Logical Access Policy

January 29, 2025

GTEL Advisors, LLC

6120 Berkshire Lane North
Plymouth, Minnesota 55446
Phone: 612-386-4141
1/29/2025

Table of Contents

1. Introduction

The [Agency Name] Technology Logical Access Control Policy (the "Policy") is designed to provide a framework for managing and controlling access to the agency's information systems. It outlines the principles and processes for granting, monitoring, and revoking user access to ensure the confidentiality, integrity, and availability of data and systems. This Policy ensures that access to sensitive data and systems is granted based on the principle of least privilege, and that it aligns with industry standards such as the NIST Cybersecurity Framework and the Criminal Justice Information Security (CJIS) Policy.

2. Purpose of the Policy

The purpose of this Policy is to:

- Define procedures for managing logical access to [Agency Name]'s systems and sensitive data.
- Ensure that only authorized users have access to critical agency resources, based on job responsibilities and security clearance.
- Prevent unauthorized access to sensitive information, including Criminal Justice Information (CJI).
- Establish a structured approach to monitoring, auditing, and revoking access as needed.

3. Scope

This Policy applies to all employees, contractors, and third-party vendors who require access to [Agency Name]'s information systems. It includes all systems, applications, and networks used for the processing, storage, or transmission of agency data, including systems that handle sensitive or regulated data such as CJI.

4. Governance and Compliance

4.1 NIST Cybersecurity Framework

This Policy is aligned with the NIST Cybersecurity Framework (CSF), specifically the "Protect" and "Detect" functions, which focus on managing access to critical systems and monitoring access for signs of unauthorized activity. [Agency Name] follows the NIST framework to manage cybersecurity risks and protect against unauthorized access, focusing on the following areas:

- Identify: Identify systems and data requiring protection, and define roles and responsibilities for logical access.
- Protect: Implement access control policies and technical safeguards to protect information and systems.
- Detect: Continuously monitor for unauthorized access and anomalies that could indicate a breach.

- Respond: Ensure that procedures are in place for responding to access-related security incidents.
- Recover: Implement recovery procedures for access and information systems following a security incident.

4.2 Criminal Justice Information Security Policy (CJIS)

As part of its operations, [Agency Name] may access, store, or process Criminal Justice Information (CJI), which requires compliance with the CJIS Security Policy. The CJIS Security Policy mandates strict access controls for systems that store or process CJI, including the following requirements:

- Logical access controls to restrict access to CJI to authorized personnel only.
- Authentication methods to ensure that only authorized users can access CJI.
- Continuous monitoring and auditing of access to CJI.

5. Logical Access Control Requirements

5.1 User Account Management

User accounts must be created, managed, and deactivated in accordance with the following guidelines:

- Account Creation: Accounts should only be created for individuals who require access for their job responsibilities. Access must be reviewed and authorized by the appropriate department head.
- Account Modification: Any changes in a user's role, job responsibilities, or clearance must trigger a review and modification of access privileges.
- Account Deactivation: Accounts should be deactivated immediately when an employee or contractor no longer requires access, such as upon termination, role change, or leave of absence.

5.2 Authentication and Authorization

To ensure secure access to systems, the following authentication methods will be used:

- Password Requirements: Passwords must be complex, consisting of a combination of letters, numbers, and symbols. Passwords should be at least 8 characters long and changed every 60-90 days.
- Multi-Factor Authentication (MFA): MFA is required for accessing sensitive systems, especially those containing CJI. MFA may involve a combination of something the user knows (password), something the user has (smart card or token), and something the user is (biometric data).
- Role-Based Access Control (RBAC): Access to systems and data must be granted based on the user's role within the organization. Access permissions should be the minimum necessary to perform job duties, adhering to the principle of least privilege.

5.3 Access Control Lists and Role-Based Access

Access to information and resources will be controlled using access control lists (ACLs) and role-based access (RBAC), ensuring that:

- Each user is granted access to only those resources necessary for their role.
- Specific users or groups may have different levels of access to various systems and data based on the sensitivity of the information.
- Sensitive data, including CJI, will be restricted to individuals with appropriate clearance or need-to-know access.

5.4 Access Control Enforcement

[Agency Name] will implement technical controls to enforce access restrictions, including:

- Access Control Software: Automated tools to enforce access control policies, such as directory services (e.g., Active Directory), identity management systems, and network security tools.
- Network Segmentation: Critical systems, particularly those handling sensitive data, will be isolated on secure network segments with limited access.

6. Monitoring and Logging

6.1 Access Logging

All access to sensitive systems and data, including CJI, must be logged. Access logs must include:

- User identification (e.g., username or ID).
- Time and date of access.
- Resources accessed or modified.
- Actions taken during access (e.g., login, file retrieval).

Logs should be retained for a minimum period of one year and be secured against tampering or unauthorized access.

6.2 Log Review and Analysis

Access logs must be regularly reviewed by security personnel for any signs of unauthorized access or anomalies. This includes:

- Monitoring for failed login attempts, account lockouts, and unusual access times.
- Reviewing logs for attempts to access systems or data outside of a user's assigned role.

7. Access Termination and Revocation

7.1 Access Deactivation

Access to agency systems and sensitive data must be revoked immediately upon termination of employment or contract. The following actions must be taken:

- Disable user accounts.
- Revoke access to all systems, databases, and applications.
- Ensure that any sensitive or confidential data is returned or properly disposed of.

7.2 Removal of Access for Departing Personnel

For departing personnel, the IT department will ensure that access to all physical and logical systems is revoked, including:

- Deactivation of system login credentials.
- Termination of VPN or remote access privileges.
- Collection and secure disposal of any agency-owned devices (laptops, phones, etc.).

8. Security of Remote Access

8.1 Virtual Private Network (VPN)

Remote access to [Agency Name]'s internal systems must be secured via a Virtual Private Network (VPN). All remote users must use the agency's VPN to access internal systems, ensuring encrypted communications.

8.2 Multi-Factor Authentication (MFA)

MFA is required for all remote access, providing an additional layer of security. Users will authenticate using at least two methods: a password and a one-time code generated by an MFA device or app.

9. Incident Response for Unauthorized Access

9.1 Detection and Reporting

Unauthorized access attempts or anomalies detected during log reviews should be immediately reported to the IT security team for investigation. Detection methods include:

- Automated alerts for unusual access patterns or failed login attempts.
- Employee-reported suspicious activity.

9.2 Incident Investigation

The IT security team will investigate all incidents of unauthorized access, which may include:

- Reviewing access logs.
- Conducting interviews with the involved users.
- Identifying the cause of the incident and implementing corrective actions.

10. Training and Awareness

10.1 Access Control Training

All employees, contractors, and third-party users must receive training on:

- Proper use of access controls and authentication methods.

- The importance of protecting passwords and credentials.
- Reporting suspicious access or security concerns.

10.2 Security Awareness Programs

Security awareness programs should be ongoing and regularly updated to address emerging threats, including phishing attacks and social engineering tactics that may be used to gain unauthorized access.

11. Compliance and Auditing

11.1 Regular Audits

[Agency Name] will conduct regular audits of access control systems and logs to ensure compliance with this policy and identify any weaknesses or non-compliance with established procedures.

11.2 Compliance with CJIS Security Policy

Access control practices must comply with the CJIS Security Policy, which includes additional requirements for access to CJI, such as regular audits, monitoring, and reporting.

12. Policy Violations and Enforcement

Violations of this policy, such as unauthorized access or failure to comply with access control procedures, will result in disciplinary action, including potential termination of employment or contracts. Serious violations may also lead to legal action.