعية عن أمن المعلومات مع حاجات المنظمة.
- ضرورة مراعاة التزام الأفراد الآخرين (كأفراد الصيانة، المستشارين، المتعاقدين، القوى العاملة المؤقتة، عمال النظافة، الخ) المتعاملين مع المنظمة والمتاح لهم الوصول إلي أصول معلومات المنظمة بقواعد وشروط الأمن الموافق عليها.

### تفهم استخدام أمن نظم وتكنولوجيا المعلومات:

لا يجب أن يكون فهم استخدام نظم وتكنولوجيا المعلومات من منظور فني صرف لمن يستخدمون البرمجيات، تحديد نوع الأجهزة المتوافرة ومواصفاته الفنية، بل إن المطلوب فهمة ومعرفته عند استخدام النظم والتكنولوجيات يتمثل في التالي:

- ما الذي سوف يكون عليه تأثير حدث أمن رئيسي علي سمعة وشهرة المنظمة؟ وعلي أدائها المالي والتشغيلي، الخ؟
- كيف يصبح حرجا علي المنظمة وتوابعها التي تساند نظم وتسهيلات المعلومات مثل شبكة الويب، والبريد الإلكتروني، وتسهيلات الوسائل أو الوسائط المتعددة، الخ؟
- كيف تستجيب المنظمة جيدا للقوانين والتشريعات الملائمة، كما في حالة قوانين الملكية الفكرية، التجارة الإلكترونية والتوقيع الإلكتروني؟
- ما مسؤوليات المنظمة القانونية المرتبطة بأمن المعلومات؟



وحتى يمكن للمنظمة تطوير سياسات فعالة لأمن المعلومات، يجب عليها القيام بالمتطلبات والشروط المرتبطة بتقدير المخاطرة والبحث عن الأبعاد المعرضة للأخطار والهجمات المختلفة. ويجب أداء هذه العملية علي أساس دوري للبحث عن المشكلات الظاهرة وغير الظاهرة كما في حالات المزاوالات السيئة المرتبطة بكلمات المرور، حذف التحديثات والحزم في تسهيلات البنية الأساسية، أجهزة الموديم للمكالمات غير المعتمدة وغير ذلك من مخاطر ترتبط بشبكة معلومات المنظمة.

### تطوير سياسة أمن المعلومات:

يمثل هذا النشاط المتطلب الأول لمعيار المنظمة الدولية للتوحيد القياسي ISO 17799 الخاص بإدارة أمن المعلومات. وتعتبر السياسة الموثقة لأمن المعلومات جوهرية وضرورية، وخاصة إذا قصد نجاح أمن المعلومات، حيث أنها تمثل الطريقة الفعالة للتعامل مع الأعذار المساقة بعدم المعرفة عن الأشياء أو المهام. وتبني سياسة أمن المعلومات علي حاجات العمل أو المنظمة وترتبط بالمخاطر التي تصادفها أو تتعرض لها المنظمة المعنية ويتحتم عليها ضرورة فهمها والالتزام بأهمية تطبيقها. وفي هذه الحالة، يجب إعادة تأكيد أن أمن المعلومات ليس أمرا فنيا فقط يمكن تصحيحه والتغلب عليه بتركيب حائط نيران Firewall. بل إن هذا يمثل أيضا عملا إداريا يجب علي القوي العاملة بالمنظمة والأطراف الأخرى المتعاونة معها الاعتراف باستلام تقرير سياسة أمن المعلومات والتعهد بتطبيق ما جاء به من مبادئ ومعايير وقبول مقاييس صارمة في حالة عدم الالتزام بذلك. وكأي عملية توثيق موجهة، توجد مخاطر في أن إعداد هذه السياسة وصيانتها وتوزيعها قد ينتج عنها بيروقراطية في حد ذاتها، لذلك يصبح الحكم الجيد والصائب علي الأمور المتضمنة ضروري فيما يتصل بالنسب التي يجب تبنيها والأخذ بها، إلي جانب عدم التقليل في تقدير الجهد الذي بذل في إعداد هذه السياسة وحفظها أو صيانتها.



وتتوافر كثير من المبادئ والأسس لإعداد سياسة أمن المعلومات التي يجب يمكن أن تصبح مفيدة ، إلا أن قيمتها المضافة سوف تقرر كيفية النجاح التي توصل بها ويعمل علي تطبيقها ومتابعتها المستمرة. علما أن وثيقة أو تقرير سياسة الأمن المبنية علي أسس معينة وتحفظ أو تخزين علي أحد رفوف المكتبة أو أحد أدراج الحفظ لا تعني وجود سياسة أمن ولكنها لا تلبى أي قيمة للعمل، بل يجب تعميمها والتدريب عليها وتطبيقها ومراجعتها باستمرار. لذلك يجب أن يساند نشر تقرير سياسة أمن المعلومات حملة توعية عن الأمن لإعلام القوي العاملة بالمنظمة والأطراف الأخرى المتعاملة معها بأهمية تطبيق سياسة الأمن الموثقة، حيث يعتبر ذلك خطوة مهمة عند تدريب وتوعية العاملين الجدد في المنظمة.

### محاسبة إدارة أمن المعلومات:

يمكن في هذا الإطار عدم تحديد مدي محاسبة ومسئولية القائمين علي أي عمل في وقت معين بالعناصر الأربعة المتمثلة في: أي شخص، شخص ما، كل شخص، لا شخص. والتي يمكن تعريفها بأن كل شخص فكر أن شخصا ما سوف يقوم بالعمل أو المهمة المعينة التي في الحقيقة يمكن لأي شخص أن يؤديها، إلا أنه في النهاية لم يتم بأدائها أي شخص. ويمثل هذا القول الشائع حجم الكارثة عند إدارة أمن المعلومات بهذه الطريقة. ويتطلب تجنب هذه الحالة التعرف علي أن أمن المعلومات لا يمثل مشكلة من مشكلات تكنولوجيا المعلومات، بل يمثل مشكلة للمديرين أنفسهم لا يمكنهم التنازل عن مسؤولياتهم تجاهها. لذلك يجب علي الإدارة العليا بأي منظمة التعرف علي حاجات الأعمال وقيمة الأصول المطلوب حمايتها وتأمينها، وجعل الموارد متوافرة لنشر الأمن الضروري لها، واختبارها وإدارتها وصيانتها باستمرار.

وعلي هذا الأساس، يجب ان يقوم مديرو تكنولوجيا المعلومات أو مراكز المعلومات بأداء الأدوار التالية:

- المبادرة في وضع مقاييس أمن المعلومات.
- تنسيق أعمال الأمن في المنظمة بكل قطاعاتها وإداراتها وأقسامها. وبذلك يصبح في الإمكان محاسبة المديرين المختصين عن الطريقة التي تنفذ وتشغل بها كل الأوجه الفنية والأمنية التي تتضمن الخيارات المستخدمة، وكيف ومتي يرجع فيها لسياسة الأمن المطبقة، وما هي الموارد التي تصب في المهام التي يكلفون بأدائها وكيفية أدائها بطريقة جيدة. أما مسئولياتهم الأخرى فتختص بمدي الترتيب للدخول للتطبيقات والنظم والشبكات المتاحة، وإعداد الاختبارات لتعريف نقاط الضعف ونواحي القصور في إجراءات الأمن المطبقة، والقيام بتطوير وتحسين سبل اكتشاف البرامج والشفرات والأعمال المتطلبة لتقليل الإنذارات الزائفة، إلي جانب تنظيم وإدارة الأمن وتنفيذ مقاييسه المتفق عليها حتى يمكن تأكيد أن مصادر معلومات المنظمة آمنة من أي هجمات أو مخاطر داخلية أو خارجية.

