WEEK 5| Chapter 5: Asset Management

Objectives

- Assign information ownership responsibilities
- Develop and use information classification guidelines
- Understand information handling and labeling procedures
- Identify and inventory information systems
- Create and implement asset classification policies

الأهداف

- تعيين مسؤوليات ملكية المعلومات
- تطوير واستخدام إرشادات تصنيف المعلومات
- فهم التعامل مع المعلومات وتصنيف الإجراءات
- تحديد وجرد نظم المعلومات
- إنشاء وتنفيذ سياسات تصنيف الأصول

Information Assets and Systems

- What is an information asset?
  - A definable piece of information, stored in any manner, and recognized as having value to the organization
  - It includes raw, mined, developed, and purchased data
  - The information is used by the company (regardless of size) to fulfill its mission or goal
  - Could be any information, such as customer and employees data, research and proprietary data, intellectual property data, and operational plans and procedures that have value to the company
  - Information Systems
    - Provide a way and a place to process, store, transmit, and communicate the information
    - Usually a combination of both hardware and software assets
    - Can be off-the-shelf or customized systems
  - If compromised the consequences could include embarrassment, legal liability, financial ruin, and even loss of life

أصول المعلومات والنظم

- ما هو أصل المعلومات؟
  - جزء محدد من المعلومات ، مخزنة بأي شكل من الأشكال ، ومعترف بأنها ذات قيمة للمؤسسة
  - وهي تشمل البيانات الأولية والمعدنية والمتطورة والمشتراة
  - يتم استخدام المعلومات من قبل الشركة (بغض النظر عن حجمها) لتحقيق رسالتها أو هدفها
  - يمكن أن تكون أي معلومات ، مثل بيانات العملاء والموظفين ، والبحوث وبيانات الملكية ، وبيانات الملكية الفكرية ، والخطط والإجراءات التشغيلية التي لها قيمة للشركة.
  - نظم المعلومات
    - توفير طريقة ومكانًا لمعالجة المعلومات وتخزينها ونقلها وإيصالها
    - عادة ما يكون الجمع بين أصول الأجهزة والبرمجيات
    - يمكن أن يكون أنظمة جاهزه أو مخصصة
  - إذا تعرض للخطر ، يمكن أن تشمل العواقب الإحراج ، والمسؤولية القانونية ، والخراب المالي ، وحتى الخسائر في الأرواح.

Example of Information Assets and Systems

- Data stores or warehouses of information about customers, personnel, production, sales, marketing, or finances.
- Intellectual property (IP) such as drawings, patents, music scores or other publication that have commercial value
- Operational plans and procedures that have value to the company
- Research documentation
- Strategic and operational plans and procedures that define the organization

مثال على أصول المعلومات والأنظمة

- مخازن البيانات أو مستودعات المعلومات حول العملاء أو الموظفين أو الإنتاج أو المبيعات أو التسويق أو المالية.
- الملكية الفكرية (IP) مثل الرسومات أو براءات الاختراع أو نتائج الموسيقى أو غيرها من المطبوعات التي لها قيمة تجارية
- الخطط والإجراءات التشغيلية ذات القيمة للشركة
- وثائق البحث
- الخطط والإجراءات الاستراتيجية والتشغيلية التي تحدد المنظمة

Information Assets and Systems cont.

- Information Ownership
  - ISO stands for information security officer
  - The ISO is accountable for the protection of the organization. Compare this with:
    - The information owner is responsible for the information he owns
    - The information custodian is responsible for implementing the actual controls that protect the information assets
  - The ISO is the central repository of security information

أصول المعلومات والنظم

- ملكية المعلومات
  - ISO يرمز إلى ضابط أمن المعلومات
  - ISO مسؤولة عن حماية المنظمة. قارن هذا مع:
    - مالك المعلومات هو المسؤول عن المعلومات التي يملكها
    - أمين المعلومات هو المسؤول عن تنفيذ الضوابط الفعلية التي تحمي أصول المعلومات
  - ISO هو المستودع المركزي للمعلومات الأمنية

