# وسائل تحقيق أمن المعلومات

**وسائل تحقيق أمن المعلومات هي مجموعة الآليات والإجراءات والأدوات التي تستخدم للوقاية من المخاطر أو تقليل الخسائر بعد وقوع الحدث على المعلومات وأنظمتها.**

**وتختلف وسائل الحماية من حيث الطبيعة والغرض وفيما يلي بعض هذه الآليات:**

- **نظم الإنذار المبكر Awareness system**
- **التوثق من شخصيات المستخدمين Authentication**
- **التحكم في الوصول Access Control**
- **تشفير البيانات Encryption**
- **برامج كشف ومعالجة الفيروسات Antivirus**
- **الجدار الناري Firewall**
- **النسخ الاحتياطية Backup**

## ❖ نظام الإنذار المبكر:

**يستخدم في هذه الآلية أجهزة حساسة (Sensors) للإنذار المبكر ضد السرقة والحريق والكوارث الطبيعية مثل الزلازل والبراكين والفيضانات ,وأجهزة حساسة ضد المواد المشعة والمواد السامة كما تشمل كاميرات المراقبة الموصلة مع شاشات العرض (Monitors) ومع أنظمة الهاتف النقال.**

## ❖ التوثق من شخصيات المستخدمين

**هو وسيلة يتم بها التحكم في الأشخاص المسموح لهم بالوصول للمعلومات والنظم العاملة عليها, إذ أن الوصول للمعلومات بواسطة الأشخاص غير المصرح لهم بذلك يؤدي لفقد سرية المعلومات وربما صحتها واتاحيتها والذي يؤدي بدوره للخسارة المالية والقانونية وفقدان ثقة الزبائن.**
**وتتكون هذه الآلية من عمليتين هما:**

١. **التعرف على الشخص Identification**
٢. **التحقق من الشخص Authentication**

**وتستخدم عملية التحقق من المستخدمين التقنيات التالية :**

- **بطاقات الهوية العادية Identity Cards**
- **كلمات السر Passwords**
- **البطاقات الذكية المستخدمة للتعريف Smart Cards**
- **وسائل التعريف البيولوجية Biological Identification التي تعتمد على سمات معينة في شخص المستخدم متصلة ببنائه البيولوجي مثل بصمة الاصبع أو الوجه أو بصمة العين أو الصوت Voice او بصمة الاوردة الدموية.**
- **المفاتيح المشفِرة Encryption Keys**
- **الأقفال الإلكترونية Electronic Locks التي تؤمن بوابات الدخول والخروج .**

**ومن أقوى وسائل التعريف والتوثق تلك التي تجمع بين تقنيتين أو أكثر من التقنيات السابقة . وأيا كانت وسيلة التعريف التي سيتبعها نظام التوثق authentication ، فإنها تخضع لنظام أمن وشروط**

وإرشادات أمنية يتعين مراعاتها ، ***كلمات السر*** على سبيل المثال وهي الأكثر شيوعا من غيرها من النظم، تتطلب أن تخضع لسياسة مدروسة وإرشادات يمكن تلخيصها في الآتي:

١. كل كلمات المرور يجب أن يتم تغيرها بشكل دوري (٦٠ يوم على الأقل حسب المواصفات العالمية)
٢. يجب أن تلتزم بالحد الأدنى للطول وهو ثمانية حروف (حسب القياسات الدولية).
٣. يجب أن تركب من خليط من الحروف(كبيرة وصغيرة) والأرقام والرموز.
٤. يجب أن لا ترتبط بشكل مباشر وسهل التخمين بأي معلومات خاصة بالمستخدم مثل اسم المستخدم ,اللقب,تاريخ الميلاد...الخ
٥. يجب عدم تفعيل الدخول التلقائي(auto login) لأنظمة الحاسب أو تذكير كلمات المرور في حالات الأنظمة الحساسة.

وكذلك باقي التقنيات ، حيث كل تقنية تحتوي على شروط امنية يجب مراعاتها لتحقيق الهدف.

### ❖ التحكم في الوصول Access Control

حق الوصول هو أحد الوسائل المُستخدمة لحماية البيانات ، وهو عبارة عن حق يُمنح إلى مُستخدم نظام معلومات (جوازات، دوائر أمنية، مرور، أحوال مدنية، وكالات سفر أو خطوط طيران...)، بحيث يمكن للموظف استخدام هذا الحق لخدمة العميل أو المواطن مثل: (عمليات التجديدات، الحجوزات...) أي أن له الحق في القيام بإجراء معين في منطقة معينة من نظام المعلومات لا يمكن له أن يتعداها، ويجب أن تكون العمليات مُسجلة بحيث يمكن معرفة اسم الموظف أو المُستخدم المسؤول عن حدوث خطأ معين في وقت معين على النظام.