INFORMATION SECURITY POLICY

City of Helena/Lewis and Clark County IT&S

Information Security Policy Manual

Version Control

Policy Code:	ITSEC002	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

The purpose of this document is to establish City of Helena/Lewis and Clark County IT&S (IT&S) continuous commitment to the security of sensitive and proprietary information, and the management risks associated with this information throughout business operations.

This document will also provide policy and procedure for risk analysis, risk management, assigned security responsibility, and evaluation of compliance with applicable laws, regulations, and policies.

The following policy is applicable to all members of IT&S staff, vendors, and business partners.

2. Goals

IT&S' enterprise cybersecurity program is organized to preserve and improve the confidentiality, integrity, and availability of IT&S' information, systems, and relevant technologies. Goals of the cybersecurity program include the prevention and identification of security incidents, as well as reducing the damages resulting from security incidents. Additionally, the program facilitates the compliance of information security policies and procedures with internal policies, laws and regulations, and established contractual agreements.

3. Commitment of Management

IT&S' senior management supports and fully commits to the implementation of the cybersecurity program. Management recognizes the importance of information security and understands implementing a risk-based, proactive, and adaptive information security management program is the most effective way to combat threats to the confidentiality, availability, and integrity of information.

4. Industry Standards and Frameworks

The Security Officer or delegate is committed to ensuring the cybersecurity program aligns with industry standards, security best practices, and the requirements of applicable laws and regulations. To support a well-structured and effective, risk-based cybersecurity program, the Security Officer or delegate has adopted the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

5. Roles and Responsibilities

The following sections define the roles and responsibilities associated with the enterprise cybersecurity program. Security tasks in this policy and IT&S' other security policies may be delegated.

5.1. Director, Information Technology

The IT&S Director is responsible for the following:

- Approving proposed goals for information security controls
- Approving policies and procedures
- Approving the implementation of controls
- Oversee risk management activities, including the acceptance of residual risk and providing guidance on risk mitigation
- Ensuring the cybersecurity program is implemented in accordance with this policy
- Reviewing the existing goals and overall performance of the cybersecurity program
- Coordinating audit functions as well as necessary policy and procedure revisions
- Ensuring that all employees and relevant third parties are familiar with the cybersecurity policies

- Producing documentation of information security activities as needed

5.2. Information Technology Security Committee

The Information Technology Security Committee (ITSC) will oversee the information security function and its activities. A Security committee is an important factor in ensuring that the information security function supports organizational missions and objectives.

The ITSC consists of the following:

- Lewis and Clark County Department Representatives
- IT&S Director

The ITSC is responsible for the following:

- Supporting development and implementation of an enterprise wide information security management program
- Reviewing security initiatives as well as proposed, expected, and recent changes to the cybersecurity program.
- Reviewing the long- and short-range plans of IT operations to ensure that they are in alignment with corporate objectives
- Reviewing reported security incidents or vulnerabilities and develop action plans to meet cybersecurity program goals and review the quality and effectiveness of incident and vulnerability management
- Review adequacy of resources and allocation of resources in terms of time, personnel and equipment

The ITSC will meet quarterly, as well as whenever significant change in technology, change of business objectives, changes in the business environment, etc. occurs.

Due to the diverse components of information security, the ITSC may require participation from individuals outside of the core ITSC. These individuals make up the “Extended” Team, which includes, but is not limited to:

- Legal Counsel
- Human Resources
- Operations Manager

The Extended Team is responsible for the following:

- Maintaining involvement in meetings pertaining to information security as requested by the ISSC
- Reviewing team responsibilities and communication requirements
- Discussing current extended team practices and receiving feedback

5.3. Security Officer

The Security Officer’s responsibilities, include, but are not limited to:

- Leading the development, enforcement, and monitoring of the enterprise cybersecurity program and risk management strategies, and the supporting security policies, procedures, and standards.
- Implementation and maintenance of internal security policies and procedures, including annual reviews and approval of policies.