### تنفيذ أدوات ومنتجات الأمن الملائمة:

يتطلب تنفيذ الأمن الفني اختيار وتوريد تنوع كبير من المنتجات والأدوات المحتاج إليه والتي يجب إعداد ودفن سجل فعالية خاص بها. ولهذه الأدوات والمنتجات قيمة محدودة أن لم تتركب وتوضع موضع التنفيذ بطريقة ملائمة. ويلاحظ أن الأداء الشائع لموردي هذه الأدوات والمنتجات، توريدها في مكونات معمارية يشار إليها بالفاظ مثل: «Cut of the Box» or «Shrink-Wrapped» التي تتضمن من بين الأوجه الأخرى: رقم تعريف تمهيدي للمستخدم Initial User ID ، وكلمة المرور Password لمدير أو إداري الأمن الذي قد يكون معروفا للمتطفلين Hackers. لذلك يجب تغيير هذه القيم بمعايير محددة موافق عليها قبل استخدام هذه المنتجات. ويكون مديرو أمن المعلومات المهنيين مسئولين مباشرة عن تطوير وإدخال وإدارة العمليات التي تساند إدارة ومراجعة عقود التوريد مع



سياسات الأمن المطبقة لكي يستجاب لشروطها وقواعدها المتفق عليها. وتشتمل هذه العمليات علي مهمة مراجعة الحالات، الأحداث والاتجاهات بالإضافة إلي الإشعارات والإنذارات الصناعية. وتبني المزاولة الأحسن Best Practice لتلك العمليات علي استخدام مركزية إدارة أمن المعلومات التي تؤكد التوريد المركزي وتوزيع التسهيلات علي النقاط المحددة مع تأكيد حصول المستخدمين النهائيين علي أي تحديث للبرمجيات المخصصة لحماية البيانات والبرامج من الفيروسات الضارة مثلا.



## الفصل الرابع:

### اعتبارات وأبعاد أمن المعلومات

يستعرض في هذا الفصل اعتبارات وأبعاد أمن المعلومات التي تشكل مع المتطلبات السابق الإشارة إليها المدخل الرئيسي لأمن وشفافية المعلومات.

#### اعتبارات أمن المعلومات:

يمكن تحديد ثلاث أبعاد رئيسية لأمن المعلومات هي:

#### 1 عدم تواجد أمن محقق بالكامل:

أي نظام أو أداة معلومات لا توجد طريقة واحدة لاعتماده. وتقتصر معرفة كيف استخدام النظام أو الأداة على عدد محدود جدا من الأفراد، حيث لا تظهر أو تكتشف للكثيرين غير المؤهلين والمدربين. وفي مجال أمن المعلومات الذي لا يتقبل 100% من الصناعة، يمكن ملاحظة التالي:

- تصمم البرمجيات لأداء وظائف معينة، فإن الخبراء المطورين ومنهم المتطفلين مثل كل من Hackers ، و Crackers يمكنهم عمل ذلك لأداء أشياء أخرى أيضا.
- لا توجد حتى الآن برمجيات كاملة الإتقان 100%، حيث أن كل البرمجيات تشتمل على أخطاء Bugs في التشفير أو الترميز في برامج الحاسبات.

وتعتبر العبارات الأربع التالية صحيحة بطريقة عملية في الواقع الفعلي:

- البرمجيات الجديدة تتضمن وتعني أخطاء جديدة.
- الأخطاء القديمة لا تصلح دائما.
- لا تطبق التصحيحات Fixes دائما.
- قد تشتمل التصحيحات على أخطاء جديدة.

## 2 الموازنة بين المخاطرة والتكلفة:

كل من يأخذ الإجراءات المختلفة لحماية الممتلكات والأنفس والدرجة التي تنفذ بها هذه الإجراءات تتأثر بواسطة مدى التقدير بالمخاطر المحيطة والرغبة لقبول القيود التي سوف تفرضها هذه الإجراءات في حياتنا اليومية وتكلفتها.

ويجب التعرف علي أنه في الحياة الحقيقية يمكن حدوث التالي:

- علي الرغم من إجراءات الحماية التي نتخذها، لا يوجد ضمان بأنها لا تكون فعالة كل الوقت.
- تتغير المخاطر بمرور الوقت ضد ما نسعى إليه من إجراءات لحماية أنفسنا. وتحتاج عملية التقويم وإجراءات الحماية المتخذة لأمن المعلومات إلي أن تتغير بالتبعية حتى تكون فعالة.

ويتمثل مكون مزاولة أمن المعلومات الجوهرية في تقويم وتقدير قيمة الأصول المطلوب حمايتها مع التهديدات المعرضة لها وأثار هذه الاختراقات والثغرات علي أمن المعلومات. وعلي ذلك، يصبح من الضروري تعريف مستوي المخاطرة الكامنة الممكن تقبلها.

## 3 توازن الحاجة للأمن وعدم الرضى عن الوضع القائم:

كما سبق ذكره، لا يوجد في عالم اليوم شئ كامل ومتقن كلية، ويعتبر ذلك صحيحا وحقيقيا فيما يتصل بالمعلومات والممتلكات والأنفس. ويتضمن كل إجراء أمن مضاف عملية أو نشاط إضافي موجه لمستخدمين نهائيين. وكلما تضاف هذه الإجراءات فقد تصبح، في نفس الوقت، معوقات يجب التغلب عليها بواسطة كل مستخدم نهائي، بغض النظر عن تذكره لكلمات مرور عديدة وما شابه ذلك من إجراءات أمنية. ونتيجة لذلك، يزداد تحميل مدير أو إداري النظام بأعباء جديدة عليه استيعابها وتنفيذها.

## أبعاد أمن المعلومات:

عند التعرض للإبعاد المختلفة لأمن المعلومات، يمكن استقرائها من تحليل معايير أمن المعلومات وخاصة ما أصدرته المنظمة الدولية للتوحيد القياسي ISO من معيار ISO 17779 الصادر عام 1999 المبني علي معيار معهد المعاييرة البريطاني BS 7799 الصادر عام 1995 ويعتبر كأساس نظام إدارة أمن المعلومات، ويمكن أن يلاحظ أن هذا المعيار يتسم بالتالي:

- عدم ذكر ضرورة وجود حائط نيران Firewall بدلا من ذلك يبين التحفظات المطلوبة لمنع دخول برمجيات مصابة ومعدية Malicious واكتشافها بسرعة.
- التمييز بين النظم المختلفة وعدم وجود نظام واحد يطبق في كل المنظمات، لذلك يصبح من الضروري أن تعرف كل منظمة علي متطلبات الأمن الخاصة بنظم معلوماتها.

## الأبعاد والمكونات لأمن المعلومات:

### 1 سياسة الأمن:

الغرض من سياسة أمن المعلومات يتصل بتقديم توجيه مناسب ومساندة إدارية لأمن المعلومات والتوصية بما يلي:

- إنشاء منتدى لأمن المعلومات علي مستوي الإدارة العليا في المنظمة.
- تقديم حملات وبرامج للتوعية والتدريب علي أمن المعلومات.
- إدارة المخاطرة كمدخل من مداخل العملية الإدارية في المنظمة.
- التوافق مع القوانين والتشريعات الملأئمة.

وعلي هذا الأساس، فإن أي وثيقة أو تقرير سياسة أمن المعلومات يجب أن تتضمن التالي:

- حاجة المنظمة لخطة طوارئ Contingency Plan.
- الحاجة لمساندة حفظ البيانات والمعلومات بفعالية وكفاءة.
- تجنب البرمجيات المصابة.
- توفير إجراءات رقابة علي الوصول لنظم المعلومات وبياناتها.
- تقرير الأحداث التي تتعرض لها المنظمة فيما يخص أمن معلوماتها.
- تحديد الإجراءات المطلوب اتخاذها عند حدوث عدم التوافق مع السياسة، من حيث النشاط المصاب، الاستخدام غير المناسب، الخ.

## 2 تنظيم الأمن:

- يهدف هذا البعد تركيز إدارة أمن المعلومات في المنظمة علي التالي:
- صيانة أمن تسهيلات معالجة المعلومات التنظيمية وأصول الوصول إليها من قبل الأطراف الثالثة
  - صيانة أمن المعلومات فيما يتعلق بمسئولية معالجة المعلومات وخدمات إتاحتها أو إمدادها المتعاقد عليها خارجياً من خلال «التعهيد Outsourcing».

ويحتاج تنظيم الأمن إلي إمداد المعالم التالية علي الأقل:

- إنشاء منتدى داخلي لأمن المعلومات.
- إقامة الترتيبات المختلفة لتنسيق أمن المعلومات.
- تخصيص مسؤوليات أمن المعلومات للوظائف أو القوي العاملة المختصة.
- تعريف المخاطر المصاحبة لأمن المعلومات مع إمكانيات وصول الطرف الثالث للبيانات والمعلومات.
- تأكيد أن متطلبات الأمن قد حددت في العقود والتعاقدات مع الأطراف الثالثة.
- تضمين متطلبات الأمن مع التعاقدات الخارجية.



