Acceptable Use

January 29, 2025

GTEL Advisors, LLC

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

Table of Contents

Introduction 2

Purpose of the Policy 2

Scope 2

Governance and Compliance 2

4.1 NIST Cybersecurity Framework 2

4.2 Criminal Justice Security Compliance 3

Acceptable Use of Technology 3

5.1 General Usage Guidelines 3

5.2 Internet and Email Use 3

5.3 Social Media 4

5.4 Remote Access and Mobile Devices 4

Prohibited Uses 4

6.1 Illegal Activities 4

6.2 Harassment and Discrimination 4

6.3 Security Violations 4

6.4 Unauthorized Software and Hardware 5

Security and Data Protection 5

7.1 Access Control and Authentication 5

7.2 Data Encryption and Protection 5

7.3 Device and Network Security 5

7.4 Incident Response 5

Monitoring and Enforcement 5

8.1 Monitoring Use of Technology 5

8.2 Enforcement of Policy Violations 5

Introduction

This Technology Acceptable Use Policy (the "Policy") establishes the guidelines and responsibilities for the use of [Agency Name] technology resources. This includes all devices, software, networks, data, and communication platforms provided by the agency for business-related activities. This Policy ensures compliance with the National Institute of Standards and Technology (NIST) Cybersecurity Framework and addresses the security needs required for handling criminal justice data in accordance with federal, state, and industry regulations.

Purpose of the Policy

The purpose of this Policy is to:

- Safeguard the confidentiality, integrity, and availability of [Agency Name]'s technology resources.
- Ensure compliance with cybersecurity standards as prescribed by the NIST Cybersecurity Framework.
- Uphold security measures aligned with the handling of criminal justice data, ensuring compliance with relevant legal and regulatory requirements.
- Prevent misuse of technology resources and ensure responsible use in a way that does not compromise operational effectiveness or security.

Scope

This Policy applies to all employees, contractors, vendors, consultants, and third-party service providers who use [Agency Name] technology resources. It covers devices, software, systems, networks, internet access, email, and any other technology used in the course of conducting agency business, both within the corporate environment and remotely.

Governance and Compliance

4.1 NIST Cybersecurity Framework

[Agency Name] aligns its technology use and security protocols with the NIST Cybersecurity Framework (CSF) to manage and mitigate cybersecurity risks. This includes the five key functions outlined by NIST:

1. Identify: Develop an understanding of [Agency Name]'s technology resources and the risks associated with their use, focusing on asset management, business environment, and governance.
2. Protect: Implement safeguards, such as access controls and data protection measures, to ensure the secure use of technology.
3. Detect: Continuously monitor and detect cybersecurity events that could affect [Agency Name]'s systems.

4. Respond: Develop plans and capabilities for responding to security incidents or breaches in a timely manner.

5. Recover: Ensure recovery capabilities to restore normal operations after a cybersecurity event or breach.

4.2 Criminal Justice Security Compliance

As [Agency Name] may deal with criminal justice data or partner with organizations that do, we are committed to ensuring compliance with security regulations specific to the criminal justice field, including but not limited to:

- CJIS Security Policy: Compliance with the Criminal Justice Information Services (CJIS) Security Policy set forth by the Federal Bureau of Investigation (FBI), which governs the access, storage, and transmission of criminal justice information.
- HIPAA: Ensuring that personal and sensitive data, including medical and criminal justice information, is handled in compliance with the Health Insurance Portability and Accountability Act (HIPAA) and other relevant standards.
- State and Local Regulations: Compliance with applicable state, county, or municipal regulations concerning criminal justice information security.

All users must take extra caution when handling, storing, or transmitting criminal justice-related data to prevent unauthorized access and ensure compliance with these stringent security standards.

Acceptable Use of Technology

5.1 General Usage Guidelines

Technology resources provided by [Agency Name] should only be used for business-related purposes, such as:

- Performing job functions, including tasks that involve handling sensitive or classified data, criminal justice information, or confidential agency information.
- Participating in professional development and communication activities related to job duties.

