**Most common Security Policies**

|  |  |  |
| --- | --- | --- |
| **Security Policy** | **Definition** | **Example** |
| Data Handling Policy | This aspect of the policy defines whether data is for use within the company, is restricted for use by only certain roles or can be made public to anyone outside the organization. | A company that handles customer information may have a policy to keep that information on secure servers accessible only to authorized employees. |
| Password Policy | A set of guidelines for creating and managing strong, secure passwords. | A company may require its employees to create passwords with a combination of upper and lower case letters, numbers, and special characters, and to change them regularly. |
| Acceptable Use Policy (AUP) | A set of rules defining appropriate use of the company's IT resources by employees. | A company may have a policy prohibiting the use of social media in the workplace or the download of unauthorized software. |
| Bring Your Own Device (BYOD) Policy | A policy that defines the rules for the use of personal devices in the workplace. | A company may allow its employees to use their own mobile devices, such as smartphones and tablets, to access email and other company resources, but with restrictions on what  information can be accessed and how it is stored. |
| Privacy Policy | A set of guidelines defining how customers' or users' personal information will be collected, used, and protected by the company. | An e-commerce website may have a privacy policy defining how customers' payment information is collected and protected. |
| Change Management Policy | A set of guidelines defining how changes to the company's IT environment should be managed and implemented. | A company may have a policy requiring review and approval of changes to software or hardware before they are implemented in production. |

**Change Management Components**

1. - Request for Change: All of the major change management practices address a common set of core activities that start with a request for change (RFC) and move through various development and test stages until the change is released to the end users.
2. - Approval: These processes typically include: Evaluating the RFCs for completeness, Assignment to the proper change authorization process based on risk and organizational practices, Stakeholder reviews, resource identification and allocation, Appropriate approvals or rejections, and Documentation of approval or rejection.
3. - Rollback: Depending upon the nature of the change, a variety of activities may need to be completed. These generally include: Scheduling the change, Testing the change, Verifying the rollback procedures, Implementing the change, Evaluating the change for proper and effective operation, and Documenting the change in the production environment. Rollback authority would generally be defined in the rollback plan.

# **Data Handling**

Here we will summarize the data Life Cycle

|  |  |
| --- | --- |
| **Lifecycle** | **Description** |
| Create | Creating the knowledge, which is usually tacit knowledge at this point. |
| Store | Storing or recording it in some fashion (which makes it explicit). |
| Use | Using the knowledge, which may cause the information to be modified, supplemented or partially deleted. |
| Share | Sharing the data with other users, whether as a copy or by moving the data from one location to another. |
| Archive | Archiving the data when it is temporarily not needed. |
| Destroy | Destroying the data when it is no longer needed. |

## **Practices**

|  |  |
| --- | --- |
| **Concept** | **Definition** |
| Classification | Businesses recognize that information has value and others might steal their advantage if the information is not kept confidential, so they classify it. |
| Labeling | Security labels are part of implementing controls to protect classified information. It is reasonable to want a simple way of assigning a level of sensitivity to a data asset, such that the higher the level, the greater the presumed harm to the organization, and thus the greater security protection the data asset requires. |
| Retention | Information and data should be kept only for as long as it is beneficial, no more and no less. |
| Destruction | Data that might be left on media after deleting is known as remanence and may be a significant security concern. |

**Logging and Monitoring Security Events**

**Ingress monitoring** refers to surveillance and assessment of all inbound communications traffic and access attempts. **Some tools include**:

Firewalls Gateways

Remote Authentication Servers IDS/IPS Tools

SIEM solutions

Anti-malware solutions

**Egress monitoring** is used to regulate data leaving the organization’s IT environment. The term currently used in conjunction with this effort is data loss prevention (DLP) or data leak protection. The **DLP solution should be deployed so that it can inspect** all forms of data leaving the organization, including:

Email

Copy to portable media File transfer protocol (FTP)

Posting to web pages/websites Applications/application programming interfaces (APIs)

# **Encryption & Cryptography**

**Encryption** protects our personal and business transactions; digitally signed software updates verify their creator’s or supplier’s claim to **authenticity**.

**Cryptography** is used to protect information by keeping its meaning or content secret and making it unintelligible to someone who does not have a way to decrypt (unlock) that protected information.

Let associate the security principles to this concepts:

**Encryption:** Authenticity

**Cryptography:** Confidentiality and Integrity

## **Symmetric Encryption & Assymetric**

|  |  |  |  |
| --- | --- | --- | --- |
| **Cryptography Type** | **Definition** | **Simple real example** | **Use Cases** |
| Symmetric Encryption | A type of encryption in which the same key is used for both encrypting | A lock that uses the same key to lock and unlock a door. | Encrypting bulk data (backups, hard drives, portable media), Encrypting messages traversing communications channels (IPsec, TLS), Streaming large-scale, time- |

|  |  |  |  |
| --- | --- | --- | --- |
| **Cryptography Type** | **Definition** | **Simple real example** | **Use Cases** |
|  | and decrypting the data. |  | sensitive data (audio/video materials, gaming, etc.) |
| Asymmetric Encryption | A type of encryption that uses a distinct pair of keys, one public and one private, for encrypting and decrypting the data. | A mailbox in which anyone can put a letter (public key) in it, but only the  owner of the mailbox can open (using their private key) and read the letters that have been left there. | VPNs, Certificates SSL/TLS, SFTP. |

**Configuration Management**

Is a process and discipline used to ensure that the only changes made to a system are those that have been authorized and validated.