Role of data owner

- Defining the asset
- Assigning value to the asset
- Defining the level of protection required
- Deciding who should have access to the asset
- Delegating day-to-day security and operational tasks
- Ongoing governance

not the one who will be tasked with implementing security controls

دور مالك البيانات

- تحديد الأصل
- تعيين القيمة إلى مادة العرض
- تحديد مستوى الحماية المطلوبة
- تحديد من يجب أن يكون لديه حق الوصول إلى الأصل
- تفويض المهام الأمنية والتشغيلية اليومية
- حوكمة مستمرة

ليس الشخص الذي سيتم تكليفه بتنفيذ ضوابط الأمان

Information Security Officer

- Accountable for the protection of the information asset.
- Managing the day-to-day controls
- Provide direction and guidance as to the appropriate controls and to ensure that controls are applied consistently throughout the organization
- ISO central repository of security information
- Publishes the classification criteria, maintains the information systems inventories, and implements broad strategic and tactical security initiatives

ضابط أمن المعلومات

- مسؤول عن حماية أصول المعلومات.
- إدارة عناصر التحكم اليومية
- توفير التوجيه والإرشاد فيما يتعلق بالضوابط المناسبة وضمان تطبيق الضوابط باستمرار في جميع أنحاء المنظمة
- مستودع ISO المركزي للمعلومات الأمنية
- ينشر معايير التصنيف ، ويحافظ على قوائم جرد نظم المعلومات ، وينفذ مبادرات أمنية استراتيجية وتكتيكية واسعة النطاق

Policy Statement:

- All information assets and systems must have an assigned owner.
- The Office of Information Security will maintain an inventory of information ownership.
- Owners are required to classify information and information systems in accordance with the organizational classification guidelines.
- Owners are responsible for determining the required level of protection.
- Owners must authorize internal information and information system access rights and permissions. Access rights and permissions must be reviewed and approved annually.
- Owners must authorize third-party access to information or information systems. This includes information provided to a third party.
- Implementation and maintenance of controls is the responsibility of the Office of Information
- Security; however, accountability will remain with the owner of the asset.

بيان السياسة:

- يجب أن يكون لجميع أصول المعلومات والنظم مالك معين.
- سيحتفظ مكتب أمن المعلومات بقائمة لملكية المعلومات.
- يُطلب من المالكين تصنيف أنظمة المعلومات والمعلومات وفقًا لإرشادات التصنيف التنظيمية.
- يتحمل المالكون مسؤولية تحديد مستوى الحماية المطلوب.
- يجب على المالك تخويل حقوق الوصول والأذونات الداخلية للمعلومات ونظام المعلومات. يجب مراجعة حقوق الوصول والأذونات والموافقة عليها سنويًا.
- يجب على المالك تخويل وصول طرف ثالث إلى المعلومات أو أنظمة المعلومات. ويشمل ذلك المعلومات المقدمة إلى طرف ثالث.
- تقع مسؤولية تنفيذ وصيانة الضوابط على عاتق مكتب المعلومات
- الأمان؛ ومع ذلك ، ستظل المسؤليه مع مالك الأصول

Information Classification

- The objective of an **information classification system** is to differentiate data types.
- Definitions:
  - **Information Classification**
    - Information classification is the organization of information assets according to their sensitivity to disclosure
  - **Classification Systems**
    - Classification systems are labels that we assign to identify the sensitivity levels

تصنيف المعلومات

- الهدف من نظام تصنيف المعلومات هو التمييز بين أنواع البيانات.
- تعريفات:
  - **تصنيف المعلومات** - تصنيف المعلومات هو تنظيم أصول المعلومات وفقا لحساسيتها للإفصاح
  - **أنظمة التصنيف** - أنظمة التصنيف هي تصنيفات نقوم بتعيينها لتحديد مستويات الحساسية

Information Classification Lifecycle Process

- Assignment of classification ends with declassification. The information owner is responsible for managing this process.
- Document the information asset and the supporting information systems.
- Assign a classification level.
- Apply the appropriate labeling.
- Document “special” handling procedures (if different from organizational standards).
- Conduct periodic classification reviews.
- Declassify information when (and if) appropriate.

