odga OFFICE OF DATA GOVERNANCE AND ANALYTICS

Data Security Policy Sample

Purpose

The purpose of this Data Security Policy is to outline the principles and procedures for ensuring the security of data within [Agency]. This policy aims to protect the confidentiality, integrity, and availability of data, and to comply with applicable laws, regulations, and standards, specifically VITA Standard Sec 530.

Scope

This policy applies to all employees, contractors, and third-party agents who handle, manage, or use data owned by or entrusted to [Agency].

Definitions

Term	Definition
Data	Any information that is stored electronically or in physical form.
Confidential Data	Data that must be protected due to privacy, legal, or regulatory requirements.
PII	Personal information means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted: • Social security number • Driver's license number or state identification card number issued in lieu of a driver's license number • Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts • Passport number • Military identification number Medical information means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:

Term	Definition
	• Any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional • An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records *As per Information Security Standard ITRM Standard SEC530-01.0*
Data Owner	The person or entity responsible for the overall data governance of a dataset, typically a senior leader within the organization.
Data Steward	An individual responsible for managing a dataset and ensuring its quality and metadata accuracy.
Data User	Any individual who interacts with data for analysis, reporting, or operational purposes.
Data Custodian	IT personnel responsible for the technical environment and security where data is stored, processed, and transmitted.
ISO	Information Security Officer is responsible for developing and managing the agency’s information security program.
Obfuscation	The process of making data difficult to understand or interpret without changing its format or usefulness for specific purposes.
Masking	Replacing sensitive data with realistic but fake data while maintaining the data's format and structure.
Tokenization	Substituting sensitive data elements with non-sensitive equivalents called tokens, which retain the essential information without compromising security.
Encryption	Converting data into a coded form that can only be read by authorized parties who have the decryption key.

Roles and Responsibilities

Role	Responsibility
Data Steward	• Ensure data accuracy, completeness, and consistency. • Monitor data usage and compliance with policies and regulations. • Maintain metadata and data documentation. • Facilitate data quality assessments and improvements. • Manage and update the business glossary to ensure it reflects current terminology and definitions.
Data Owner	• Define data governance policies and procedures. • Approve access to data and determine data classification levels.

Role	Responsibility
	• Ensure compliance with legal, regulatory, and organizational requirements.
Data User	• Use data responsibly and ethically. • Protect sensitive data and report any breaches or suspicious activities. • Adhere to data usage guidelines and security policies.
Data Custodians	• Implement and maintain technical safeguards to protect data. • Ensure data backup, recovery, and disaster recovery procedures are in place. • Manage access controls and monitor data system security.
ISO	• Develop and implement security policies and procedures to protect data. • Conduct regular risk assessments and implement strategies to mitigate identified risks. • Ensure compliance with relevant laws, regulations, and standards. • Manage incident response and recovery efforts. • Promote security awareness and training programs. • Collaborate with data stewards and custodians to ensure data security measures are in place and effective. • Report on the organization's security posture to senior management and relevant stakeholders.

Policy

All [AGENCY] employees must adhere to the following data security policies when creating, managing, or using data.

> "It is the policy of the COV (§2.2-603.F) that each Agency Head is responsible for securing the electronic data that is held by the agency and shall comply with the requirements of §2.2-2009. In addition, the Director of every department is responsible for the security of the agency's electronic information, and for establishing and maintaining an agency information security program compliant with this policy and meets all of the requirements established by COV ITRM Security Standards." - ITRM Policy SEC519-01

Access Control

- The Data Custodian must work with the ISO and Data Stewards to implement the principle of least privilege, granting data access only to those who need it for their job functions.

- The Data Custodian must work with the ISO to use strong authentication and authorization mechanisms to control access to data.

Data Protection

- The Data Custodian must work with the ISO and Data Stewards to encrypt confidential and restricted data at rest and in transit.
- The Data Custodian must use approved encryption algorithms and key management practices as described in Sec 530.
- File level encryption must be established for all cloud and on-premises databases with sensitive data to provide encryption at rest (e.g. SQL Server's Total Database Encryption - TDE).
- Any tables that contain PII must be encrypted and columns with Protected PII obfuscated through encryption or masking (e.g., Always Encrypted or Dynamic Data Masking).
- All encryption keys must be stored in secure storage such as Azure Key Vaults or a Hardware Security Module (HSM).
- Network traffic between agencies should use end to end encryption such as MACSec and traffic must be separated from other Agencies. Network traffic that does not need to be securely transmitted may use the public internet.

Network Security

- The VITA team and ISO must implement firewalls, intrusion detection/prevention systems, and other network security controls to protect data.
- The VITA team and ISO must regularly update and patch network devices and systems to address vulnerabilities.

Endpoint Security and Access

- The VITA team and ISO must use antivirus software, endpoint detection and response (EDR) solutions, and other endpoint security measures.
- The VITA team and ISO must ensure endpoints are regularly updated and patched.
- All new accounts, permission changes, and group memberships must be logged and require management or Data Steward approval.
- Database logging must be enabled to include user database login sessions and the logs must be kept for at least 90 days or as required by Sec 530.

Data Backup and Recovery

- The Data Custodian must regularly back up critical data and ensure backups are stored securely.

- The Data Custodian must test data recovery procedures periodically to ensure data can be restored in the event of a loss.

Incident Response

- The ISO must ensure an incident response plan is developed and maintained.
- The ISO must train employees on incident reporting procedures.
- The ISO must conduct regular incident response drills and reviews.

Monitoring and Auditing

- The VITA security team must implement logging and monitoring to detect and respond to date-related security incidents.
- The VITA security team, in conjunction with the ISO, must conduct regular data security audits and assessments to ensure compliance with policies and identify areas for improvement.

Compliance

- The Data Steward must ensure ongoing compliance with relevant laws, regulations, and standards.
- The Data Owner and ISO must conduct regular audits to ensure compliance with data security policies.
- The Data Steward and the ISO must monitor data access and usage for unauthorized activities.
- The Data Steward and the ISO must report and respond to data breaches in accordance with incident response procedures.
- Compliance with this policy is mandatory for all departments and individuals involved in dataset management.
- Non-compliance may result in corrective actions as determined by the [Agency] leadership.

Training and Support

- The Data Steward must provide training for all employees on data security policies and best practices.
- The Data Steward must promote a culture of data security awareness throughout the organization.

Policy Review

This Policy will be reviewed and updated annually from the approval date, or more frequently if appropriate. Any staff members who wish to make any comments about the Policy may forward their suggestions to [AGENCY Contact].

Related Policies

[AGENCY] Policies, Standards and Procedures
Data Governance Policy
Data Quality Policy
Metadata Management Policy
Data Stewardship Policy
Data Retention Policy
Data Privacy Policy

The [Agency] adheres to all Commonwealth Information Technology Resource Management (ITRM) policies and standards for security and architecture Policies, Standards & Guidelines | Virginia IT Agency.

VITA Related Policies
IT Information Security Policy - SEC519
Information Security Standard - SEC530
IT Risk Management Standard - SEC520

Version History

Version Number	Revision Date	Description of Change	Author
V1	6/10/2024	Initial Draft	Chris Burroughs