Identification: Baseline identification of a system and all its components, interfaces and documentation.

Baseline: A security baseline is a minimum level of protection that can be used as a reference point. Baselines provide a way to ensure that updates to technology and architectures are subjected to the minimum understood and acceptable level of security requirements. A set of security controls or system settings used to ensure uniformity of configuration throughout the IT environment.

Change Control: An update process for requesting changes to a baseline, by means of making changes to one or more components in that baseline. A review and approval process for all changes. This includes updates and patches.

Verification and Audit: A regression and validation process, which may involve testing and analysis, to verify that nothing in the system was broken by a newly applied set of changes. An audit process can validate that the currently in-use baseline matches the sum total of its initial baseline plus all approved changes applied in sequence.

**Terminologies and key concepts**

|  |  |
| --- | --- |
| **Term** | **Description** |
| Application Server | A computer responsible for hosting applications to user workstations. |
| Asymmetric Encryption | An algorithm that uses one key to encrypt and a different key to decrypt the input plaintext. |
| Checksum | A digit representing the sum of the correct digits in a piece of stored or transmitted digital data, against which later comparisons can be made to detect errors in the data. |
| Ciphertext | The altered form of a plaintext message so it is unreadable for anyone except the intended recipients. In other words, it has been turned into a secret. |
| Classification | Identifies the degree of harm to the organization, its stakeholders or others that might result if an information asset is divulged to an unauthorized person, process or organization. |
| Configuration management | A process and discipline used to ensure that the only changes made to a system are those that have been authorized and validated. |
| Cryptanalyst | One who performs cryptanalysis which is the study of mathematical techniques for attempting to defeat cryptographic techniques and/or information systems security. |
| Cryptography | The study or applications of methods to secure or protect the meaning and content of messages, files, or other information, usually by disguise, obscuration, or other transformations of that content and meaning. |
| Data Loss Prevention (DLP) | System capabilities designed to detect and prevent the unauthorized use and transmission of information. |
| Decryption | The reverse process from encryption. |
| Degaussing | A technique of erasing data on disk or tape (including video tapes) that, when performed properly, ensures that there is insufficient magnetic remanence to reconstruct data. |
| Digital Signature | The result of a cryptographic transformation of data which, when properly implemented, provides the services of origin authentication, data integrity, and signer non-repudiation. |

|  |  |
| --- | --- |
| **Term** | **Description** |
| Egress Monitoring | Monitoring of outgoing network traffic. |
| Encryption | The process and act of converting the message from its plaintext to ciphertext. |
| Encryption System | The total set of algorithms, processes, hardware, software, and procedures that taken together provide an encryption and decryption capability. |
| Hardening | A reference to the process of applying secure configurations (to reduce the attack surface) and locking down various hardware, communications systems, and software, including operating system, web server, application server, application, etc. |
| Hash Function | An algorithm that computes a numerical value (called the hash value) on a data file or electronic message that is used to represent that file or message and depends on the entire contents of the file or message. |
| Hashing | The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data. |
| Information Sharing | The requirements for information sharing by an IT system with one or more other IT systems or applications, for information sharing to support multiple internal or external organizations, missions, or public programs. |
| Ingress Monitoring | Monitoring of incoming network traffic. |
| Message Digest | A digital signature that uniquely identifies data and has the property such that changing a single bit in the data will cause a completely different message digest to be generated. |
| Operating System | The software "master control application" that runs the computer. It is the first program loaded when the computer is turned on |
| Patch | A software component that, when installed, directly modifies files or device settings related to a different software component without changing the version number or release details for the related software component. |
| Patch Management | The systematic notification, identification, deployment, installation and verification of operating system and application software code revisions. |
| Plaintext | A message or data in its natural format and in readable form; extremely vulnerable from a confidentiality perspective. |
| Records | The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve |

|  |  |
| --- | --- |
| **Term** | **Description** |
|  | as a basis for verifying that the organization and the information system are performing as intended. |
| Records Retention | A practice based on the records life cycle, according to which records are retained as long as necessary, and then are destroyed after the appropriate time interval has elapsed. |
| Remanence | Residual information remaining on storage media after clearing. |
| Request for change (RFC) | The first stage of change management, wherein a change in procedure or product is sought by a stakeholder. |
| Security Governance | The entirety of the policies, roles, and processes the organization uses to make security decisions in an organization. |
| Social engineering | Tactics to infiltrate systems via email, phone, text, or social media, often impersonating a person or agency in authority or offering a gift. A low-tech method would be simply following someone into a secure building. |
| Symmetric encryption | An algorithm that uses the same key in both the encryption and the decryption processes. |
| Web Server | A computer that provides World Wide Web (WWW) services on the Internet. |
| Whaling Attack | Phishing attacks that attempt to trick highly placed officials or private individuals with sizable assets into authorizing large fund wire transfers to previously unknown entities. |