تصنيف دورة حياة عملية المعلومات؟

- تعيين التصنيف ينتهي مع تخفيض التصنيف. مالك المعلومات هو المسؤول عن إدارة هذه العملية.
- توثيق أصل المعلومات ونظم المعلومات الداعمة.
- تعيين مستوى تصنيف.
- تطبيق التصنيف المناسب.
- توثيق إجراءات المناولة "الخاصة" (إذا كانت مختلفة عن المعايير التنظيمية).
- إجراء مراجعات التصنيف الدورية.
- إلغاء تصنيف المعلومات عندما تكون مناسبة.

Classification Systems

- FIPS-99 - Sensitivity of the data to be protected
- Government and Military - Based on Executive order of who is handling the data
- Commercial - As per the organization’s hierarchy, decided by the information owner

أنظمة التصنيف

- FIPS-99- حساسية البيانات المراد حمايتها
- الحكومة والعسكرية - بناءً على الأمر التنفيذي لمن يتعامل مع البيانات
- تجاري - وفقًا للتسلسل الهرمي للمؤسسة ، يقرره مالك المعلومات

Information Classification

- Federal Information Processing Standard 199 (FIPS-199) requires information owners to classify information and information systems based on CIA criteria as:
  - Low potential impact
    - the loss of CIA could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals
  - Moderate potential impact
    - the loss of CIA could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.
  - High potential impact
    - the loss of CIA could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals
  - SC of information type = {(confidentiality, impact), (integrity, impact), (availability, impact)},

تصنيف المعلومات

- يتطلب المعيار الفيدرالي لتجهيز المعلومات 199 (FIPS-199) من مالكي المعلومات تصنيف أنظمة المعلومات والمعلومات بناءً على معايير CIA على النحو التالي:
  - تأثير محتمل منخفض
    - من المتوقع أن يكون لخسارة CIA تأثير ضار محدود على العمليات التنظيمية أو الأصول التنظيمية أو الأفراد
  - تأثير محتمل معتدل
    - من المتوقع أن يكون لخسارة CIA تأثير ضار خطير على العمليات التنظيمية أو الأصول التنظيمية أو الأفراد.
  - تأثير محتمل مرتفع
    - من المتوقع أن يكون لخسارة CIA تأثيرًا ضار بشكل كارثيًا على العمليات التنظيمية أو الأصول التنظيمية أو الأفراد
  - SC نوع المعلومات = {(السرية ، التأثير) ، (السلامه ، التأثير) ، (التوافر ، التأثير)} ،

Examples of FIPS-199 classification

- An organization managing public information on its web server determines that there is no potential impact from a loss of confidentiality (that is, confidentiality requirements are not applicable), a moderate potential impact from a loss of integrity, and a moderate potential impact from a loss of availability
- The resulting SC of this information type is expressed as follows:
- Security Category (SC) public information ={(confidentiality,n/a), (integrity,moderate), (availability,moderate)}

أمثلة على تصنيف FIPS-199

- تحدد منظمة تدير المعلومات العامة على خادم الويب الخاص بها أنه لا يوجد أي تأثير محتمل من فقدان السرية (أي أن متطلبات السرية غير قابلة للتطبيق) ، وتأثير محتمل معتدل من فقدان النزاهة ، وتأثير محتمل معتدل من الخسارة من التوافر
- يعبر عن SC الناتج عن هذا النوع من المعلومات على النحو التالي:
- معلومات عامة عن فئة الأمان (SC) = {(السرية ، n / a) ، (السلامه ، متوسط) ، (التوفر ، متوسط)}

Information Classification Cont.