### 3 تصنيف الأصول ورقابتها:

يهدف هذا البعد تعريف مجال إدارة أمن المعلومات وتأكيد أن أصول المعلومات قد أعطيت مستوى ملائم من الحماية. والمنظمة التي تطبق معيار ISO 17799 تقرر أي من أصول المعلومات يكون له تأثير علي تشغيل وإتاحة أنشطة المنظمة أو العمل. ويتطلب ذلك تحليل احتمالية تقرير المخاطرة، وتكتشف الأخطار المعينة ضعف أو قصور معين يؤدي إلي إتلاف أو توقف أصل أو مجموعة من الأصول عن العمل. وتعرف المخاطرة بواسطة تجميع قيمة قابلية النظام التعرض للهجوم أو الأخطار، كما تعرف وتحدد كل الأصول المرتبطة بمجال أمن المعلومات والقائمين علي حفظها وصيانتها.

### 4 أمن الأفراد:

الغرض من بعد أمن الأفراد تقليل مخاطر الأخطاء البشرية، السرقات، الاختلاسات أو سوء استخدام التسهيلات وبصفة معينة التالي:

- تأكيد أن كل المستخدمين النهائيين ملمين بمخاطر وقضايا أمن المعلومات يمكنهم مساندة سياسات أمن المنظمة في بيان أعمالها العادية الجارية.
- تقليل الأعطال والأضرار التي تتسبب من القصور في أداء الأمن بالإضافة إلي التعلم من هذه الأحداث. والمهام المطلوب اتخاذها لتلبية هذا المتطلب تتمثل في التالي:
  - تضمين اعتبارات ومسئوليات الأمن في توصيف الوظائف وإعداد عقودهم.
  - تدريب المستخدمين النهائيين.
  - تحديد تهديدات ومزاوولات الاستجابة في حالات العجز عن الأداء وأحداث الأمن.

### 5 الأمن الطبيعي والبيئي:

الغرض من هذا البعد يتمثل في تأكيد صحة وأمن تسهيلات معالجة

المعلومات التي تتمثل في التالي:

- تقليل مخاطر فشل النظم وتوقفها.
- حماية سلامة البرمجيات والمعلومات.
- صيانة وحفظ سلامة وتوافر معالجة المعلومات وتسهيلات الاتصالات.
- تأكيد حماية البنية الأساسية أو التحتية المساندة.
- تأكيد حماية المعلومات في الشبكات.
- منع تحطم أو أتلانف الأصول الخاصة بنظام المعلومات.
- استعراض ضياع المعلومات ، تعديلها أو سوء تبادلها بين المنظمات. (S,Obaid,2021).

## 6 الرقابة علي الوصول:

الغرض من الرقابة علي الوصول Access Control لنظم المعلومات يتمثل في التالي:

- منع الوصول غير المعتمد لنظم المعلومات.
- تأكيد حماية الخدمات الشبكية.
- اكتشاف الأنشطة الضارة أو غير المعتمدة.
- تأكيد أمن المعلومات عند استخدام تسهيلات الحاسبات أو العمل عن بعد

وفي هذا الصدد، يمكن ملاحظة أنه حتى الاستخدامات الفردية قد يكون لها وصولا قانونيا لنظم المنظمة، وبياناتها ومعلوماتها، كما قد لا تتضمن حقوقهم وصولا عالميا لكل أصول المعلومات المتاحة. وتحتاج أي منظمة لتعريف من له حقوق الوصول، إلي ماذا ومتي؟ ويمكن تحديد الأنشطة العادية المصاحبة للرقابة علي الوصول في التالي:

- تفسير متطلبات الرقابة علي الوصول والتركيز علي السرية والخصوصية
- إدارة حقوق وصول المستخدمين الفردية.
- تفسير مسؤوليات المستخدمين الفردية
- تفسير الآليات الملائمة للوصول لشبكة المعلومات، التطبيق المعين ونظام التشغيل المستخدم.
- تحديد السياسات والمزاوولات المختلفة لمراجعة الوصول إلي النظام واستخدامه.
- توضيح السياسات والمزاوولات لمنح إمكانيات الوصول البعيد للعاملين عن بعد وللمستخدمين المعدات المحمولة.

## 7 تطوير النظم وصيانتها:

يهدف هذا البعد تأكيد بناء الأمن في نظم المعلومات من حيث:

- منع ضياع أو فقد بيانات المستخدم، تعديلها، أو الاستخدام الخاطيء لها في نظم التطبيقات المختلفة.
- حماية سرية المعلومات وسلامتها.
- تأكيد أن نظم المعلومات وأنشطتها المساندة تؤدي بطريقة ملائمة ومؤمنة.
- حفظ أمن برمجيات وبيانات التطبيق المعين خلال دورة حياة النظام.

ويتطلب ذلك أداء التالي:

- تفسير متطلبات أمن نظم المعلومات وتطبيقاتها.
- تفسير دور الرقابة علي عملية التشفير Cryptography.
- تأكيد أمن ملفات النظام.
- تأكيد أمن تطوير ومساندة عمليات الأمن المختلفة.

## 8 إدارة استمرارية الأعمال:

يهدف هذا البعد إلى التخلص من تعارض العمليات وتوقفها، وحماية العملية الحرجة من الأعطال والفسل والكوارث المختلفة. وفي هذا الإطار يمكن تمييز ثلاث أنشطة هي:

- استعادة سيناريوهات الكوارث Disaster Recovery التي يمر بها النظام وسبل التغلب عليها؛ ويمثل ذلك مسؤولية الأطراف المختلفة التي يتعامل معها أمن النظام وتقدم الاتصالات وإدارة العمليات الفنية الأساسية التي يعتمد عليها استخدمات الآخرين عن بعد، مع تقليد البنية التحتية المناسبة لتلك السيناريوهات.
- استمرارية الأعمال Business Continuity يمثل المستوي الثاني الخاص باستمرار أداء الأنشطة الأساسية والمفسرة جيدا من موقع لآخر. ويحدد ذلك مسؤولية الإدارة العليا وعدد العاملين المطلوب الوصول إليهم علي أن يكونوا مستعدين للقيام بهذه المسؤوليات عندما يطلب منهم ذلك.
- إدارة الأزمات Crisis Management التي تعتبر من مسؤوليات الإدارة العليا. وتتضمن الاتصال مع كل الأطراف الخاصة والمهتمة بأعمال الأمن عند حدوث الأزمات المختلفة.

## 9 التوافق:

يهدف التوافق أو الالتزام Compliance تجنب أي ثغرات أو اختراقات لأي قوانين أو تشريعات مدنية أو جنائية ويعرف الالتزامات المتعاقد عليها والارتباطات مع سياسات الأمن التنظيمية وفعالية عمليات مراجعة النظام والإجراءات الأمنية.

ويتطلب هذا البعد معرفة شاملة بالإطار التشريعي والقانوني الذي تعمل فيه المنظمة، بالإضافة إلى مراجعة سياسات المن من هذا المنظور. وتصبح هذه المراجعة جزءا جوهريا لعملية التوافق والالتزام.



## الفصل الخامس:

### توجيهات أمن وشفافية نظم المعلومات

يشمل هذا الفصل علي تحديد معالم توجيهات ومعايير أمن وشفافية نظم المعلومات وتطبيقاتها وخدماتها. وبذلك سوف يستعرض الغرض من التوجيهات والمعايير، ومجالها، وأهداف الأمن بالإضافة إلي تحديد المبادئ العامة التي تبني عليها توجيهات ومعايير أمن وشفافية نظم المعلومات.

