ACCESS CONTROL AND AUTHORIZATION POLICY

City of Helena/Lewis and Clark County IT&S

Information Security Policy Manual

Version Control

Policy Code:	ITSEC005	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 define the rules for access and authorization to City of Helena/Lewis and Clark County IT&S (IT&S) information systems. This includes ensuring only approved individuals have access to networks (LAN, VPN, wireless), email, file servers, SQL databases, applications, or any other systems.

This document applies to all IT&S information systems.

2. Roles and Responsibilities

Roles and Responsibilities	
Security Officer	• Coordinating and overseeing reviews and updates of user accounts and related access to privileges. This includes but is not limited to account creations, modifications of access permissions, disabling of user accounts, etc. • Approving privileged IT accounts, such as Domain Administrator accounts
Human Resources Manager Hiring Manager Department Director Supervisor	• Submitting user account requests to the IT&S Department.
IT&S Team/Helpdesk	• Creating, modifying, and deleting user accounts. This includes granting, modifying, and terminating user access. • Reviewing user accounts and access permissions and disabling or deleting inactive accounts.

3. Access Prerequisites

All users requesting access to a IT&S information system must first be on-boarded by the Human Resources Department, and must sign the IT Acknowledgement Form indicating that they have read, comprehend, and will adhere to the Information Security Policy. The signed agreements are filed on an internal network drive.

4. Access Authorization and Implementation

This section outlines the different processes for new accounts, approval, submission, etc. to networks (LAN, VPN, wireless), email, file servers, databases, applications, or any other technologies. All requests must be submitted using the KACE Systems Management Appliance Ticketing System (KACE). Alternatively, a request may be submitted via email and the IT&S Team will manage a ticket in KACE.

4.1 Account Creation

New User accounts must be requested by the Department Director, Supervisor, or Human Resources using the 'New Ticket Form Process' option within the menu and selecting the respective action.
All requests must be approved by the IT Director. Once approved, the account is created, and permissions are granted by the IT&S Team. User access is granted based on the user's job description and role within IT&S. Segregation of duties is implemented to reduce information security risk.

4.2 Change Requests

Change requests for existing users must be submitted by the Department Director or Supervisor through KACE. The Director or Supervisor must select the 'New Ticket Form Process' option and then select the respective action. The form should include the reason for the access change and the additional level of access required and/or the access that should be removed. Access change requests may require additional review and approval by the IT Director.

In response to changes in job roles or other internal transfers, a user's existing access rights must be reviewed, removed, and adjusted to ensure access is limited to what is absolutely necessary for the user's job function. The Department Director or Supervisor is responsible for determining what access is needed for the new position and any access that is no longer necessary. The IT&S Team is responsible for removing permissions (via Active Directory) that are no longer necessary for the user's new job role and granting the additional access that is necessary.

4.3 Request Submission

All requests must be submitted through KACE-and will be kept as record of the user's authorization to access IT&S information systems and sensitive data.

4.4 Account Permissions

Users will only have access to the systems and data that are necessary for their job functions. All submitted requests will be reviewed to ensure that the proper access permissions are granted using the principle of least privilege.

As access permissions are granted, users are responsible for securely exercising such privileges in accordance with IT&S's Acceptable Use Policy and any additional organizational requirements.

The Department Director or Supervisor is responsible for determining the appropriate access for new users, and the IT&S Team is responsible for evaluating change requests to ensure access is appropriate for the user's new position. In cases where the change request is not typical for the position, the Windows Administrator may escalate the request to the IT Director for validation of appropriate access. Asset owners may also be consulted by the IT&S Team prior to granting access, if needed to confirm appropriate permissions.

4.5 Privileged Access

Privileged access will be restricted and monitored. Users are only granted privileged access if needed to complete their specific job responsibilities. Users will not be provided with local administrative rights unless required for their job function. The IT Director must authorize all privileged access. Privileged access is reviewed at least monthly as part of the account review process.

Privileged users, such as Domain Administrators, will only use their elevated accounts when necessary for specific tasks. Normal business operations such as email and internet use will be performed with a standard, non-privileged user account.

If shared, generic accounts are required for technical reasons, such as service accounts or system-level accounts, the IT Director will ensure these accounts are monitored and the passwords are stored in a secure, encrypted password manager. These passwords will be changed as soon as possible when a user with access leaves or changes roles. The IT Director or Windows Administrator will also securely communicate any password changes to all appropriate staff.

5. Access Termination

The following sections detail the process used to disable or delete a user account. IT&S reserves the right to revoke access rights and terminate user accounts at any time without prior notification.

5.1 Disabling a User Account

Department Directors or City/County Attorneys may request that a user account be disabled by submitting a ticket through KACE. Department Directors or City/County Attorneys will notify the IT&S Team if any planned employee separations so that access can be disabled accordingly.

The IT Director or Security Officer may also authorize immediate disabling of an account if needed to address or contain a suspected or confirmed incident. When an employee leaves the company, access must be removed immediately.

No data from these accounts will be deleted and all account information will remain in place until the IT Directory or Security Officer has approved data deletion.

5.2 Account Review and Certification

The IT Director or Security Officer will conduct quarterly account reviews of all user accounts and their permissions to ensure all access privileges are appropriate, and that inactive or unnecessary accounts are identified and disabled as needed. This applies to IT&S networks, applications, systems, remote access, etc.

The review and certification process includes:

- Validating each user/role/group has a continued need to access IT&S applications and networks.
- Validating each user/role/group has access only needed to perform the assigned duties.
- Validating access to any sensitive data is authorized and correct.
- Disabling any user who no longer needs access to IT&S applications/networks.