Employees should not use agency technology for activities unrelated to their job, especially if it involves potential risks to data security, confidentiality, or agency reputation.

5.2 Internet and Email Use

Employees should:

- Use internet resources and email for work-related purposes. Personal use of these resources is permitted but should not interfere with work duties or cause excessive use of bandwidth.
- Avoid accessing unauthorized websites, including those that may pose security threats (e.g., malicious sites, illegal content, or sites with unauthorized downloads).

- Exercise caution when sending emails containing sensitive or confidential information, especially with respect to criminal justice data. Proper encryption and secure transmission protocols must be used.

5.3 Social Media

Employees should adhere to the following guidelines when using social media:

- Do not post or share information that could harm the reputation of [Agency Name] or compromise the security of criminal justice data or any other proprietary agency information.
- Employees should avoid using agency systems or networks to manage personal social media accounts.

Any activity that creates conflicts of interest or violates legal or ethical standards could result in disciplinary action.

5.4 Remote Access and Mobile Devices

Employees who access [Agency Name] technology resources remotely must:

- Use secure, agency-approved methods for remote access, such as Virtual Private Network (VPN) connections.
- Ensure that mobile devices (e.g., smartphones, laptops, tablets) used for business purposes are properly secured, encrypted, and protected by strong passwords.
- Report any lost or stolen devices immediately to the IT department.

Prohibited Uses

6.1 Illegal Activities

Use of agency technology resources for illegal activities, including but not limited to:

- Accessing or distributing illegal content.
- Participating in cybercrimes, identity theft, or fraud.

These actions are prohibited and may result in legal consequences.

6.2 Harassment and Discrimination

Technology resources should not be used to create, transmit, or store material that harasses, discriminates, or intimidates others, including inappropriate content based on race, gender, religion, or any other protected status.

6.3 Security Violations

Employees must not engage in activities that:

- Bypass or attempt to bypass agency security measures.
- Access unauthorized systems, applications, or data.
- Install unauthorized software or hardware that may compromise security.

6.4 Unauthorized Software and Hardware

Employees must not install unapproved software or hardware on agency systems. Only software that has been properly vetted and authorized by the IT department should be used. Unauthorized external storage devices such as USB drives should not be used without permission.

Security and Data Protection

7.1 Access Control and Authentication

All users must adhere to strict access control policies, which include:

- Using strong, unique passwords and multi-factor authentication (MFA) where applicable.
- Ensuring that access is granted based on the principle of least privilege, with users only able to access data relevant to their roles.
- Regularly reviewing and updating access privileges to ensure they align with current roles.

7.2 Data Encryption and Protection

All sensitive data, particularly criminal justice data, must be encrypted when stored and transmitted. Employees should follow agency guidelines to:

- Ensure that all sensitive or regulated data is encrypted using industry-standard encryption protocols.
- Avoid sending sensitive information via unprotected email or other unencrypted communication methods.

7.3 Device and Network Security

All devices must be secured using appropriate security measures:

- Enable firewalls, antivirus software, and anti-malware tools on all devices.
- Devices must be updated regularly to ensure protection from known vulnerabilities.

7.4 Incident Response

Employees are required to report any suspected security incidents immediately. The agency maintains an incident response plan to mitigate potential breaches and restore systems to normal operations.

Monitoring and Enforcement

8.1 Monitoring Use of Technology

[Agency Name] reserves the right to monitor all use of its technology resources to ensure compliance with this Policy. Monitoring may include tracking internet activity, email communications, and access to agency systems.

8.2 Enforcement of Policy Violations

Violations of this Policy may result in disciplinary actions, including but not limited to:

- Warnings or reprimands.
- Suspension of access to technology resources.
- Termination of employment or contracts.
- Legal action in cases of illegal activity or breach of regulations.