#### الغرض العام من توجيهات أمن المعلومات:

يقصد من الأغراض العامة لتوجيهات Guidelines ومعايير Standards أمن المعلومات التي تشكل وتطبق من قبل الأجهزة والمنظمات المعنية بالتوحيد القياسي والمعايرة مساعدة عمليات التطوير اللاحقة لنظم المعلومات واستخدامها. وبذلك ينظر إلي هذه الأغراض المنظمة والحاكمة كضرورة لا بد منها لزيادة الوعي بالمخاطر التي تواجه نظم المعلومات وإعادة تأكيد مدى مصداقيتها وجودتها، كما تتطلب من المنظمات والمصالح المختلفة التنسيق فيما بينها لخلق إطار شامل لأمن نظم المعلومات. كما تهدف التوجيهات والمعايير إلي زيادة الوعي بأهمية أمن نظم المعلومات، ومقاومة الاختراقات التي تواجهها من الداخل والخارج، وتجميع إحصائيات تخص أمن المعلومات بالمنظمة المعنية. وعلي هذا الأساس، ينظر إلي أغراض توجيهات ومعايير أمن المعلومات، علي أنها تحقق التالي:

- زيادة الوعي بالمخاطر التي تواجه نظم المعلومات وبطرق التأمين والإنقاذ المتوافرة للتغلب علي هذه المخاطر.
- خلق إطار عام لمساعدة أولئك المسؤولين في المنظمات والهيئات العامة والخاصة لتطوير وتنفيذ مقاييس وإجراءات

- ومزاوالات متناسقة مع أمن المعلومات ونظمها.
- دعم التعاون بين القطاعات والمنظمات المختلفة في تطوير وتنفيذ هذه القياسات والإجراءات والمزاوالات.
- رعاية الثقة فيما يتصل بنظم المعلومات وبالطريقة التي تقدم بها للمستخدمين.
- تسهيل تطوير واستخدام نظم المعلومات علي كافة المستويات القطاعية، القومية والدولية.
- دعم التعاون الدولي في تحقيق أمن نظم المعلومات.

### مجال التوجيهات والمعايير:

تتجه توجيهات ومعايير أمن المعلومات إلي التطبيق في كل نظم المعلومات، سواء كانت مملوكة، مشغلة، أو مستخدمة بواسطة كيانات أو منظمات ذات طبيعة عامة أو خاصة، أو لأغراض ذات طابع عام أو خاص. وقد تحمي عناصر هذه التوجيهات والمعايير بواسطة قوانين الملكية الفكرية أو الملكية الصناعية أو أي قوانين وتشريعات أخرى. وكما سبق تحديده، فإن الغرض من التوجيهات والمعايير يرتبط أساسا بالتطبيق الكامل لها علي كل المستويات، وتوجه لكل الأطراف المعنية المتضمنة في نظم المعلومات، وتنسق بين مدخلين مزدوجين. أحدهما لنظم المعلومات المرتبطة بالأمن القومي، والآخر متعلق بكل نظم المعلومات الأخرى.

ومن المقبول به والملاحظ حاليا، أن الحكومات في معظم دول العالم قد تجد من الضروري إصباح السرية المطلقة علي التوجيهات والمعايير وخاصة ما يرتبط بالمدخل الأول، وخاصة في حالات الأمن القومي وحفظ وصيانة النظام العام، علي أساس أن للحكومات حق السلطة المعترف به في القانون العام لعمل ما يجب عمله واتخاذ بصفة مطلقة في هذه المجالات الحيوية. علي أن أي ابتعاد عن التوجيهات والمعايير سوف يؤثر علي تنفيذها، علما بأن التوقعات علي الرغم من

قلتها التي ترتبط بالسلطات القائمة تصبح ذات أهمية عظمى. وقد يتنبأ أن المعلومات الملائمة، سواء المتضمنة في نظام معلومات عام أو خاص، سوف تكون معروفة لكل أو بعض الأطراف العاملة والمتعاملة والمهتمة بالمنظمة المحددة وفقا لسياسة الأمن المحدد بمدى التوافر والسرية والسلامة.

و يمكن أن تخاطب توجيهات ومعايير أمن المعلومات المجالات التالي:

- القطاعات العامة والخاصة.
- التطبيقات المختلفة في كل نظم المعلومات.
- القدرة علي المساندة بواسطة الإجراءات والمزاوالت المتعددة.
- توافر أمن المعلومات.

### أهداف أمن المعلومات:

يمثل أمن نظم المعلومات حماية توافر موارده ومكوناته والعمل علي سريتها وسلامتها. وفي غياب أمن كاف لنظم وتكنولوجيا المعلومات والاتصالات، لا تستخدم كل قدراتها وطاقاتها. ويؤدي غياب أو نقص الأمن إلي فقد الثقة في النظام إلي توقفه وعدم الاستفادة القصوى منه مما يجعله عبئاً علي المنظمة. وعلي هذا الأساس يجب حماية النظام والمعلومات من الأضرار التي قد تؤدي إلي فشل النظم وتعود بالخراب علي منظماتها والعاملين بها. ويعتبر أمن النظم من الركائز الضرورية والحاكمة في حماية الأفراد والمنظمات من الأضرار الناتجة من قصور لأمن، حيث يعتمد كل من الأفراد والمنظمات علي أداء نظم معلوماتهم من خلال ضمان أمنها بطرق دقيقة، ملائمة وموثوق منها. ومن الأمثلة الواضحة لأمن نظم المعلومات ما يمكن مشاهدته في نظم معلومات المستشفيات، نظم الرقابة علي المرور أو الملاحة الجوية، محطات القوي النووية، الخ. ويتجه الأمن إلي حفظ فعالية وكفاءة نظم المعلومات، وتأكيد مستوي مناسب لتوافرها وسريتها وسلامتها، إلي جانب تسهيل تطويرها واستخدامها من قبل الأفراد المعنيين بأغراض جديدة غير

تقليدية تختلف عن تلك التي تطبق بالفعل، كما تسهل استغلال تكنولوجيا المعلومات بأقصى طاقاتها وإمكانياتها. وبذلك يسهم مجال أمن النظم في حماية حقوق واهتمامات كل المعتمدين في التعامل معها من بحمايتها وصيانتها من الضرر الناتج من فشل إجراءات توافرها وسريتها وسلامتها.

## المبادئ العامة للتوجيهات والمعايير الخاصة بأمن المعلومات:

### 1 المحاسبة: Accountability

يحدد مبدأ المحاسبة ضرورة التعبير والتخصيص عن المسؤوليات والمحاسبة عنها في المواقف المختلفة المتصلة بأمن نظم المعلومات، من يمتلكها ومن يقدموها ومن يستخدمها وكل الأطراف الأخرى المرتبطة والمهتمة بها. ويتضمن ذلك:

- المديرون التنفيذيون.
- المبرمجون.
- مقدمو خدمات الصيانة.
- مديرو نظام المعلومات مثل، مديرو البرمجيات، التشغيل، والشبكات.
- مديرو تطوير البرمجيات.
- المديرون المسؤولون عن أمن نظام المعلومات.
- مراجعو نظم المعلومات داخليا وخارجيا.

### 2 التوعية: Awareness

يقصد بهذا المبدأ مساعدة الأفراد المهتمين قانونيا بنظم الأمن علي التعلم والتعرف عن أمن نظام المعلومات. ولا يقتصر ذلك علي مجرد النجاح لنظام المعلومات أو مقاييس أمن معينة، ولا يجب أن ينشأ كاتجاه لأمن مدفوف بالمخاطر. وفي هذا الإطار، فإن مستوي المعلومات التي يسعى إليه والمطابق لهذا المبدأ، يجب المساعدة في الحصول عليه بدون تهاون في إجراءات الأمن. ويتضمن هذا



المبدأ الملاك والمقدمون، حيث قد توجد حالات يحتاج فيها إلي التزود بمعلومات حول أمن النظام. علي سبيل المثال، قد يدخل مالك شبكة معلومات في اتفاق أو اشترك في خدمة قد ترغب منظمة أخرى في استخدامها لتقديم خدمات لأطراف ثالثة. وقد يتطلب مالك النظام، كجزء من الاتفاق، أن تقدم أو تتوافر له مستويات أمن معينة. وفي هذه الحالة، قد يرغب هذا الشخص أو تلك المنظمة المالكة للنظام التعرف علي أمن نظام معلوماته. وتشبيهاً بذلك، قد تتعاقد أي منظمة مع مالك شبكة المعلومات أو الحاسب الآلي لتقديم خدمات معينة قد تتطلب لتأكيدات خاصة بالأمن والقدرة المستقلة في تحقيق الأمن ومراجعتة بصفة مستمرة. ويتضمن مستخدمو نظام المعلومات أيضا في مبدأ التوعية. علي سبيل المثال، المستخدم النهائي أو العميل الذي يختار بنك معين، قد يكون له اهتمام شرعي في معرفة سياسات الأمن لهذا البنك والبنوك الأخرى. واعتمادا علي سياسات الأمن المستخدمة تسوق وتروج الخدمات المصرفية كأداة لجذب العملاء. وحتى يمكن اكتساب الثقة في نظام المعلومات، يجب أن يكون الملاك ومقدمو ومستخدمو النظام قادرين وجاهزين في التوعية عن أمن المعلومات، كما يجب عليهم أيضا أن يكونوا متضمنين في حفظ وصيانة الأمن. وبذلك يصبح مبدأ التوعية هاما في اكتساب المعرفة الملائمة والتعرف علي تواجد مزاوولات وإجراءات لأمن النظام.

