Cybersecurity Policy Templates

Data Inventory Management Policy

(Last Updated April 2025)

Purpose

Our Data Inventory Policy aims to establish a comprehensive framework for identifying, classifying, and managing the data assets within our organization. This policy aims to provide clear guidelines and procedures for documenting the types, locations, and sensitivity levels of our data and defining ownership and accountability. This policy seeks to enhance data governance, protect sensitive information, and ensure compliance with privacy regulations and data protection requirements by implementing effective data inventory practices. Through regular data audits, mapping exercises, and classification standards, we strive to improve data visibility, enable effective data protection measures, and minimize the risk of unauthorized access or data breaches. By prioritizing data inventory management, we enhance our overall cybersecurity posture, reduce data-related risks, and maintain the trust and confidence of our stakeholders.

Scope

The Data Inventory Policy applies to all our organization's employees, contractors, and stakeholders and encompasses the systematic identification, classification, and management of all data assets within our IT infrastructure. This policy covers all types of data, including sensitive, personal, confidential, and regulated information. It sets forth guidelines for data discovery, classification, and mapping to understand data assets' location, sensitivity, and ownership. The policy defines procedures for maintaining an accurate and up-to-date data inventory, including retention periods, sharing agreements, and disposal practices. It also outlines the responsibilities of individuals involved in data inventory processes, including data owners, IT administrators, and data stewards. Compliance with this policy is mandatory for all individuals within the organization, and any deviations or exceptions require approval from the designated authority responsible for data inventory and cybersecurity governance.

Safeguards

To achieve the organization's overall mission, and the purpose of this cybersecurity policy, the organization shall:

DTA-01	Maintain a data inventory management system to track data managed by the organization.
DTA-02	Ensure the organization's data inventory management system maintains an Inventory of data managed by the organization and under its control.
DTA-03	Ensure the organization's data inventory management system maintains an Inventory of data managed by the organization and under the control of third parties.
DTA-04	Ensure the organization's data inventory management system maintains documented definitions of categories of data managed by the organization.
DTA-05	Ensure the organization's data inventory management system defines data owners for all data managed by the organization.
DTA-06	Ensure the organization's data inventory management system tracks the necessity of the data managed by the organization when the organization's data owners approve it.
DTA-07	Ensure the organization's data inventory management system tracks the business purpose of all data managed by the organization.
DTA-08	Ensure the organization's data inventory management system tracks data that should be masked in information systems.
DTA-09	Ensure the organization's data inventory management system tracks the classification, criticality, and sensitivity of all data managed by the organization.
DTA-10	Ensure the organization's data inventory management system documents the location of all data managed during the processing lifecycle.

DTA-11	Maintain a system to automatically inventory and classify items managed by the organization (whether onsite or located at a third party).
DTA-12	Ensure that the organization's data inventory system automatically discovers data managed by the organization (whether onsite or at a third party).
DTA-13	Ensure that the organization's data inventory system automatically classifies and labels data managed by the organization (whether onsite or located at a third party).
DTA-14	Ensure that the organization's data inventory system automatically discovers when its private data is located in publicly available locations.
DTA-15	Ensure that the organization's data inventory system is integrated with the organization's asset inventory system.
DTA-16	Ensure that the organization's data inventory system logs and alerts events related to the data managed by the organization (such as access, changes, and deletions).
DTA-17	Ensure that the organization's data inventory system logs and alerts events related to the system configuration files managed by the organization (such as access, changes, and deletions).
DTA-18	Define a process the organization shall use to define data retention periods for different types of data managed by the organization.
DTA-19	Define a process the organization shall use to archive data managed by the organization whenever possible.

Policy Sanctions

Non-compliance with this policy may result in disciplinary action in line with our corporation's human resources procedures. Consequences may range from mandatory refresher training and written warnings to temporary suspension of remote access privileges and, in severe cases, termination of employment or contractual obligations. Individuals could be subject to legal consequences under applicable laws if violations involve illegal activities. These sanctions emphasize the critical importance of cybersecurity, the individual's role in protecting our digital assets, and the potential risks associated with policy violations. Enforcement will be consistent and impartial, with the severity of the action corresponding directly to the seriousness of the breach.