Data Classification and Handling Standards

Ryan Coon

CYB-690

Dr. Kimberly Ford

October 1, 2025

**Information Ownership**

"Information ownership" signifies the ethical and legal right to control and oversee information created or possessed by an individual, group, or organization. Effective information management hinges on proper handling, labeling, and categorization, tailored to the sensitivity, criticality, and confidentiality of the data. This involves establishing clear responsibilities for the privacy, availability, and integrity of information assets, such as customer data, financial records, and trade secrets.

To ensure data security, organizations must implement vulnerability mapping and management, which involves identifying and addressing potential security threats and weaknesses through measures like patching and configuration adjustments. Robust configuration and patch management are vital for maintaining system security and regulatory compliance. Access to data must be strictly controlled based on its sensitivity and confidentiality, with specific handling rules established for each classification level. Information ownership policies should clearly define roles and responsibilities, encompassing information classification, handling, and labeling practices.

**Vulnerability Mapping, Management, and Tracking**

Vulnerability management solutions provide a framework for addressing security flaws. When a straightforward patch isn't the optimal solution, security teams, system owners, and administrators must determine the best course of action. Remediation can range from deploying readily available software patches to the more complex task of rebuilding an organization's physical server infrastructure.

To enhance the Business Continuity Plan (BCP) for an ERP system, a three-level categorization system requires an amendment. This policy should encompass vulnerability mapping, management, and tracking, along with the necessary user access controls. Vulnerability mapping is crucial for identifying weaknesses within an information system, often aided by risk assessments that pinpoint potential threats and vulnerabilities. Once identified, vulnerabilities must be managed and tracked, a process that includes mitigating and reducing their impact. This can be achieved by implementing security measures that limit the potential for exploitation. Maintaining a detailed record of vulnerabilities and their resolution is essential for ongoing security.

**Significance of Configuration and Patch Management**

Configuration management is the practice of ensuring that a system's hardware, software, and associated documentation remain current and consistent. This approach helps prevent issues like software bugs, compatibility problems, and configuration drift. Establishing secure configuration settings is a complex task that requires specialized knowledge and expertise. However, simply setting up a secure configuration isn't enough; ongoing maintenance is crucial to preserve its security attributes. This helps prevent the gradual erosion of security due to changes, new vulnerabilities, or software updates.

To effectively manage all devices, operating systems, and applications within an environment, a centralized solution is essential. This solution provides a comprehensive view of all endpoints and the capability to deploy and update standard configurations across the entire environment. Patch management involves identifying, acquiring, and installing software patches on a system, which is vital for system maintenance and security. Effective patch management enables the identification of necessary patches, assessment of their applicability, and verification of their successful deployment and execution. By implementing all essential patches, the likelihood of system failures and security breaches is significantly reduced.

**Communicating the Assigned Classification**

Classification 1 :

Access to Top Secret Material

Access to Top Secret data is strictly limited to individuals with the appropriate security clearance. This sensitive information must be stored in a secure environment, such as a locked file cabinet or safe. Unauthorized modification of Top Secret data is strictly prohibited; only specifically authorized personnel may make changes, and all modifications must be meticulously tracked and recorded. Regular backups of Top Secret data are required, and these backups must also be stored securely. Printing of Top Secret data is permitted only for authorized individuals, and all printed copies must be immediately destroyed after use.

Classification 2:

Secret Access

Access to Secret-classified material is restricted to individuals who possess the necessary security clearance. This information must be stored securely, such as in a locked file cabinet or safe. Modifications to Secret information are permitted only by specifically authorized personnel, and all changes must be documented and tracked. Regular backups of Secret information are required and must be stored in a secure location. Printing of Secret information is limited to authorized individuals, and all printed copies must be immediately destroyed after use.

Classification 3:

Confidential Access

Access to Confidential information is limited to individuals with the required clearance level. This data must be stored securely, such as in a locked file cabinet or safe. Only authorized personnel may modify Confidential data, and all changes must be tracked and recorded. Regular backups of Confidential data are required and must be stored in a secure location. Printing of Confidential information is restricted to authorized personnel only, and all printed copies must be immediately destroyed after use.

Classification 4:

Only for Use in Official Capabilities Access

Access to data designated "For Official Use Only" (FOUO) is restricted to personnel with the appropriate clearance. This information must be stored securely, such as in a locked file cabinet or safe. Only authorized personnel are permitted to modify FOUO data, and all modifications must be tracked and recorded. Regular backups of FOUO data must be maintained in a secure location. Printing of FOUO data is limited to authorized personnel, and all printed copies must be marked with the "For Official Use Only" disclaimer and immediately destroyed after use.

**Handling Standards**

The ERP system employs three data classifications to manage information security, Public Data, Sensitive Data, and Confidential Data.

Public Data - This data is openly accessible to all system users and does not require specific security measures.

Sensitive Data - This data requires careful handling and is accessible only to authorized users. Access to sensitive data must be monitored and restricted as needed.

Confidential Data - This data demands the highest level of care and is accessible only to authorized users. Access to confidential data must be tightly controlled and closely monitored.

References:

Heimdal Security. (2020, August 25). *Patch Management Policy: A Practical Guide*. Heimdal Security Blog. https://heimdalsecurity.com/blog/patch-management-policy/

Microsoft. (2025). *What is Vulnerability Management? | Microsoft Security*. Www.microsoft.com. https://www.microsoft.com/en-us/security/business/security-101/what-is-vulnerability-management