### 3 الأخلاقيات: Ethics

في الحقبة المعاصرة، صارت نظم المعلومات تتخلل مجتمعاتنا وثقافاتنا، وقد صاحب ذلك نمو التوقعات والقواعد المرتبطة بالأمن الملائم في إمداد واستخدام هذه النظم. ويساند هذا المبدأ تطوير معايير اجتماعية ترتبط بأمن المعلومات التي تمثل أوجه مهمة في التعبير عن المعايير والتوجيهات لكل أعضاء المجتمع علي كافة مستوياتهم وأعمارهم بالإضافة إلي غرسها في أذهان الطلاب



والشباب والعاملين وتتضمن في الأعراف المعمول بها منذ الصغر. أي أن نظم المعلومات وأمنها يجب أن تقدم وتستخدم بالطريقة التي تحترم بها الحقوق والاهتمامات الشرعية للآخرين.

#### 4 المجالات المتعددة البنية والمتداخلة: Multidisciplinary

عند تصميم وصيانة مقاييس ومزاومات وإجراءات أمن نظم المعلومات، يصبح من المهم عرض ومراجعة المدى الشامل لاحتياجات ومتطلبات الأمن وخياراته المتوافرة. علي سبيل المثال، قد يتواجد في أي منظمة استشارة الأفراد الفنيين، أفراد الإدارة والإدارة القانونية، المستخدمين وغيرهم فيما يتصل بتكامل النظم وإجراءات الأمن بطريقة متداخلة ومتعددة مع العلم بأن لكل هذه المجموعات والأطراف المتضمنة في النظم وأمنها منظورات ومتطلبات وموارد مختلفة يجب استشارتها ومعرفتها لكي تجمع المعلومات النابعة عنها معا لإنتاج مستوي أمثل لأمن النظام المستهدف. كما أنه علي مستوي السياسة، فإن التوجيهات تسهم في إعادة تقوية الأمن بنضوج كاف. من جهة أخرى، يعترف هذا المبدأ باستخدام نظم المعلومات لأغراض عديدة مختلفة (5)، وبتنوع متطلبات الأمن نتيجة لذلك. علي سبيل المثال، قد تختلف حاجات المصالح الحكومية والمدنية للأمن عن المصالح الأمنية والحربية، كما يتنوع ويختلف أمن المعلومات فيما يتصل بكل نوع من قطاعات الأعمال والتجارة وغيرها.

#### 5 التناسبية: Proportionality

لا يتطلب كل نظام معلومات أقصى درجة من الأمن، كما أنه من المهم ألا تكون النظم آمنة بدرجة غير كافية، أي أنه من غير الجدوى أن تتعدى إجراءات الأمن المتطلبات المعقولة للنظام. وتختلف هرمية نظم المعلومات وحاجاتها الأمنية من قطاع لآخر ومن منظمة لأخرى، أي لا يوجد حل واحد لمشكلات وقضايا الأمن المختلفة والمتعددة. وفي تقويم حاجات الأمن، يجب معرفة المعلومات المستهدفة أولا

بحيث يخصص قيمة لها، كما يجب إعداد مقاييس ومزاومات وإجراءات الأمن الممكنة وتوفيرها لحماية عناصر نظام المعلومات المختلفة، وتحسب تكاليف تنفيذ وصيانة خيارات الأمن. وعلي هذا الأساس، يجب تحديد أوزان وقياس مستوي نوع الأمن المعين في مواجهة احتمال الأضرار الخطيرة التي يتعرض لها، بالإضافة إلي تكلفة مقاييس الأمن ذاتها، مع القيام بتحليل نظام المعلومات في سياق كل الإجراءات والنظم الأخرى المتطابقة، أي أن مبدأ التناسبية يتضمن مستويات وتكاليف ومقاييس ومزاومات وإجراءات الأمن التي يجب أن تكون ملائمة ومناسبة لقيمة ودرجة اعتماد الثقة واعتمادية نظام المعلومات، في مواجهة خطورة واحتمالية ومدى الضرر الكامن في النظام كمتطلبات للأمن المطلوبة.

## 6 التكامل: Integration

يعتبر أمن نظام المعلومات ذا فاعلية وكفاءة عند تصميم النظام ذاته، وتستتبط صيغ ملائمة له لكي تختبر لتجنب عدم التوافق وتقليل تكاليف الأمن الكلية له. ويتطلب الأمن في كل مرحلة من مراحل دورة حياة عملية تطوير نظام المعلومات المرتبطة بجمع البيانات والمعلومات وخلقها ومعالجتها وتخزينها ونقلها واستبعادها في كل مرحلة. ويختص مبدأ التكامل بالمقاييس والمزاومات والإجراءات الخاصة بأمن المعلومات التي يجب أن تتكامل وتنسق معا ومع غيرها من الأبعاد الأخرى في المنظمة لخلق نظام أمن معلومات متكامل ومتناسق.

## 7 الفورية أو الآنية: Timeliness

في بيئة نظم المعلومات المتواصلة والمتداخلة معا تتلاشى أهمية الوقت والمكان علي مستوي العالم. ويمكن الوصول لنظم المعلومات بغض النظر عن الموقع الطبيعي لها. ويعترف مبدأ الفورية أو الآنية، (1) أنه طبقا لطبيعة نظم المعلومات المتصلة والمتداخلة



والعابرة للحدود واحتمال حدوث الأضرار لهذه النظم بسرعة، قد تحتاج الأطراف المتضمنة إلي العمل معا بسرعة متناهية لمجابهة التحديات التي توجه نظم المعلومات. واعتمادا علي ثغرات الأمن. ويعترف هذا المعيار بحاجة القطاعات العامة والخاصة إلي إنشاء إجراءات للتعاون السريع الفوري والفعال استجابة لثغرات وأخطار الأمن. وعلي ذلك، يجب أن تعمل كل الأطراف المعنية بطريقة منسقة وبسرعة لمنع أي أخطار أو ثغرات في نظم المعلومات الخاصة بها.

### 8 إعادة التقييم: Reassessment

يعترف هذا المبدأ بديناميكية نظم المعلومات في طبيعتها، مع العلم أن متطلبات أمن نظم المعلومات تتغير علي الدوام ولا تعتبر ثابتة في كل الأوقات. وعلي ذلك، يجب أن تمر نظم المعلومات بعملية تقييم مستمرة ودورية تتعلق بقيمتها وخطورة احتمال مدي الأضرار التي تتعرض لها. بالإضافة إلي متابعة مهمة التنفيذ في ضوء التطورات التكنولوجية الحديثة سواء المطبقة بواسطة الجهة المالكة للنظام أو المتوافرة للاستخدام من قبل الآخرين. أي أن أمن نظم المعلومات يجب إعادة تقييمه دوريا، حيث أن نظم المعلومات ومتطلبات أمنها تتغير خلال الوقت.

