Data Security and Privacy - Key Concepts

Table of Contents

Introduction **2**

Key points in this document **2**

Data security **3**

Privacy **3**

Confidentiality, integrity, availability – The CIA security triad **4**

Confidentiality *4*

Integrity *5*

Availability *5*

Authenticity, accountability, and auditability 6

INTRODUCTION

This document introduces key concepts to help you understand privacy and security risks and introduce you to important practices in creating privacy and security-aware organizations.

KEY POINTS IN THIS DOCUMENT

- IT security as a field encompasses the protection of data that is being transmitted, stored, and processed by computers.
- Data management planning must consider the protection of data from unauthorized access, alteration, and loss of quality, as well as ensuring the availability of the data to authorized individuals when required.
- Common failure points in a system are compromised credentials; weak or stolen passwords; weak network access control; poor or missing encryption; system misconfiguration; weak data storage, access, and transport policies; and data destruction.
- Privacy is about being able to create and manage boundaries to protect an individual and their personal information.
- An organization should act in accordance with individuals' understanding, consent, and expectations for how their data will be used.
- Individuals should understand why data is being collected and give their informed consent to any collection, storage, and usage, ideally at the time of collection.
- Three fundamental principles of information security are confidentiality, integrity, and availability. A government should create recovery plans that contain directives on how to deal with a loss of confidentiality, integrity, and/or, availability
    - **Confidentiality** means preventing unauthorized disclosure of data.
    - **Integrity** means preventing unauthorized or erroneous modification of data.
    - **Availability** means ensuring that data is available to authorized users when they need it.

DATA SECURITY

IT security as a field encompasses the protection of data that is being transmitted, stored, and processed by computers. Data is a valuable asset that needs protection both while at rest in a system and while in transit through a computer network.

Key concept: An organization should actively protect the data they have collected.

Data security tends to focus on limiting and controlling access to data to prevent unauthorized access. However, you should also consider how users and systems will be able to properly transport and store data.

Data management planning must consider the protection of data from unauthorized access, alteration, and loss of quality, as well as ensuring the availability of the data to authorized individuals when required. Auditing and logging procedures are a critical step in ensuring that the appropriate security measures are in place and functioning correctly.

While detailed security training in each of these areas is beyond the scope of this toolkit, areas of risk to be addressed in your data management plan include:

- your network - how your workstations and servers are connected to each other and the internet;
- your servers, web hosts, and the actual data storage infrastructure;
- your workstations - the computers on which data is accessed and work is done;
- removable data storage devices, such as USB storage devices;
- physical storage, such as filing cabinets or storage rooms;
- document and data destruction areas;
- user training, competence, and awareness;
- third-party service providers - both those providing online services, and those providing data processing, analysis, or storage capacity;
- monitoring of the systems for suspicious activity.

Common failure points in a system are compromised credentials; weak or stolen passwords; weak network access control; poor or missing encryption; system misconfiguration; weak data storage, access, and transport policies; and data destruction. To secure both physical assets (computers, storage devices, hard-copy documents) and digital assets (data), proper measures need to be implemented in a data management system.

PRIVACY

Privacy is about being able to create and manage boundaries to protect an individual and their personal information. A privacy-aware system aims to prevent that information from being used in a way that the individual would not permit. Privacy establishes boundaries to limit how an individual's personal information is treated throughout the data lifecycle (i.e., how it can be accessed, used, stored, and transmitted).

Key concept: An organization should act in accordance with individuals' understanding, consent, and expectations for how their data will be used.

When a government is implementing a data management system, privacy considerations should include:

- Legal jurisdictional requirements for data gathering, storage, and use. For a more in depth look at legal requirements around privacy, refer to the Legislation & the Duty of Privacy Protection section of the Toolkit.
- Understanding and use of the appropriate security tools.

- Minimizing access to private information by granting staff access only to the minimum data necessary to complete their duties.
- Internal privacy culture and education - aim to create organization-wide privacy awareness by:
    - Providing ongoing privacy education for existing staff and during the onboarding process for new hires. This training should include:
        - What data needs to be protected
        - How data can be lost
        - How data will be properly organized and labelled
        - Clear protocols on storing, sharing, and transporting data
        - How data will be archived and backed up
        - How data will be properly destroyed
    - Verifying staff's understanding of good data practices, organizational expectations, and policies with respect to their access to private data.
    - Promoting a culture where individuals understand the value and risks of data and are comfortable reporting concerns, mistakes, or risks of data integrity or privacy, without fear of retribution.
- Communication and consent - informed consent should be given by an individual for the collection, storage, usage, and sharing of any data they provide, with a complete understanding of the purposes for which the data is intended to be used. They must also be provided information on how to access and review their personal information, how long the information will be retained, and whether it will be kept permanently or eventually destroyed. This information must be communicated in a clear and concise way, to ensure the individual understands what they are consenting to.