Government & Military Classification Systems	أنظمة التصنيف الحكومية والعسكرية
Top Secret (TS) Applied to “any information or material the unauthorized disclosure of which reasonably could be expected to cause an **exceptionally grave damage** to the national security”	**سري للغاية (TS)** بالتطبيق على "أي معلومات أو مواد قد يُتوقع أن يؤدي الكشف غير المصرح عنه والذي يمكن أن يتسبب بشكل معقول في إلحاق ضرر جسيم بشكل استثنائى بالأمن القومي"
Secret (S) Applied to “any information or material the unauthorized disclosure of which reasonably could be expected to cause **serious damage** to the national security”	**سري (S)** بالتطبيق على "أي معلومات أو مواد قد يُتوقع أن يؤدي الكشف غير المصرح عنه والذي يمكن توقع حدوثه إلى إلحاق ضرر حقيقي بالأمن القومي"
Confidential (C) Applied to “any information or material the unauthorized disclosure of which reasonably could be expected to **cause damage** to the national security”	**خاص (C)** بالتطبيق على "أي معلومات أو مواد قد يكون من المتوقع أن يؤدي الكشف غير المصرح عنه والذي من المتوقع أن يسبب ضرراً للأمن القومي"
Unclassified (U) Applied to “any information that can generally be **distributed to the public** without any threat to national interest”	**غير مصنف (U)** تُطبق على "أي معلومات يمكن توزيعها بشكل عام على العامة دون أي تهديد للمصلحة الوطنية”
Sensitive But Unclassified (SBU) Applied to “any information of which the loss, misuse or unauthorized access to, or modification of might **adversely affect** U.S. National Interests, the conduct of the Department of Defense (DoD) programs or the privacy of **DoD personnel**”	**حساس لكن غير مصنف (SBU)** بالتطبيق على "أي معلومات قد يؤثر فيها فقدان أو سوء الاستخدام أو الوصول غير المصرح به أو التعديل عليه سلبًا على المصالح الوطنية ، أو تنفيذ برامج وزارة الدفاع (DoD) أو خصوصية موظفي وزارة الدفاع“

Information Classification Cont.

Commercial classification systems:

- No standard: Each company can choose its own system that matches its culture and needs
- Usually less complex than the government system
- The more regulated a company, the more complex the classification system it adopts
- Most systems revolve around these four classification levels:
  - Protected
  - Confidential
  - Internal Use
  - Public
- Protected
  - Data protected by law, regulation, memorandum of agreement, contractual obligation, or management discretion
  - Examples: Social Security numbers, personal health information, financial information
- Confidential
  - Data essential to the mission of an organization
  - Only available to a small circle of authorized individuals
  - Disclosure would cause significant financial loss, reputation loss and/or legal liability
- Internal Use:
  - Data necessary for conducting ordinary company business
  - Loss, disclosure, and corruption may impair the business and lead to business, financial, or legal loss
- Public:
  - Information that does not require protection
  - Information that is specifically intended for the public

تصنيف المعلومات

أنظمة التصنيف التجاري:

- لا يوجد معيار: يمكن لكل شركة أن تختار نظامها الخاص الذي يناسب ثقافتها واحتياجاتها
- عادة ما تكون أقل تعقيدًا من النظام الحكومي
- وكلما كانت الشركة أكثر تنظيماً ، كلما كان نظام التصنيف أكثر تعقيدًا
- تدور معظم الأنظمة حول مستويات التصنيف الأربعة التالية:
  - محمي
  - خاص
  - الاستخدام الداخلي
  - عامة
- محمي
  - البيانات المحمية بموجب القانون أو اللائحة أو مذكرة الاتفاق أو الالتزام التعاقدي أو تقدير الإدارة
  - أمثلة: أرقام الضمان الاجتماعي ، والمعلومات الصحية الشخصية ، والمعلومات المالية
- سري
  - البيانات الأساسية لمهمة المنظمة
  - متوفرة فقط لدائرة صغيرة من الأفراد المصرح لهم
  - سيؤدي الإفصاح إلى خسارة مالية كبيرة أو فقدان سمعة و / أو مسؤولية قانونية
- الاستخدام الداخلي:
  - البيانات اللازمة لإجراء أعمال الشركة العادية
  - الخسارة والكشف والفساد قد يضعف العمل ويؤدي إلى خسارة تجارية أو مالية أو قانونية