### 9 الديمقراطية: Democracy

تقاس متطلبات أمن نظم المعلومات في مواجهة الاهتمامات الشرعية لكل الأطراف المعنية من مطورين ومشغلين ومستخدمين يرتبطون باستخدام المعلومات وتدفعها بهدف الوصول للتوازن طبقا للمجتمع الديمقراطي. وقد يفترض البعض غير الملم بأمن نظم المعلومات بأن ذلك قد يؤدي إلي قيود في الوصول للبيانات والمعلومات وفي تدفقها وحركتها. علما، أنه علي العكس، يعزز الأمن الوصول للمعلومات وتدفعها من خلال توفير نظام أكثر دقة وموثوقية وتوافر. علي سبيل المثال، يساعد انسجام وتوافق توجيهات



ومعايير الأمن الفنية في منع تكاثر النظم المتفرقة غير المترابطة معاً، وبذلك توجد ضرورة في توافق أمن نظم المعلومات من حيث استخدامها وتدفعه بعدالة وتوازن في المجتمع الديمقراطي.

## تنفيذ أمن المعلومات :

يجب أن تسعى المنظمات المعنية علي كافة توجهاتها في تأكيد أهمية الأخذ بأمن المعلومات والتوجيهات والمعايير المنظمة له، بالإضافة إلي ضرورة التواصل والتعاون والتنسيق في تنفيذ أمن المعلومات علي كافة المستويات المؤسسية والقطاعية والقومية والدولية.

## تطوير السياسات: Policy Development

### عوامل تطوير أمن المعلومات :

#### 1 انسجام وتوافق توجيهات ومعايير الأمن عالمياً:

توجد حاجة ملحة لإعداد توجيهات ومعايير أمن فنية ملائمة ترتبط بالمنتجات والنظم المستخدمة تراعي انسجام التطبيق الجغرافي المتسع والممتد علي أوسع نطاق علي مدي العالم لمعايير أمن سياسات نظم المعلومات World Wide Harmonization of Standards. إن تطوير توجيهات ومعايير أمن المعلومات يمثل المنتج التعاوني في نظم الأمن بين الحكومات ومنظمات التوحيد القياسي والمنتجين والموردين والمستخدمين لنظم المعلومات. وبينما يستهدف التوصل لمعايير منسجمة معاً، مع مراعاة عدم وجود حل أمن واحد لكل المنظمات، فإن احتياجات الأمن تتنوع إلي حد كبير من قطاع لآخر، من شركة أو منشأة لأخرى، من إدارة أو وحدة تنظيمية لأخرى، أو من نظام معلومات لآخر، الخ. ويؤدي نقص أو عدم الفهم المتوازي للمستخدمين إلي مخاطر جمة خارج نطاق التوحيد التكنولوجي المطلوب.

وعلي ذلك تتمثل الخطوة الأولى في إعداد سياسة الأمن إلي ضرورة التعرف علي التنوع الضمني لحفظ وحماية نظام المعلومات ومدى احتياجات المستخدمين المتغيرة وفهمهم لذلك العامل الحاكم.

## 2 ترويج الخبرة والمزاولة الأحسن :

ضرورة قيام كل الأطراف المعنية بأمن نظم المعلومات علي كافة مستوياتها وتنوعها بترويج خبراتها ومزاولاته الأحسن Promotion of Expertise and Best Practice في إعداد وتنفيذ سياسات أمن المعلومات الخاصة بها، بهدف تعزيز وترقية الخبرة والوعي بمفاهيم المزاولات الأحسن. ويشتمل ذلك علي تحديد الانطباعات الشخصية في تحليل المخاطر وإدارتها وتأمين النظم ومراجعتها. وقد تتنوع برامج إعداد سياسات الأمن المطبقة من قطاع لآخر أو من منظمة لأخرى. علي سبيل المثال، تختلف متطلبات سياسات أمن المعلومات في القطاع المصرفي عنها في القطاعات الأخرى.

## 3 إبرام العقود الصحيحة:

يلاحظ أن أهداف الأطراف المختلفة المرتبطة بالمعاملات أو التصرفات الإلكترونية لا تختلف عما هو متواجد في المعاملات الورقية التقليدية لحد كبير. وبصفة عامة، فإن المشاركين في نقل المعلومات، سواء كانت إلكترونية أو ورقية، يريدون معرفة والتأكد من أن المعلومات المرسلة والمتدفقة هي المرغوبة وترد من مصادر معتمدة وموثوق منها، كما أنها تصل في الشكل المرغوب فيه غير المتغير وغير المعالج صورياً. وعلي الرغم من أن أهداف أطراف المعاملات الإلكترونية والورقية متشابهة لحد كبير، إلا أن الطريقة في تحقيق هذه الأهداف ليست متشابهة بالتبعية، حيث أنها تختلف فيما يتعلق بطرق إنشائها، استخدامها، إرسالها، تخزينها، والوصول إلي المعلومات فيها. كما تختلف أيضا الطرق المستخدمة لحماية المعلومات بها من الأضرار والمخاطر التي قد تواجهها.

وعلي ذلك، فإن التحدي الذي يواجه المؤسسات والمنظمات المختلفة يتمثل في إعادة المعاملات والتأكد من صحتها بنفس مستوى الثقة التي تتوافر حالياً للمعاملات الورقية التقليدية. وقد يتحقق ذلك من خلال عدد من الطرق منها:

- إمكانية تطبيق القواعد الحالية للمعاملات الإلكترونية.
- إمكانية تعديل القواعد الحالية وتطوير قواعد جديدة.
- إمكانية تطبيق الوسائل التكنولوجية الحديثة.
- القيام بدراسات إضافية وتحسين القوانين والتشريعات التجارية التي تتضمن المعاملات الإلكترونية.
- تقوية المسؤوليات القانونية المرتبطة بصحة العقود والتعاقدات

#### 4 تخصيص المخاطر والمسئولية القانونية:

تؤثر ندرة تواجد قواعد للعقوبات والجزاءات التي تختص بتحديد الأضرار الناتجة من مدي تدني وانخفاض الإجراءات الأمنية وترتبط بتخصيص هذه المخاطر والمسئوليات القانونية Allocation of Risks and Liabilities علي فعالية وكفاءة النظم المطبقة لأمن المعلومات. وقد تشتمل هذه القواعد علي كل الأطراف المتضمنة في إجراءات الأمن كالبائعين، الموزعين، مشغلي الاتصالات، مقدمي الخدمات، المستخدمين، الخ. كما تتضمن نظاما عديدة تستخدم في نقل المعلومات التي تكون خارج سيطرة أو مراقبة معالج المعلومات المختص. وقد تكون حقوق وواجبات الأطراف المتضمنة في أمن النظام غير واضحة في حالات الأخطاء، حذف البيانات أو تشويهها مما قد يؤدي أيضا إلي فشل النظام وما يتعرض له من حوادث جمة.

وتتضح الحاجة لتواجد قواعد أمن المعلومات المرتبطة بتخصيص المخاطر والمسئولية القانونية عنها عند سرقة أو فقد اعتمادات إلكترونية محولة بين المؤسسات المصرفية أو المالية عبر الحدود الدولية علي سبيل المثال. وقد تتضمن هذه التحويلات كميات نقدية كبيرة وهي مزاوالات مالية شائعة جدا. وفي حالة عدم كفاية قواعد



تخصيص المخاطر والمسئولية القانونية حيال ذلك، يجب العمل علي تطويرها في نطاق سياسة الأمن لتحديد المسئوليات القانونية في حالات الاحتيال والغش والتحويلات السلوكية واللاسلكية المتسمة بالإهمال وعدم الموثوقية منها.