Key concept: Individuals should understand why data is being collected and give their informed consent to any collection, storage, and usage, ideally at the time of collection.

The decision to collect and store information about individuals comes with tremendous responsibility. A violation of privacy can lead to irreparable harm to both the individual and the government's reputation. Additionally, data stewards have a duty to ensure that information is presented and used accurately so that it cannot be misconstrued or interpreted in a way that was not intended.

CONFIDENTIALITY, INTEGRITY, AVAILABILITY – THE CIA SECURITY TRIAD

CIA is an acronym that embodies the three fundamental principles of information security that form the cornerstone of an organization's security infrastructure (no relation to the United States intelligence agency): confidentiality, integrity, and availability.

A government should create recovery plans that contain directives on how to deal with a loss of confidentiality, integrity, and/or, availability. Directives should include the steps to take to prevent further losses and minimize the impacts of the incident.

Confidentiality

Confidentiality means preventing unauthorized disclosure of data. Data confidentiality focuses on assuring that private or confidential data is not disclosed or made available to those who are not permitted to access the information.

A loss of confidentiality can result from poor security measures or data leaks by personnel. Confidentiality can be violated both intentionally through direct attacks on the system or unintentionally by way of human error, inadequate security controls, or user knowledge gaps.

- An example of poor security measures would be creating data backups by copying unencrypted data files to a removable USB drive and removing the drive from the job site.
- An example of a data leak would be staff providing data to a 3rd party without first confirming if they are authorized to access the information.

Measures to ensure confidentiality will need to be part of your data management plan, including:

- Implementing strong access controls and authentication measures
- Data encryption policies for storage, processing, and transit
- User education through security awareness training
- Remote wiping of lost assets

Integrity

Integrity means preventing unauthorized or erroneous modification of data. It focuses on ensuring that the data can be trusted; is correct, authentic, and reliable; and that the data has not been corrupted or modified in ways that it shouldn't be. Examples of a loss in data integrity include:

- Errors and omissions in data from authorized users, which can negatively affect the analysis.
- A malicious attack on the system where an actor is attempting to modify, delete or corrupt information.

Integrity includes both data integrity and system integrity. Data integrity means assuring that when data and programs are modified, any changes are done in a controlled, specified, and authorized way, and that these changes can be documented and tracked. System Integrity means ensuring that the system performs unimpeded when processing data as intended, and there is no deliberate or inadvertent unauthorized modification of data. In data management, it is critical to be able to detect integrity issues and determine how the data has been compromised.

Your data management plan should include measures to ensure integrity such as:

- Implementing industry standard and tested encryption algorithms.
- Utilizing digital signatures and digital certifications to establish trust relationships.
- Utilizing an intrusion detection system to detect access events.
- Auditing and logging system access by authorized and unauthorized users.
- Version control systems.

Availability

Availability means ensuring that data is available to authorized users when they need it. A well-functioning data management system ensures that not only are the data and resources available when an authorized user needs to access it, but the systems are available and respond in a prompt fashion. Availability can be impacted inadvertently by authorized users or intentionally by a malicious actor. Availability can also be impacted by external factors such as power failures, natural disasters, or system failures. Examples of situations that can lead to a loss of availability include:

- An authorized user unknowingly disconnects a data resource from the network, making it inaccessible to other users who need the information.

- An external denial of service attack on a public web server that prevents the system from responding in a timely fashion to actual legitimate data requests.
- A power failure due to a storm event that causes network servers to shut down.

Your data management plan should include measures to maintain data availability, such as:

- Fault tolerance and redundancy for servers, networks, and services.
- Denial of service countermeasures.
- Power infrastructure and natural disaster risk assessment.
- System patching and upgrades.
- System and data backups.

Authenticity, accountability, and auditability

A key challenge with allowing user access to a system is **authenticity -** determining if a user is who they say they are, and if their need to access the system or data is legitimate. This starts at the point when a user is requesting initial access. The level of verification needs to be proportional to the type of request being made (i.e., requests for access to larger data sets or more sensitive data should have a higher level of verification). Your government should have documented processes for authenticating access requests. When an individual or organization requests new access, these processes provide guidance for verifying their identity and their need for data access, which will form the initial part of the trust relationship between the user and the data management system.

The concept of authenticity links strongly with authentication (see the document "Data Security and Privacy – Access and Use).

When users access data or perform actions within the system, their actions and access need to be traceable. This provides **accountability** for users of the system and for the organization, as it demonstrates that the organization is monitoring whether authorized users are following policies and procedures when accessing data. Systems need to be able to keep logs of activities so that forensic analysis can be conducted in the event of a security breach.

Coupled with this is the concept of **auditability**. Auditability refers to the ability to verify that your systems, hardware, and network are all functioning correctly, and that any actions taken by authorized users can be tracked.

Developing accountability and auditability standards will also help to detect system faults or malfunctions, and intrusion attempts against the system. Your data management plan should include what actions will be logged and how they will be monitored and controlled.