During quarterly account reviews, any accounts that have been inactive for at least 90 days will be disabled as necessary. The IT Director or Security Officer is responsible for coordinating the updating of access privileges as necessary and deleting accounts when needed.

5.3 Deleting a User Account

User accounts will be deleted based upon the results of the quarterly account review, or when explicitly directed by Department Directors or City/County Attorneys. When a user account is deleted, all user data for the user account may be erased.

6. Account Components

Users must be assigned a unique user ID to provide accountability when accessing systems and data. Shared accounts are prohibited, unless required by the system such as service accounts (See 4.5 Privileged Access)

6.1 User Identification

All User Accounts, when possible, will use the convention of first-initial and last name (i.e. John Doe = jdoe) for unique user identification. User IDs should not be reused, for example after an employee has been terminated the same user name should not be used when creating another user.

6.2 Password Policy

User accounts will be authenticated by using strong passwords. Any default passwords on systems or applications will be changes to a unique, strong password.

The following list contains the minimum requirements for passwords:

- 16 characters in length at minimum. Privileged accounts, such as Domain Administrators, and service account must be at least 25 characters in length.
- At Least 3 of the 4 possible character types:
  - Upper-case and lower-case letters
  - Numerical digits
  - Symbols (!#&@)
- Must be different than previous 24 passwords
- Must be changed every ninety (90) days
- Use passphrases, song lyrics, or whole sentences. Passwords must not be based on information readily known (e.g., birthdates, job titles).
- Passwords for work accounts must never be the same as passwords used for personal accounts.

Users that have been issued a separate user account to perform privileged functions (i.e. Domain Administrators) must ensure the password for their privileged account is different from their non-privileged, standard user account.

Further, passwords should not be disclosed to anyone and should not be sent electronically. Passwords should never be written down and should only be stored electronically using an approved password storage application. If a user suspects their password has been compromised, the password must be changed immediately, and the event should be reported to the IT&S Team.

Two-Factor Authentication

Two-factor authentication will be used to further support strong authentication and prevent unauthorized access to IT&S systems and applications as determined by IT Director or Security Officer. Two-factor authentication is required for the following:

- Remote access to IT&S's internal network. (i.e. VPN Access)
- Administrator accounts (I.e. Domain Admin). For instance, to perform privileged administrative functions on servers or network devices.
- Cloud platforms
- Other

The IT Director or Security Officer will determine additional instances where two-factor authentication is required and must approve the method or type of two-factor authentication prior to its implementation.

7. Account Logoff and Lock-Out

IT&S systems, applications, and any additional technologies that access, store, or transmit sensitive data will be configured to automatically logoff after a maximum of ten (15) minutes of inactivity.

Accounts for all systems must have security controls to resist brute-force attacks. Accounts will be locked after five (5) unsuccessful login attempts within two (2) minutes. The system will unlock automatically after a period no shorter than ten (10) minutes.

8. Management of User Credentials

When creating a new user account or resetting a user's password, a unique and complex temporary password will be provided, which the user must be prompted to change upon first login. Initial and temporary passwords will be generated using pseudo-random number generator algorithms. Default passwords on accounts, systems, and applications must be changed prior to deployment.

Authentication information, including passwords, security tokens or other types of credentials, must not be shared with anyone except for the user to whom they are assigned.

Before providing credentials to a user, the identity of the user must be verified. The credentials must be communicated in a secure manner, that reduces the likelihood of the credentials being intercepted by an unauthorized user. This may include:

- Issuing the credentials to the user via their encrypted company email.
- Issuing the credentials over the phone, after verifying the user's identity.
- Issuing the credentials to the user in-person.

Credentials must never be sent together with the user ID over the same communication channel. For example, a user ID and a password must never be sent in the same email.

9. Remote Access

Only employees who have been approved by the IT Director may remotely access company resources. Remote access will be provided via an authenticated and encrypted Virtual Private Network (VPN) that is configured to terminate idle sessions after 2 hours of inactivity. Remote access requires the use of strong two-factor authentication and is restricted to IT&S devices that comply with company security requirements and other internal policies.

For security reasons, the Security Officer or IT&S Team must have up-to-date information regarding all employees who have been approved for remote access to the company network, as well as any employees whose approval has been revoked or temporarily suspended. The standard termination procedures for all staff include checking for remote access permissions and revoking them.

10. Physical Access

Physical access to IT&S facilities and system is managed by the Security Officer. Upon hire, employees may be is issued a key or proximity card to permit access to and throughout IT&S facilities. If a proximity card is lost or misplaced, the card must be deactivated, and another card reissued. In the event that a key is lost or misplaced, the impacted facility and entry points may require rekeying.

Authorizing, issuing, reviewing, and terminating physical access to IT&S facilities and systems must comply with the requirements of this policy, the Physical Security Policy, and any other applicable company policies. Employees are not provided with access to any third-party data centers or hosting providers.

11. 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 IT Director or Security Officer will adhere to the continual validation, review, and updating of this policy.
- When evaluating this policy, any instances of unauthorized access as well as any discrepancies in access control responsibilities must be considered. Additionally, any sudden alterations or terminations of access rights must be acknowledged.
- Upon formal review of this policy, the IT Director or Security Officer must perform any necessary revisions and proceed to properly communicate policy changes throughout the organization as necessary.
- Revisions must be approved by the IT&S Steering Committee and IT Board.

12. References

NIST Cybersecurity Framework References

- ID.AM – Asset Management
- PR.AC – Access Control
- PR.DS – Data Security
- PR.PT – Protective Technology
- PR.IP – Information Protection Processes and Procedures

Policy References

- Acceptable Use Policy