VENDOR MANAGEMENT POLICY

City of Helena/Lewis and Clark County IT&S

Information Security Policy Manual

Version Control

Policy Code:	ITSEC003	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 policy is to establish the requirements and procedures for ensuring the confidentiality, integrity, and availability of data and technology resources that are accessed, stored, or transmitted by third parties on behalf of City of Helena/Lewis and Clark County IT&S (IT&S). This policy provides a framework for vetting, managing, and terminating agreements with third party vendors, and ensuring third parties operate in compliance with applicable laws, regulations and policies.

Vendors may include anyone who provides service on behalf of, or provides services to IT&S, which involves access to sensitive and proprietary data and/or technology resources.

This document applies to all IT&S employees, partners, vendors, contractors, and technology resources.

2. Roles and Responsibilities

Roles and Responsibilities	
Security Officer	• Document all contracts and security agreements with third parties which clearly define the roles and responsibilities of any/all vendors and IT&S with regards to access management, data handling, and other security functions. • Review and update all contracts, Service Level Agreements (SLA), Non-disclosure agreements, and other vendor agreements at least annually. • Provide access to vendor contracts and agreements to IT&S staff as necessary. • Monitor and report any violations associated with a particular vendor.

3. Vendor Selection

The proper selection of vendors requires analyzing and evaluating the personnel, services, security programs, and operational procedures of the outsourced entity. IT&S will follow current procurement rules, whether it's selecting a vendor via limited solicitation, RFP, RFQ, etc. As necessary, IT&S will exercise due diligence prior to formally selecting a vendor, as means for confirming the validity and security of third party operations. This includes identifying and assessing the risks related to third parties in accordance with the Risk Management section outlined within the Information Security Policy. The IT Director is responsible for ensuring that the appropriate measures have been taken for fully assessing the risk related to third party service providers, taking into consideration the information, technologies, and operational procedures involved.

Due diligence may include requesting and reviewing both public and confidential information such as references, financial records, risk assessments, technical assessment reports, compliance reports, etc. Additionally, IT&S may perform or request background checks for third party service providers.

4. Vendor Agreements

Prior to accessing, receiving, or transmitting any sensitive or proprietary data and/or technology resources, IT&S will form an agreement with the third party vendor. This agreement must outline

terms of the transmissions between IT&S and the vendor, as well as the security requirement for the data and technologies that will be created, accessed, and stored by the vendor.

The third party must sign the agreement prior to performing any services or receiving access to IT&S technologies and information assets. Non-disclosure agreements must also be signed by vendors prior to receiving access to sensitive or proprietary data and/or systems. All vendor agreements will be reviewed at least annually and updated as necessary.

4.1 Agreement Requirements

The IT&S Director is responsible for developing the vendor contract and ensuring the contract includes the appropriate clauses related to security, delivery of service, and management of IT&S information and technology assets.

The contract between County IT&S and the vendor will require, at minimum, that the vendor:

- Implement effective security controls to prevent the unauthorized use or disclosure of IT&S information and technology assets. The vendor must implement administrative, physical, and technical safeguards that appropriately protect the confidentiality, integrity, and availability of the information and technology assets that it creates, maintains, or transmits on behalf of IT&S.

- Report to IT&S, in a timely manner, any unauthorized access, use, modification, or disclosure of sensitive data and systems, and any security incidents that the vendor becomes aware of. Vendors must agree to cooperate with IT&S investigation and comply with requests for evidence and information to support the investigation. Further, the vendor must mitigate any harmful effects to sensitive data and systems in response to such security incidents.

- Notify IT&S of employee separations, transfers, or other situations that necessitate modification or termination of the employee's access to IT&S data, facilities, or systems.

- Comply with the requested termination of the agreement(s) by destroying all sensitive and proprietary data stored or retained by the vendor, and return all IT&S assets. The vendor must also maintain confidentiality upon the termination of the agreement(s).

The contract between IT&S and the vendor requires approval from the Board of County Commissioners.

4.2 Vendor Compliance

All vendors entrusted with regulated data types must be compliant with all applicable legal and regulatory requirements. IT&S may request such vendors to provide proof of compliance prior to entering into a service agreement and annually therein after. Should IT&S become aware of a vendor's failure to comply with the applicable laws and regulation, the agreement may be terminated immediately.

4.3 Agreement Review and Revision

The IT&S Director will periodically review all vendor agreements at least annually, or when there are significant changes in operational procedures and technologies. The agreements will be updated to reflect changes to applicable laws and regulations, or other relevant documents. All agreements require approval from the Board of County Commissioners.

Vendors may be subject to annual audits in order to confirm their fulfillment of agreed upon services and security requirements, as well as their compliance with applicable laws and regulations. The IT&S Director will be responsible for coordinating and documenting the results of such audits.

4.4 Incident Response

A security incident involving IT&S data and systems should be handled in accordance with the Incident Response and Disaster Recovery policies. This includes contacting vendors as necessary. Vendors may be subject to audit and review following a security incident.

4.5 Insurance

Vendors must be compliant with insurance limits and requirements. Limits and requirements are subject to change.

CONTRACTOR agrees to maintain general liability insurance from an insurance carrier licensed to do business in the State of Montana in the amount of seven hundred and fifty thousand dollars ($750,000.00). for each occurrence (minimum) and one million five hundred thousand dollars ($1,500,000.00) aggregate. CONTRACTOR also agrees to maintain workers compensation insurance from an insurance carrier licensed to do business in the State of Montana. Proof of general liability and workers compensation insurance shall be provided to the ENTITY prior to commencing work under this agreement. The ENTITY must be listed as an additional insured on the general liability insurance certificate for this agreement. Insurance certificates will be attached to this agreement.

5. Termination of the Agreement

If the agreement between a vendor and IT&S must be terminated, the following steps are required:

1. IT&S must confirm that the vendor has securely and properly destroyed all data stored, transmitted, or accessed on behalf of IT&S. This also includes immediately terminating any remote or direct access to IT&S systems that has been provided to vendor, as well as promptly returning all assets to IT&S.

2. The agreement must be marked as terminated and kept for a period of 3 years before destruction.

6. Policy Maintenance and Management

The IT&S Director 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 IT&S Director will adhere to the continual validation, review, and updating of this policy.

- When evaluating the effectiveness of this policy, any violations of vendor agreements, surrounding the confidentiality, integrity, and availability of IT&S information and technology assets, will be considered.

7. References

NIST Cybersecurity Framework References

- ID.GV – Governance
- PR.AT – Awareness and Training
- PR.DS – Data Security
- PR.IP – Information Protecting Processes and Procedures
- DE.DP – Detection Processes
- RS.CO - Communications

Policy References

- Information Security Policy – Risk Management
- Incident Response Plan
- Disaster Recovery Plan