DATA INTEGRITY AND ENCRYPTION POLICY

City of Helena/Lewis and Clark County IT&S

Information Security Policy Manual

Version Control

Policy Code:	ITSEC009	Approved By:	IT&S Steering Committee 3/24/2021 IT Board 4/8/2021
Owner:	IT&S	Effective Date:	4/8/2021

Revision History

Date	Version	Created by	Description of change

Table of Contents

1. Purpose and Scope

This document outlines the standards and methods for ensuring the confidentiality and integrity of sensitive and proprietary information. In addition, this policy will provide guidelines for acceptable, proven methods of encryption.

This document applies to all IT&S employees and technology resources.

2. Roles and Responsibilities

Roles and Responsibilities	
IT&S Director	• Sponsor and administer the Integrity and Encryption Policy. • Assign responsibilities for implementing the Integrity and Encryption Policy requirements.
Security Officer	• Document policy for data integrity and validation of controls. • Implement specific systems for logging and monitoring all system activity. • Ensure appropriate training for personnel in installing, monitoring, and maintaining systems for data integrity and validation of controls.
System Operators or End Users	• Operate in adherence with the Information Security Policy. • Report any suspected incidents or policy violations to the Security Officer.

3. Data Integrity and Encryption

This section describes the mechanisms that corroborate that sensitive data has not been altered or destroyed in an unauthorized manner.

3.3.Transmission Security

File Transfers

All transmissions of sensitive data will be limited to what is absolutely necessary. All sensitive data that is transmitted through a public network (such as the Internet) must be encrypted or transmitted through an encrypted tunnel. Any servers used for the secure transmission of files must require a login with a secure password (see *Acceptable Use Policy*). Required methods of secure file transmission include, but are not limited to:

- SSL/TLS
- VPN
- SSH and SCP
- SFTP and FTPS

Email

Emails, both internal and external, that contain sensitive information must be encrypted during transit, as well as at rest on the email server. Emails must be sent through the secure email application, Microsoft O365. Whenever possible, City of Helena/Lewis and Clark IT&S (IT&S) will send information using both at rest and transmission encryption.

3.4.Data at Rest

Access control systems will be implemented to ensure that all access to sensitive information is properly authorized. Systems must also be implemented for logging network activity such as:

- File access, modification, creation, and deletion
- Database create, update, and delete operations

Each user of IT&S information systems must have an account for their exclusive use. These user accounts will be used to audit changes and access to sensitive information. Refer to the *Audit Controls Policy* and *Access Control Policy* for more information.

IT&S will use encryption to secure sensitive data at rest. Sensitive data at rest must be stored in encrypted files, volumes, databases, servers, workstations, etc. As an additional safeguard, IT&S will implement full disk encryption whenever possible.

3.5.Violation of Integrity

The Security Officer is responsible for the storage of sensitive information and must implement methods of verifying data integrity. All suspected violations of data integrity or compromises of data will be handled in accordance with the *Incident Response Policy*.

4. Policy Maintenance and Management

The Owner of this document must evaluate and perform any necessary updates to this document at least once per year. The owner may delegate tasks related to this policy as appropriate.

- Security Officer will adhere to the continual validation, review, and updating of this policy.
- When evaluating this policy, the number of gaps or incidents related to data integrity and encryption may be considered.
- Upon formal review of this policy, Security Officer must perform any necessary revisions and communicate policy changes throughout the organization as necessary.

5. References

NIST Cybersecurity Framework References

- PR.DS – Data Security
- PR.PT – Protective Technology
- PR.AC – Access Control

Policy References

- Access Authorization and Control Policy
- Audit Controls Policy
- Incident Response Policy