DATA GOVERNANCE AND
MANAGEMENT TOOLKIT

January, 2021
Version 1

Data Security and Privacy - Components to Data Management Plans

Table of Contents

INTRODUCTION

Your government's data management plan needs to consider the protection of data as a three part ongoing data security cycle of **prevention, detection,** and **response**.

When developing a data management plan, traditionally the focus has been on preventing unwanted access and putting safeguards in place to protect the data. However, users (authorized and unauthorized) can find their way around security safeguards, and systems still fall victim to data loss and unwanted access. This is partially due to a lack of monitoring and communication when data protection measures fail. In many cases, an organization may not even know if something has been compromised or accessed until well after the breach has occurred.

A comprehensive data protection strategy includes not just prevention of unwanted access or data loss, but also strategies for ongoing monitoring and detection of issues and having response strategies in place that can be acted upon when an issue arises.

KEY POINTS IN THIS DOCUMENT

- Your government's data management plan needs to consider the protection of data as a three part ongoing data security cycle of prevention, detection, and response.
    - The goal with prevention is to develop access control policies and procedures that will limit access to and within the entire data system. Your data management plan should include policies about types of user groups, what resources users can access, and how they will be permitted access.
    - The goal with detection is to develop policies and procedures around monitoring for authorized and unauthorized access attempts. Your data management plan should include policies and plans detailing what resources will be managed and how, as well as an audit review plan which details when logs will be reviewed, who will have access to them, log retention time, and log destruction policies.
    - The goal with response is to develop policies and procedures that will guide the organization in responding to incidents identified through detection. The data management plan should outline the types of responses needed, specific actions required, and how stakeholders will be notified.
- Your data management plan should address the following security and privacy considerations: encryption, authentication, user access, data storage, data transport, and data destruction.

PREVENTION

The goal with **prevention** is to develop access control policies and procedures that will limit access to and within the entire data system, including both digital access and physical access. **This should include policies about types of user groups, what resources users can access, and how they will be permitted access.** It also includes physical security of both digital and hardcopy assets, such as how servers are physically protected from unwanted access as well as how resources are protected from unexpected physical damage (such as from fire or flooding). Consider also how the data system is protected digitally from unwanted access or attacks with firewalls, how data will be protected when it is "at rest" on the system, and how it will be protected when being transported (both over the network and physically) with industry standard encryption algorithms. Security awareness training should be conducted on an annual basis and forms a key component of the data management plan (see the section on "Security and Privacy Awareness Training" on the "Data Security and Privacy" page of the Toolkit for more information).

DETECTION

The goal with **detection** is to develop policies and procedures that will identify what assets and actions will be monitored using access and audit logs. **System and data accesses need to be logged and reviewed for both authorized access and for unwanted access attempts.** This includes using an Intrusion Detection System (IDS) to monitor external access. The IDS is designed to detect unwanted access attempts to the network and log them for auditing and forensic analysis. Detection policies also need to be developed for physical assets, such as monitoring access to server locations and to secure physical document storage.

Key components of an effective data management plan include policies and plans detailing what resources will be managed and how, as well as an audit review plan which details when logs will be reviewed, who will have access to them, log retention time, and log destruction policies.

RESPONSE

The goal with **response** is to develop policies and procedures that will guide the organization in responding to incidents identified through detection. **The data management plan should outline the types of responses needed, specific actions required, and how stakeholders will be notified**. Types of responses include how to respond to data theft, hardware failure, physical damage, external threats, unauthorized system access, etc. It is critical to identify individuals who will be part of an incident response team for managing the response to different types of incidents. Further response could involve computer forensics to find additional details about the failure and to document how the system was compromised, how it was detected, and the status of the response.

INCORPORATING THE SECURITY CYCLE INTO THE DATA MANAGEMENT PLAN

Prevention, detection, and response form part of an ongoing cycle. The organization's initial planning outlines how prevention will be put in place. This is followed by detection monitoring. When a failure occurs, response to the failure will be executed. As part of the response, an analysis of why the failure occurred, how it was accomplished, and what was lost (and the impact to the organization) must be conducted. This analysis will be used to update the prevention plan to ensure that a similar failure does not impact your government in the future. Detection and response planning also need to be updated to reflect the changes.

These operations should be cyclical and ongoing. It is a challenge in security to be 100% secure, as the threat landscape is constantly changing and new methods of attack are developed. Using this approach, your government will be able to adapt to changes. This includes reviewing and auditing your data protection strategy on an ongoing basis, to ensure that it is operational and functional and continues to meet your government's data management needs. Failure to plan and review can cripple an organization and lead to undetected failures, loss of data, and lack of operability for an organization.

Table 1 below presents key areas that require focus to maintain data privacy and security in a system.

TABLE 1. CRITICAL SECURITY AND PRIVACY CONSIDERATIONS IN DATA MANAGEMENT PLANS.

Concept	Focus
Encryption	The goal of encryption is to control unwanted access to data. Data is protected using a "lock and key" mechanism. Once encrypted, data is transformed to a form that is not understandable. Only an authorized user will have the encryption key required to unlock the data to make it usable. In addition to securing data from access, encryption can also limit unwanted modification of data. Different strengths and types of encryption can be used and need to be considered when designing a data management strategy (see the downloadable document "Data Security and Privacy – Access and Use").
Authentication	Used to determine the identity of a user attempting to gain access to a system or resource. Measures such as a username and password or other authenticator are used to verify identity. It is critical to develop strong password policies (see the downloadable document "Data Security and Privacy – Access and Use").
User access	Used to identify and control what resources authenticated users can access. The data management strategy should identify user access roles (see the downloadable document "Data Security and Privacy – Access and Use").
Data storage	When data is stored, the appropriate data protection measures need to be put in place. These measures define how privacy will be maintained and outline where data will be stored. This applies to both electronic and physical data such as paper records and digital assets (e.g, data on removable devices). The data management strategy should include policies regarding the storage of data (see the downloadable documents "Data Archiving" and "Data Storage").
Data transport	Protocols and procedures for ensuring that security and privacy of data is maintained while data is in transit. Data transport protocols should include guidelines for protecting data while it is being transported across a network as well as protocols regarding the transport of data on removable devices such as USB drives, and movement of physical records.

	Data transport also focuses on the transmission of information via email. Email transmissions are inherently insecure and susceptible to being intercepted. The data management strategy should include policies on how data will be protected during transport (see the downloadable document "Data Security and Privacy – Access and Use").
Data destruction	Protocols and procedures for ensuring that security and privacy are maintained during the destruction of data. For physical records, this requires monitoring and tracking of documents destroyed using secure shredding. For digital assets, this involves the proper deletion of data, including any back-ups or duplicate data sets. It also includes the "aging out" of obsolete data, hardware, and storage media, i.e., ensuring that old computers and storage devices are properly erased and destroyed in a secure fashion. When data is destroyed, it is critical to maintain a record of the destruction so that if in the future the data is being requested, there is an audit path indicating the proper removal of data from the system (see the downloadable document "Data Archiving").