

Data and asset classification

Protecting an organization's business operations and assets from security threats, risks, and vulnerabilities is important. You previously learned what it means to have a security mindset. That mindset can help you identify and reduce security risks and potential incidents.

In this reading, you will learn about key data classification types and the difference between the low-level and high-level assets of an organization.

Classifying for safety

Security professionals classify data types to help them properly protect an organization from cyber attacks that negatively impact business operations. Here is a review of the most common data types:

- **Public data**
- **Private data**
- **Sensitive data**
- **Confidential data**

Public data

This data classification does not need extra security protections. **Public data** is already accessible to the public and poses a minimal risk to the organization if viewed or shared by others. Although this data is open to the public, it still needs to be protected from security attacks. Examples of public data include press releases, job descriptions, and marketing materials.

Private data

This data classification type has a higher security level. **Private data** is information that should be kept from the public. If an individual gains unauthorized access to private data, that event has the potential to pose a serious risk to an organization.

Examples of private data can include company email addresses, employee identification numbers, and an organization's research data.

Sensitive data

This information must be protected from everyone who does not have authorized access. Unauthorized access to sensitive data can cause significant damage to an organization's finances and reputation.

Sensitive data includes personally identifiable information (PII), sensitive personally identifiable information (SPII), and protected health information (PHI). Examples of these types of sensitive data are banking account numbers, usernames and passwords, social security numbers (which U.S. citizens use to report their wages to the government), passwords, passport numbers, and medical information.

Confidential data

This data classification type is important for an organization's ongoing business operations.

Confidential data often has limits on the number of people who have access to it. Access to confidential data sometimes involves the signing of non-disclosure agreements (NDAs)— legal contracts that bind two or more parties to protect information—to further protect the confidentiality of the data.

Examples of confidential data include proprietary information such as trade secrets, financial records, and sensitive government data.

Asset classification

Asset classification means labeling assets based on sensitivity and importance to an organization. The classification of an organization's assets ranges from low- to high-level.

Public data is a low-level asset. It is readily available to the public and will not have a negative impact on an organization if compromised. Sensitive data and confidential data are high-level assets. They can have a significantly negative impact on an organization if leaked publicly. That negative impact can lead to the loss of a company's competitive edge, reputation, and customer trust. A company's website address is an example of a low-level asset. An internal email from that company discussing trade secrets is an example of a high-level asset.

Key takeaways

Every company has their own data classification policy that identifies what type of data is in each category. It will be important to your success as a security professional to familiarize yourself with that policy. Understanding different data and asset classification types is important. It helps you prioritize what data needs to be protected most. It also helps you recognize what assets need higher levels of security and what assets need minimal security.