- Maintaining awareness of security best practices, trending threats, and common information security frameworks.
- Determining any necessary changes or enhancements to the security program in response to new technology and threat information, as well as changes to applicable laws and regulations.
- Evaluating and communicating potential security risks related to acquisition of new software, third-party services, and other major changes in technology or the business environment.
- Leading development and implementation of the enterprise cybersecurity training program. This includes ensuring all users receive appropriate security training and understand relevant security policies and procedures.
- Leading and overseeing cybersecurity risk management activities. This includes identification of risks, determining residual risks, and providing guidance on risk mitigation and risk treatment activities.
- Reporting the outcome of risk assessment and risk management activities to the IT&S Director, including status of risks, proposed risk treatment plans, and ensuring accepted risks are documented.
- Providing direction to the IT Department on the appropriate implementation of security policies and the necessary administrative, physical, and technical security controls to effectively mitigate risks.
- Evaluating, approving, and documenting exceptions to security policies and procedures.
- Scheduling periodic evaluations of the enterprise security program and technical controls, including annual technical and non-technical assessments.
- Scheduling and overseeing internal audit functions related to the security program, including audit planning, audit criteria, and reporting.
- Developing and managing response and recovery strategies related to cybersecurity incidents, disasters or emergencies, and non-compliance with internal security policies and procedures.
- Scheduling and coordinating regular testing of business continuity, disaster recovery, and incident response plans.
- Providing oversight and direction for security incident investigations. This includes reviewing the outcome of investigations related to breaches and security incidents, and determining recommendations and action items for avoiding reoccurrence.
- Developing and communicating security initiatives, objectives, budgets, and goals related the enterprise cybersecurity program for approval by ITSC.
- Providing regular reports to the ITSC describing the overall status of the information security program, including areas of strength, deficiencies, and status of risks.

5.4. IT Board

The IT Board is responsible for the following:

- Adopting IT policies and procedures
- Approving cybersecurity projects and recommending funding to the City and County Commissioners.

5.5. Internal Audit

IT&S will assign internal audit tasks to personnel that possess an appropriate level of independence and objectivity over the business process or set of controls to be audited. For example, if an audit is being performed to evaluate access termination processes, the individual(s) who is responsible for carrying out user de-registration and access terminations should not be involved in any of the audit activities related to evaluating this process. As a general rule, individuals should not be checking (or auditing) their own work. Individuals assigned with internal audits tasks are responsible for evaluating cybersecurity policies, procedures, and controls in accordance with an agreed upon audit plan to ensure they are sufficiently implemented and operating effectively to support company missions and objectives. All findings must be documented in an audit report and reported to relevant management and the ITSC.

5.6. Information and System Owners

All information owners and system owners are responsible for maintaining compliance with the cybersecurity policies as well as meeting the cybersecurity program goals.

5.7. Users

Users are responsible for familiarizing themselves with the relevant cybersecurity policies, adhering to the cybersecurity policies, and attending recurring security awareness training.

6. Contact with Special Interest Groups

IT&S is committed to ensuring that its employees maintain knowledge regarding the most current developments in the field. To support this goal, IT&S staff are members of or subscribe to various special interest groups regarding IT security and other support forums. Examples of such groups include [MTLGIT, MS-ISAC, SANS, US-CERT, and vendor update] distribution lists.

7. Policies and Procedures

The Security Officer will ensure appropriate and effective security controls are implemented in compliance with relevant laws, regulations, and policies based upon IT&S' current environment when analyzed in reference to the likely contribution toward protecting sensitive data. In deciding which security measures to use, the Security Officer will take into account IT&S size, complexity, and capabilities. In addition, its technical infrastructure, hardware, software, security capabilities, and costs of implementation will also be considered, as well as the likelihood and impact of potential risks to sensitive data.

If implementing a safeguard required by law, regulations, and/or policies is determined to be unfeasible or unnecessary, the Security Officer will:

- Document why it would not be reasonable and appropriate to implement the safeguard, or security control.
- Implement an equivalent, alternative security measure if reasonable and appropriate.

7.1. Policy and Procedure Review

The IT Security Committee will review the policy, make needed updates, and communicate changes as needed. Reviews and updates may occur more frequently in the case of changes in regulations, laws, or standards; significant changes in technology or system configurations; changes in the business environment; or changes in the organizational structure. Each policy includes a revision history where reviews and updates must be documented.

8. Evaluation

To support a culture of continuous improvement, IT&S cybersecurity program will undergo periodic evaluations and testing. The scope of evaluation and testing will include relevant policies, procedures, and security controls related to the cybersecurity program and risk management activities.

The Security Officer is responsible for coordinating a technical and non-technical evaluation at least annually, in order to determine the effectiveness and maturity of IT&S security program. Evaluations are also intended to identify compliance with applicable laws, regulations, and policies. Evaluations may be done internally, or by a third party.

8.1. Non-Technical Evaluation

Non-technical evaluations will include interviews with appropriate staff members, inspections of the physical environment, and review and analysis of IT&S policies and procedures. Other evaluations may include sampling and analysis of key performance indicators such as total number of security incidents, system outages, outstanding high-risks, and more.

8.2. Technical Evaluation

Technical Evaluations may include vulnerability assessments, external penetration testing, internal penetration testing, analysis, and manual verification of configurations and existing technical controls. These evaluations must be completed at least once every year.

8.3. Reporting

The results from the non-technical and technical evaluations will be documented, with all findings and recommendations for improving IT&S security program and compliance standing included. This report will be reviewed by the IT Director for decision-making, prioritization, and resource allocation, and incorporated in risk management activities.