عامة:

- المعلومات التي لا تتطلب الحماية
- المعلومات المخصصة للجمهور

Reclassification/Declassification

- The need to protect information may change
- With that change, the label assigned to that information may change as well
- The process of downgrading sensitivity levels is called declassification
- The process of upgrading sensitivity levels is called reclassification

رفع تصنيف / تخفيض السرية

- قد تتغير الحاجة لحماية المعلومات
- مع هذا التغيير ، قد تتغير التسمية المعينة لتلك المعلومات أيضًا
- تسمى عملية تقليل مستويات الحساسية تخفيض التصنيف
- تسمى عملية ترقية مستويات الحساسية رفع التصنيف

Labeling and Handling Standards

Information labeling:

- Labeling is the vehicle for communicating the assigned classification to information custodians and users
- Labels must be clear and self-explanatory
- In electronic form, the label should be made part of the filename
- In printed form, the label should be clearly visible on the outside and in the header and/or footer

Information handling:

- Information must be handled in accordance with its classification
- The information user is responsible for using the information in accordance with its classification level

معايير رمز التصنيف و التعامل مع المعلومات

رمز تصنيف المعلومات:

- التصنيف هي وسيلة لتوصيل التصنيف المخصص لأمناء المعلومات والمستخدمين
- يجب أن تكون التصنيفات واضحة ومسفره ذاتيا
- في شكل إلكتروني ، يجب أن يكون رمز التصنيف جزءًا من اسم الملف
- في شكل مطبوع ، يجب أن يكون رمز التصنيف ظاهره بوضوح في الخارج وفي الرأس و / أو الذيل

التعامل مع المعلومات:

- يجب التعامل مع المعلومات وفقا لتصنيفها
- مستخدم المعلومات هو المسؤول عن استخدام المعلومات وفقا لمستوى تصنيفها

Information Systems Inventory

- Many organizations don’t have an up-to-date inventory
- Creating a comprehensive inventory of information systems is a major task
- Both hardware and software assets should be inventoried
- Each asset should have a unique identifier and a description
- Company assets should be accounted for at all times
- An asset management procedure should exist for moving and destroying assets
- Hardware assets include (but are not limited to):
    - Computer equipment
    - Printers
    - Communication and network equipment
    - Storage media
    - Infrastructure equipment
- Software assets include (but are not limited to):
    - Operating system software
    - Productivity software
    - Application software

جرد نظم المعلومات

- لا تمتلك العديد من المؤسسات مخزونًا حديثًا
- يعد إنشاء مخزون شامل لأنظمة المعلومات مهمة رئيسية

- يجب أن يتم جرد أصول الأجهزة والبرامج
- يجب أن يكون لكل أصل معرف فريد ووصف له
- يجب مراعاة أصول الشركة في جميع الأوقات
- يجب أن يوجد إجراء لإدارة الأصول لنقل وتدمير الأصول
- تتضمن أصول الأجهزة (على سبيل المثال لا الحصر):
  - معدات الحاسوب
  - طابعات
  - معدات الاتصالات والشبكات
  - وسائط التخزين
  - معدات البنية التحتية
- تشمل أصول البرمجيات (على سبيل المثال لا الحصر):
  - برنامج نظام التشغيل
  - برنامج الإنتاجية
  - تطبيق البرمجيات

Summary

- A company cannot defend its information assets unless it knows what it is and where it is. Furthermore, the company must also identify how critical these assets are to the business process.
- FISMA requires federal agencies to classify their information and information systems as low, moderate, or high security based on criteria identified in FIPS-199.
- Companies need an inventory of their assets and a classification system for those assets.