## 5 العقوبات والجزاءات:

تعتبر العقوبات والجزاءات Sanctions في استخدام نظم المعلومات وسائل مهمة لحماية اهتمامات الأطراف المتضمنة المعتمدة علي هذه النظم في توافر بياناتها وسريتها وخصوصيتها في مواجهة أي هجمات تعرضها للضرر والإفشاء والإتلاف. ومن أمثلة هذه الهجمات التي تعطل نظم المعلومات الفيروسات Viruses ، أو الديدان Worms التي قد تؤدي إلي تبديل البيانات، الوصول غير القانوني، الاحتيال أو خداع الحاسب الآلي، إعادة استنساخ البرمجيات بأسلوب غير معتمد، الخ. وللتغلب علي هذه المخاطر قد تختار المؤسسات والمنظمات المختلفة تنوع من الطرق والأساليب للتعرف عليها ووصفها. ويوجد اتفاق دولي علي أساس المحور المطلوب لمجابهة الأخطار والأضرار التي ترتبط بأمن نظم المعلومات من خلال القوانين الجنائية والمدنية التي تسنها الجهات التشريعية في دول العالم. وينعكس ذلك بالطبع علي تطوير القوانين والتشريعات المرتبطة بحماية البيانات والحد من جرائم الحاسبات الآلية. وفي نفس الوقت، يمكن التعرف علي كثير من العوامل التي قد تتفاقم نحو الأسوأ وتلك التي تقلل وتلطف من خطورة الأداء والتصرف المعين. وتحدد نيات الطرف المختص، نوع البيانات المتأثرة (كما في حالة بيانات الأمن القومي أو البيانات الطبية)، مدى الضرر الناجم، والمدى الذي يتعدى فيه الطرف المتضمن الاعتماد الممنوح له. وتتمثل العقوبات الإدارية المرتبطة بالانتهاكات أو الاعتداءات عن أمن المعلومات علي الغرامات التي قد تفرضها المنظمة أو الجهاز الإداري المختص التي تعتبرها كثير من الدول كافية إلي حد ما في مجال حماية البيانات. هذا إلي جانب، الأنواع الأخرى من



العقوبات المرتبطة بمقاييس الانضباط أو العقوبات المدنية المختلفة. وفي هذا النطاق ممكن أن يمتد مدى التعاون العربي والدولي في الأمور المرتبطة بقانون العقوبات علي جرائم أمن المعلومات بحيث تتضمن المساعدة المشتركة وتبادل المعلومات وتسليم المتهمين وغيرها من مجالات التعاون لحماية المعلومات وتأمينها بين الدول.

## 6 الكفاءة القضائية:

إضافة إلي كفاءة المحاكم القانونية المرتبطة بأمن المعلومات ونظمها، قد يرغب البعض إعطاء المنظمات أو الأجهزة الإدارية المعينة حقوقاً لفرض العقوبات الإدارية.

وقد تفرض وتخلق خاصية تدفق البيانات والمعلومات بين حدود الدول من جهة وحركة المنتهكين من جهة أخرى مشكلات كبيرة لمحاكمة جرائم الحاسبات والمعلومات. وعلي ذلك يجب توافر قواعد منسجمة خارج نطاق القوانين والتشريعات القومية، وخلال أو أثناء تطوير هذه القواعد، يجب أن تقوم كل دولة بمراجعة مدي ملائمة تشريعاتها وقوانينها المحلية حتى يمكن التعامل مع الهجمات والأخطار المعلوماتية المتدفقة عبر الحدود. كما أنه في حالة الدول التي قد تعترف التعاليم والمذهب المتواجدة بها علي إمكانية حدوث أحد عناصر الجرائم المعلوماتية من جهة، أولاً تعترف كلياً بهذه الجرائم من جهة أخرى، تبرز الصعوبات لتطبيق قوانين جنائية الحاسبات أو الجرائم المعلوماتية. وفي هذه الدول، يصبح من الضروري إدخال قواعد قانونية خاصة. علي سبيل المثال (٣)، سنت المملكة المتحدة قانوناً لسوء استخدام الحاسب Computer Misuse عام ١٩٩٩ عندما يحدث التطفل أو الاختراق في المملكة المتحدة أو أن التداخل البيئي يؤثر علي استخدام الحاسبات فيها.

وعندما اقتترف مواطن جريمة كمبيوترية في ولاية أو دولة أخرى، قد تظهر مشكلات عند اكتشاف الجريمة وتواجد مرتكبها في دولة المنشأ. وكثير من الدول لا تسلم مواطنيها للمحاكمة علي الجرائم

المعلوماتية لدولة أخرى. وفي هذه الحالات، يجب امتداد قواعد تسليم الخارجين علي القانون أو إمكانية نقل وقائع محاكماتهم إلي الدول المقترف بها الجريمة المعلوماتية. وسوف يسهم ذلك في تسهيل اتفاقات المساعدة المشتركة بين الدول والتعاون الإقليمي والدولي ونقل وقائع محاكمات الجرائم المعلوماتية في الأمور التي تخص أمن نظم المعلومات.

## 7 الأدلة والبراهين:

أمن نظم المعلومات التي يحسن تعزيز دقة بياناتها ومعلوماتها وتكاملها وتوافرها، تزداد قدراتها واعتمادها علي هذا الرصيد من البيانات والمعلومات، مما قد يساعد في إدخال واستخدام هذه المعلومات الموثوق منها كأدلة وبراهين موثقة في الوقائع الإدارية والقانونية. وفي إطار قواعد الأدلة والبراهين الواضحة في القانون المدني والقانون الجنائي وفي الوقائع الإدارية تصبح نظم المعلومات أكثر أمنا وتقدم تنبؤات أكثر دقة للأفعال والتصرفات المتضمنة. وعلي الرغم من ذلك، قد تعرض السجلات الإلكترونية الحالية بعض المشكلات لقوانين الأدلة المتواجدة بالفعل.

## التعليم والتدريب علي أمن المعلومات :

تتمثل المهمة الأولى في أمن المعلومات زيادة الوعي بالأمن لكل مستويات المجتمع المعاصر، في الأجهزة الحكومية والمنظمات والمؤسسات العامة والخاصة وكل الأفراد المستخدمين والمتعاملين مع نظم المعلومات، والتعرف علي أهمية وأهداف أمن المعلومات والمزاوالات الأحسن لإجراءات الأمن. ويتضمن دعم الوعي بأمن المعلومات التعرف علي المخاطر الكامنة وتطوير التوافق الاجتماعي لاستخدام نظم المعلومات بطريقة ملائمة. ومن الضروري عند بناء الوعي بأمن المعلومات تعاون كل الأطراف المعنية والتزام الإدارة المختصة وعلي وجه الخصوص الإدارة العليا بذلك. كما يجب أن تتضمن

برامج التعليم والتدريب علي موضوعات التوعية بأمن المعلومات التي توجه لفئات المستخدمين ورجال الإدارة علي كافة مستوياتهم الإدارية وأخصائيي الصيانة ومديري نظم المعلومات (مديري البرمجيات، مديري التشغيل، مديري الشبكات) ومديري تطوير البرمجيات والنظم، والمديرين المكلفين بأمن نظم المعلومات ومراجعي نظم المعلومات الداخليين أو الخارجيين المستقلين.

علي سبيل المثال، يجب تدريب المراجعين المؤهلين مهنيًا علي فحص وتدقيق وتقويم نظام المعلومات، كما يجب أن يمتلك هؤلاء المراجعين معرفة متعمقة عن تخطيط وتطوير وتشغيل نظم المعلومات، بالإضافة إلي امتلاك الخبرة الفعلية في أداء مراجعات نظام المعلومات. ومن المهم أيضا تقديم نوعية بأمن المعلومات ونظمها للمسؤولين عن تعزيز القانون وخاصة لرجال الشرطة، المدققين، القضاة، رجال النيابة العامة، الخ.

وبذلك تهدف برامج التعليم والتدريب دعم التوعية الضرورية بأهداف نظم المعلومات، والأداء الأخلاقي في استخدامها، وتطبيق إجراءات ومزاوالات أحسن للأمن.

## تقوية الأمن وإصلاحه وتبادل المعلومات والتعاون:

### 1 تقوية الأمن وإصلاحه:

يجب تواجد أساليب أمن ملائمة ممكن الوصول إليها كمقدمة لصيانة وتقوية الحقوق المرتبطة بأمن نظم المعلومات وإصلاح أي انتهاكات لهذه الحقوق. ويتضمن ذلك الوصول إلي المحاكم المختصة وتوفير أساليب التحري الملائمة للسلطات المختصة. وتتضمن اختراقات أمن نظم المعلومات فشل أدائها، تعمد إفسادها، سرقة بياناتها، انتهاك خصوصيتها، إفشاء سريتها، الخ.