9. Compliance with Legal and Contractual Requirements

IT&S identifies all relevant legal, regulatory, and contractual requirements related to information security, including on-going operational activities needed to meet these requirements. The Security Officer is responsible for periodically engaging legal counsel to identify and review applicable requirements and inform relevant internal stakeholders of such requirements to ensure controls or processes are implemented to support compliance.

The Security Officer will maintain an inventory of the applicable legal and contractual requirements and the controls in place to meet the requirements. The inventory will be used to support monitoring of implemented controls and included in relevant internal audit tasks and/or information security assessments.

10. Non-Compliance Management

In the event of non-compliance with security policies and requirements, the following actions are required:

- Identify the causes of the non-compliance
- Evaluate the need for actions to achieve compliance
- Implement appropriate corrective action
- Review the corrective action taken to verify its effectiveness and identify any deficiencies or weaknesses

These actions will be taken by the IT Director in conjunction with the user, user's supervisor, and Human Resources input as needed. The results of reviews and corrective actions are recorded and maintained to support reporting if needed for independent reviews.

11. Exception Process

Exceptions to this policy and other IT&S policies and procedures must be approved by the IT Director, providing that:

a) An assessment of the risk resulting from the non-compliance is performed;

b) Compensating controls are defined and implemented if applicable;

c) Residual risks are formally accepted by the Asset Owner as per the adopted Risk Management Framework.

Approved exceptions will be maintained by the Security Officer for reference and for annual review.

12. Information Risk Analysis and Management

In order to ensure that appropriate safeguards are implemented for the protection of sensitive data, risk analysis and risk management activities will be performed. Information Risk Analysis and Management are a continuous process of strategic assessment, mitigation, and acceptance of risks in relation to sensitive data.

The Security Officer will be responsible for coordinating Risk Analysis and Management activities. A Risk Analysis will be conducted on an annual basis, or more frequently in the case of significant organizational changes, significant changes in technology, changes to business objectives, changes in business environment, etc. Risk analysis may be conducted internally by IT&S staff or by a third party. A detailed risk assessment methodology is available in the Appendix of this policy. However, it should be noted that various methodologies may be applied for conducting IT&S risk assessments.

12.1. Asset, Threat, and Vulnerability Identification

The risk assessment processes will identify all instances of sensitive data and inventory all IT&S systems and devices that are used to collect, store, process, or transmit sensitive data. This includes both internally and externally hosted IT&S systems.

Additionally, the risk assessment process will identify all threats and vulnerabilities associated with the use of sensitive information within IT&S business processes and the core systems determined to contain sensitive data. Please refer to the *Asset Management* Policy for additional requirements surrounding the inventorying of classified systems and data types. The results of this identification phase may be documented in a Risk Analysis Spreadsheet.

12.2. Impacts and Likelihood

Once the threats and vulnerabilities to sensitive data have been identified, the potential impact and likelihood must be assessed should such security risks occur. Risk impacts and likelihoods may be assessed in reference to the Risk Assessment Methodology available in the policy appendix.

12.3. Risk Remediation

For each risk, a plan for remediation must be selected. Potential remediation options are available in the appendix of this policy. Risk levels should be used to prioritize remediation activities.

The IT Director must approve the risk remediation plan. The Security Officer is responsible for implementing the risk remediation plan. The Security Officer may delegate responsibilities as necessary to complete implementation.

All identified risks and the planned or completed risk treatment actions will be documented within a Risk Registry or other tracking mechanism to support visibility and tracking of risks. The Security Officer is responsible for maintaining the Risk Registry.

12.4. Risk Assessment Reporting

The results of risk assessments and risk treatments must be documented in a Risk Assessment Report. The Security Officer is responsible for documenting the results of annual risk assessments.

The Risk Assessment report will be communicated and reviewed by the ITSC and relevant management to ensure risk treatment plans are appropriate and to approve acceptance of risks as needed.

12.5. Risk Management Review

All identified risks and progress of risk mitigation activities will be reviewed on an annual basis. The Security Officer] will be responsible for reviewing and reporting the progress of risk mitigation activities.

13. 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.

- The Security Officer will adhere to the continual validation, review, and updating of this policy.
- When evaluating this policy, the number of errors in risk assessments and treatments as well as any discrepancies in risk management responsibilities must be considered.
- Upon formal review of this policy, the Security Officer must perform any necessary revisions and proceed to properly communicate policy changes throughout the organization as necessary.

