# AUDIT CONTROLS POLICY

City of Helena/Lewis and Clark County IT&S

Information Security Policy Manual

## Version Control

| | | | |
|---|---|---|---|
| Policy Code: | ITSEC006 | Approved By: | IT&S Steering Committee 3/24/2021<br>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 formally establish City of Helena/Lewis and Clark County IT&S (IT&S) internal auditing practices surrounding the monitoring and logging of activities within IT&S systems, applications, and relevant technologies that access, store, and transmit sensitive and proprietary data.

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

It is the responsibility of these users to reference this document for the monitoring and logging techniques applied to company information systems and technologies.

## 2. Roles and Responsibilities

The following table outlines roles and responsibilities as they pertain to the implementation of audit controls and review of audit logs.

| Example Roles and Responsibilities | |
|---|---|
| Security Officer | • Coordinating and overseeing the implementation of audit controls.<br>• Coordinating and overseeing the review of audit logs.<br>• Ensuring audit logs are retained in accordance with legal and regulatory requirements. |
| ROLE | • Implementing, configuring, and maintaining audit controls.<br>• Reviewing audit logs and communicating logged security incidents. |

## 3. Privacy and System Monitoring

Individuals using the IT&S network, information systems, applications, and relevant technologies should have no expectations of privacy. IT&S extends ownership over all data created or stored on company systems, including personal data such as emails and documents. In doing so, IT&S reserves the right to access, read, review, copy, and actively monitor and log all user and system activities as means of ensuring and preserving the confidentiality, integrity, and availability of sensitive information. When deemed necessary, IT&S reserves the right to disclose text or images to law enforcement agencies or other third parties without the employee's consent.

Through the authorized or unauthorized IT&S information systems, users are consenting to the monitoring and logging of all system activity.  Upon review, logged user activities may be subject to use in corrective action or disciplinary proceedings at the discretion of management.

## 4. Clock Synchronization

Uniform time representations across organizational devices are essential to the integrity and accuracy of event logs. Therefore, all relevant information systems, workstation, and additional technologies must be synchronized to the standard reference time used by IT&S. IT&S utilizes Coordinated Universal Time (UTC) as the single referenced time source within the organization.

All workstations, servers, facility cameras and access logs, network equipment, and relevant information systems shall utilize Network Time Protocol (NTP) software or other reliable timing mechanisms as the synchronized time source for ensuring log timestamps are consistent and set to Universal Time.

# 5. Audit Controls

Audit controls that facilitate monitoring and logging capabilities will be implemented and enabled across all information systems, facility cameras and access controls, and relevant technologies that access, store, or transmit sensitive information. The following sections outline the events and procedures for the logging of system activities.

## 5.1. Log Events

All system and user activity, including administrative and privileged user accounts, shall be monitored and recorded for review. Event logs may include, but are not limited to, records of the following system activities:

- **User information**: User IDs, successful/unsuccessful logins, login date/time, password changes, etc.
- **System Access**: Successful/rejected file access attempts, privilege escalation, file access/modification/deletions, etc.
- **System changes**: Software installations, changes to system configuration/group policy settings, etc.
- **System information**: System/application identifier, locations, date/time of key activities, etc.
- **General activity**: Use of applications, network activity, IP addresses, etc.
- **Facility Access**: Successful/unsuccessful access attempts, access date/time, etc.

# 6. Log Review and Retention

System event logs or audit reports must be periodically reviewed and in immediate response to security incidents and requests from management as well as law enforcement. The frequency of log reviews may be adjusted based on the type of log information or system criticality.

Log information must be retained for a minimum of at least 1 year. As necessary, retention time may be adjusted in response to business and system capacity needs as well as legislative, regulatory, and governing policy requirements.

Any suspicious activity identified through the review of audit log reports, should be investigated and reported as per the *Incident Response Policy*.

# 7. 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 detected and undetected security incidents may be considered in order to validate the effectiveness of the implemented audit controls.
- Upon formal review of this policy, Security Officer must perform any necessary revisions and proceed to properly communicate policy changes throughout the organization as necessary.

## 8. References

**NIST Cybersecurity Framework References**

- PR.PT – Protective Technology
- DE.AE – Anomalies and Events
- DE.CM – Security Continuous Monitoring
- DE.DP – Detection Processes

**Policy References**

- Incident Response Policy