وتوجد حاجة ملحة لبرامج تعليم واتصال وتعاون أحسن، ومشاركة المعلومات بين إدارات وأجهزة تنفيذ القانون، مشغلي قنوات



الاتصالات، مقدمي الخدمة، والبنوك علي كافة المستويات الوطنية والإقليمية والدولية. وفي هذا الصدد، يجب تعاون سلطات تنفيذ وتقوية وتنقيح القانون مع كافة الأطراف المعنية بأمن المعلومات لتسهيل الاستخبارات والتحري في الدول الأخرى. وفي هذا لإطار يجب:

- تقديم وسائل أمن ملائمة يمكن الوصول إليها لتقوية وصيانة الحقوق النابعة من تنفيذ توجيهات ومعايير الأمن.
- تقديم المساعدة والدعم الفوري فيما يتصل بالأمور الإجرائية والاستخباراتية المرتبطة بانتهاكات أمن نظم المعلومات

## 2 تبادل المعلومات:

تبادل الحكومات ووحدات القطاع العام والقطاع الخاص المعلومات فيما بينها، وتنشئ إجراءات لتسهيل وتبادل المعلومات المرتبطة بتوجيهات ومعايير الأمن التي تعمل علي تنفيذها. وكجزء من الجهود المبذولة حيال تبادل المعلومات تنشر المقاييس والمزاوولات والإجراءات التي تنشأ لمراقبة توجيهات أمن المعلومات مما يستدعي القيام بالتالي:

- تبسيط تبادل المعلومات عن توجيهات ومعايير الأمن والعمل علي تنفيذها.
- نشر المقاييس والمزاوولات والإجراءات التي تنشأ لمراعاة أمن المعلومات.

## 3 التعاون:

يجب أن تطور الحكومات كل من أجهزة القطاع العام والقطاع الخاص مقاييس ومزاوولات وإجراءات أمن سهلة ومتوافقة مع تلك المطورة من قبل الأطراف الأخرى التي تدعن وتستجيب للتوجيهات والمعايير. كما يجب أن يراعي في تطوير هذه المقاييس والمزاوولات تجنب أي تعارض وصعوبات في التطبيق. وبذلك يصبح التعاون الأساس الذي



تطور به القوانين والإجراءات المطبقة علي كافة المستويات المحلية والوطنية والإقليمية والدولية.

## الخلاصة :

استعرض هذا البحث توجهات أمن وشفافية المعلومات في ظل التوسع الكبير في استخدام تطبيقات وخدمات نظم المعلومات الإلكترونية المحملة علي كافة أنواع شبكات المعلومات (الشبكات المحلية، شبكات الإنترنت، شبكات الإكسترانت، شبكة المجال العريض وشبكة الإنترنت) التي تعتمد بعضها علي بعض، وقابليتها للتعرض للإضرار المختلفة وحاجتها لبناء الثقة فيها، وقد أدى كل ذلك إلي تعظيم موضوع أمن المعلومات ونظمها في البيئات الرقمية. وحدد مفهوم أمن المعلومات وطبقاته المختلفة، وإطاره، ومكوناته ومعاوره مع ربطه بالتهديدات التي يتعرض لها أمن نظم المعلومات والأضرار التي قد تنجم من قصور إجراءات الأمن، مع تعزيز أمن نظم المعلومات القائمة.

وناقش هذا البحث أيضا متطلبات أمن المعلومات المختلفة التي ترتبط بالأمن الطبيعي لأجهزتها وبرمجياتها وشبكاتها، وتوضيح عمليات التحقق من أمن المعلومات من حيث التعريف، الاعتماد، الإدارة والمراجعة لها، مع تفهم طرق وأساليب استخدام نظم الأمن، وتطوير السياسة الموجهة وإجراءات المحاسبة والتنفيذ المحتاج إليها. كما عرضت الدراسة الحالية اعتبارات وأبعاد أمن المعلومات، حيث تتمثل الاعتبارات في عدم تواجد نظم أمن محققة بالكامل، والتوازن بين المخاطرة والتكلفة وبين الحاجة للأمن وعدم الرضى عن الوضع القائم. أما أبعاد أمن المعلومات (٨) وخاصة ما يرتبط منها بمعايير إدارة أمن المعلومات للمنظمة الدولية للتوحيد القياسي ISO ١٧٧٧٩٩ فتشتمل علي سياسة الأمن، تنظيم الأمن، تصنيف الأصول ورقابتها،



أمن الأفراد، الأمن الطبيعي والبيئي، الرقابة علي الوصول، تطوير النظم وصيانتها، إدارة استمرارية الأعمال والتوافق. كما قد تم توضيح ضرورة إيجاد توجيهات ومعايير أمن المعلومات فيما يتعلق بالغرض العام منها ومجالها والمفاهيم الخاصة بها بالإضافة إلي تحديد المبادئ العامة منها، وكيفية تنفيذ أمن المعلومات من حيث تطوير سياسة خاصة الأمن تتسم بالانسجام مع المعايير الدولية وتروج للأطراف المعنية وتحدد المخاطر المختلفة والمسئولية القانونية وما يرتبط بها من عقوبات وجزاءات.

## المصادر والمراجع :

- أمن وشفافية المعلومات في ظل الحكومة الإلكترونية - أ.د. محمد محمد الهادي- أستاذ نظم المعلومات-أكاديمية السادات للعلوم الإدارية
- هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات، الطبعة الأولى، مكتبة الآلات الحديثة، اسيوط، ١٩٩٢. ص ٦ و ص ٢٥ .
- توم فورستر، مجتمع التقنية العالية - قصة ثورة تقنية المعلومات، الطبعة الأولى، ترجمة ونشر مركز الكتاب الأردني، الأردن، ١٩٨٩ ص ٣٣٣ .
- توم فورستر في مؤلفه ( نشر ١٩٨٨ )
- بيل جيتس - المعلوماتية بعد الانترنت ، ترجمة ونشر دار المعرفة / ١٩٩٨ الكويت ، ص ١٦٢ - ١٦٣ .
- أنظمة NetStructure من شركة انتل - مجلة الكمبيوتر وتقنية المعلومات - عدد ١٠ سنة ١٧ كانون اول ٢٠٠٠ ص ٥٤ .
- مجلة انترنت شوبر عدد ٦ / ٢٠٠٠ . ص ٢٢ .
- تطورات مشروع الانترنت [www.internet.edu](http://www.internet.edu)
- اللجنة الخاصة لنظام الانترنت. مجموعة أي بي إس إي سي العمل. اللجنة الخاصة لنظام الانترنت. إس أي جي (مجموعة منطقة أمن الإستشارية).
- Intosai. لجنة تدقيق إي بي بي (منظمة دولية لمؤسسات التدقيق العليا). علم منهج مراجعة أمن نظام معلومات: أي دليل لمراجعة أمن نظام المعلومات في المنظمات الحكومية [أكتوبر/تشرين الأول ١٩٩٥].



- Gelbstein, Eduardo and Kamal, Ahmed. Information Insecurity: A Survival Guide to the Uncharted Territories of Cyber-Threats and Cyber Security. (New York, UNICT Task Forth and UNITAR).
- Alziyyadi H, Obaid.S.Hanan, almusawi AMohammed,AL-JamaL S,(2023). E-learning after the Corona pandemic a strategic necessity and a development alternative INTERNATIONAL MINNESOTA JOURNAL OF ACADEMIC STUDIES, (VOL,1),(ISSUE,3), PP:37-15.
- Obaid, Hanan. (2021). Suggested strategies for activating the technique of geographic information systems in reducing the phenomenon of crime and terrorism «, Misan Journal of Academic Studies,(VOL :20).(ISSUE:40). pp:19-1.
- IEEE 8012.10 Standard for Interoperable Local Network Security (SILS).-
- IETF. IPSEC Working Group.
- IETF. SAAG (Security Area Advisory Group).
- INTOSAI. EPP Audit Committee (International Organization for Supreme Audit Institutions).
- Information System Security Review Methodology: A Guide for Reviewing Information System
- Security in Government Organizations [October 1995] ISO 13353: A Five Part Set of Guidelines for the Management of Information Security.
- ISO 15408: Common Criteria for Information Security Evaluation [http://www.commoncriteria.org]
- ISO 177799: Code of Practice for Management of Information Security.





- ITU Recommendation X.273; Open Systems Interconnection, Network Layer Security Protocol.
- ITU Recommendation X.509: Authentication Framework (relates to Digital certificate and Public -Key Encryption).



الجامعة الإسلامية بنينسوتا  
Islamic University of Minnesota  
المركز الرئيسي IUM