14. References

NIST Cybersecurity Framework

- ID.GV – Governance
- PR.AC – Access Control
- PR.AT – Awareness and Training
- PR.IP – Information Protection Processes and Procedures
- PR.PT – Protective Technology
- PR.DS – Data Security
- PR.DS – Security Continuous Monitoring

Policy References

- Acceptable Use Policy
- Access Control and Authorization Policy
- Asset Management Policy
- Audit Controls Policy
- Business Continuity Policy
- Incident Response Policy
- Integrity and Encryption Policy
- Physical Security Policy
- Vendor Management Policy

15. Appendix A: Risk Assessment Methodology

The risk assessment process consists of identifying information assets, and vulnerabilities and threats associated with each asset. Vulnerabilities and threats are then assessed for likelihood and impact of an exploit, taking into account existing security controls (technical or non-technical) that may mitigate or lower the overall likelihood or impact of exploit. In accordance with NIST SP 800-30, *Guide for Conducting Risk Assessments*, risk level is calculated as a combination of likelihood and impact. **FISASCORE (Information Security Risk Assessment) may also be utilized to discover and valuate risks.**

This appendix describes the steps of the risk assessment process and is intended to allow IT&S to conduct future risk internal assessments, or to characterize risk levels for newly identified vulnerabilities or threats. It should be noted that various methodologies may be applied for conducting IT&S risk assessments.

15.1. Asset Identification

The risk assessment processes must identify all instances of sensitive data and inventory all IT&S systems and devices, including hardware and software, that are used to collect, store, process, or transmit sensitive data. This includes both internally and externally hosted IT&S systems. Refer to the *Asset Management Policy* for additional requirements surrounding the inventorying and management of organizational assets.

15.2. Threats and Vulnerabilities

The risk assessment process should identify all threats and vulnerabilities associated with the use of sensitive data within IT&S business processes and the core systems determined to contain sensitive data. Each asset may be associated with multiple threats, and each threat may be associated with multiple vulnerabilities. Risk assessments will consider both intentional and unintentional threats. Examples of unintentional threats are human error due to lack of training, or data corruption due to lack of a change management process.

Typical threats to consider include:

- Data modification / destruction / corruption
- Damage or destruction of assets
- Data loss / information disclosure
- Theft of assets or data
- Malware
- Unauthorized access to systems, data, or facilities
- Unauthorized changes to systems or data
- Policy breach
- Regulatory breach
- Environmental / natural threats such as fire, water damage, temperature control, natural disaster

15.3. Likelihood Assessment

Upon the assessment of risk impacts, the likelihood of such risks occurring must be determined. When assigning values likelihood, existing security controls must be considered. The following scale may be used to characterize the likelihood of an exploit, while considering existing security controls (technical and non-technical) that may reduce the likelihood of an exploit.

Very High	No security controls provide protection. Incidents have an extremely high chance of occurring in the future.

High	Existing security controls provide insignificant levels of protection. Incidents have a high chance of occurring in the future.
Moderate	Existing security controls provide limited protection. Incidents have a fair chance of occurring in the future.
Low	Existing security controls provide considerable protection. Incidents have a low chance of occurring in the future.
Very Low	Existing security controls provide extensive levels of protection. No new incidents are expected in the future.

15.4. Impact Assessment

The following scale may be used to assess the potential impact to IT&S in the case of an exploit due to a specific threat or vulnerability. Impact can take the form of injury or loss of life, financial loss, regulatory penalties, reputational damage, or disruption to mission activities. Areas for potential impact depend on an organization's mission and priorities.

Very High	▪ The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational assets, individuals, or other organizations.
High	▪ The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals or other organizations.
Moderate	▪ The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals or other organizations.
Low	▪ The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals or other organizations.
Very Low	▪ The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals or other organizations.

15.5. Risk Matrix

Risk level is calculated as a combination of likelihood and impact. Risk levels should be used to support prioritization of remediation activities. In many cases, risk cannot be eliminated, but can be reduced by implementing security measures that reduce either the likelihood or impact of an exploit.

		Impact				
		Very Low	Low	Moderate	High	Very High
Likelihood	Very High	Very Low	Low	Moderate	High	Very High
	High	Very Low	Low	Moderate	High	Very High
	Moderate	Very Low	Low	Moderate	Moderate	High
	Low	Very Low	Low	Low	Low	Moderate
	Very Low	Very Low	Very Low	Very Low	Low	Low

15.6. Risk Treatment

Risk levels should be used to prioritize remediation activities. The treatment of unacceptable risks may include the following actions:

1. Avoiding the risk through the elimination of corresponding business activities
2. Mitigating the risks through the implementation of security controls or additional standard controls
3. Transferring the risks responsibility to an external party (i.e., insurance)
4. Accepting the risks in avoidance of unnecessary treatment costs

As mitigation techniques are selected for risk treatments, the impact and likelihood of such risks must be reassessed to establish residual risks.