# Town of Gardiner

# TOWN HALL

## INFORMATION TECHNOLOGY SECURITY AND USAGE POLICY

*ISO 27001 Aligned | New York State Compliant*

# SECTION 1: POLICY OVERVIEW AND GOVERNANCE

## 1.1 Purpose and Scope

This Information Technology Security and Usage Policy establishes comprehensive requirements for the secure and appropriate use of information technology resources within Town of Gardiner Town Hall & other town-owned properties. This policy protects town assets, ensures compliance with legal obligations, and maintains the confidentiality, integrity, and availability of town information systems and data.

### Purpose:

- Establish clear security requirements for all technology users
- Protect town data and information systems from security threats
- Ensure compliance with New York State laws and regulations
- Aligning with ISO 27001 information security management standards

## 1.2 Applicability

This policy applies to all individuals who access, use, or manage town information technology resources, including:

- All town employees (full-time, part-time, seasonal, temporary)
- Elected officials and appointed board/commission members
- Contractors, consultants, and vendors with town system access
- Volunteers working on town projects

## 1.3 Municipal Context and Legal Framework

As a New York State municipality, Town of Gardiner must comply with specific state laws and regulations:

### New York State Freedom of Information Law (FOIL)

The New York Freedom of Information Law (Public Officers Law Article 6) establishes the public's right to access government records. Town employees must understand that:

- Most town records are presumptively public and subject to FOIL requests
- Email and electronic documents are 'records' under FOIL
- Personal use of town email may create public records
- Records must be retained per NY State retention schedules (consult Town Clerk)
- Deletion of records to avoid FOIL is illegal

### Other Applicable Laws

- NY General Municipal Law § 18 (Information security breach notification)
- NY Personal Privacy Protection Law (Public Officers Law § 91-99)
- CJIS Security Policy
- Federal HIPAA regulations

## 1.4 Roles and Responsibilities

Information security is a shared responsibility. Everyone who uses town technology resources has security obligations.

### All Users (Employees, Officials, Contractors)

Every individual with access to town technology resources shares responsibility for information security:

- Comply with all provisions of this policy
- Protect passwords and authentication credentials
- Use town systems only for authorized purposes
- Immediately report security incidents and suspicious activity
- Complete required security awareness training
- Lock screens when stepping away from computers

## 1.5 Compliance and Enforcement

**NO EXPECTATION OF PRIVACY:** Users have no expectation of privacy when using town technology resources. The town reserves the right to monitor, access, review, and disclose any information transmitted, received, or stored using town systems for legitimate business purposes including security protection, policy compliance, and legal obligations.

Violations of this policy may result in progressive discipline including verbal/written warning, mandatory retraining, suspension of access privileges, suspension from employment, or termination. Serious violations may result in legal action.

# SECTION 2: INFORMATION SECURITY FRAMEWORK

## 2.1 Security Objectives (CIA Triad)

### Confidentiality

Ensure that information is accessible only to authorized individuals and protected from unauthorized disclosure. Protect sensitive resident information, safeguard confidential town documents, and control access based on need-to-know principles.

### Integrity

Maintain accuracy and completeness of information and prevent unauthorized modification. Ensure records are accurate and trustworthy, prevent unauthorized changes to town data or systems.

### Availability

Ensure authorized users have timely and reliable access to information and systems when needed. Maintain operational systems for town services and minimize downtime through proper maintenance and backups.

## 2.2 Data Classification Framework

Not all information requires the same level of protection. This framework categorizes information based on sensitivity.

### CONFIDENTIAL (Highest Sensitivity)

Information that, if disclosed, would cause severe harm. Examples: Social Security numbers, bank account information, health information (HIPAA), criminal justice information (CJIS), system passwords, attorney-client communications, personnel records, security system configurations.

### INTERNAL (Moderate Sensitivity)

Information intended for internal town use only. Examples: Internal procedures, draft documents not yet released publicly, budget deliberation documents prior to adoption, IT system documentation, vendor proposals.

### PUBLIC (Low Sensitivity)

Information approved for public release or required to be public under FOIL. Examples: Published meeting minutes, public notices, adopted budgets, general town contact information.
**IMPORTANT:** When in doubt about classification, treat information as Confidential or Internal until consulting with your department head or IT Manager.

## 2.3 Public Records and FOIL Considerations

### Understanding FOIL

New York's Freedom of Information Law (FOIL) establishes a presumption of public access to government records. Most information created or received in the course of town business is a public record that may be requested under FOIL.

### Key FOIL Principles:

- Records are presumed public unless specifically exempt
- Email, text messages, and electronic documents are records
- Deleted emails may be recoverable and subject to FOIL
- Records must be retained per state retention schedules (consult Town Clerk)

**CRITICAL:** Only the Town's Records Access Officer or Town Attorney can make determinations about FOIL exemptions. Do NOT delete or withhold records based on your own assessment.

### Email Best Practices for Public Sector:

- Assume all town emails may become public—write accordingly
- Be professional and factual in all work communications
- Minimize personal use of town email to reduce FOIL exposure
- Do not delete emails to avoid FOIL—this is illegal

# SECTION 3: ACCEPTABLE USE OF TECHNOLOGY RESOURCES

## 3.1 Authorized Use

Town technology resources are provided to support town operations and enable employees and officials to perform their duties effectively.

### Limited Personal Use

Brief, occasional personal use is permitted under these conditions:

- Personal use is brief and infrequent (a few minutes at a time)
- Does not interfere with work responsibilities
- Occurs primarily during breaks or non-work time
- Complies with all other policy provisions

**REMINDER:** All use, including permitted personal use, may be monitored and is subject to FOIL. Personal communications on town systems may become public records.

## 3.2 Prohibited Activities

The following activities are strictly prohibited and may result in immediate disciplinary action up to and including termination:

### Security Violations

- Attempting to bypass, disable, or circumvent security controls
- Sharing passwords or authentication credentials with anyone
- Accessing systems, data, or accounts without proper authorization
- Installing unauthorized software or hardware
- Disabling or interfering with security software

### Misuse of Access and Data

- Accessing confidential information without business need
- Unauthorized copying or disclosure of confidential information
- Copying town data to personal devices or accounts
- Deliberate destruction or concealment of public records

### Illegal or Unethical Activities

- Any illegal activity including fraud, theft, or harassment
- Copyright infringement or downloading pirated software/media
- Cryptocurrency mining on town systems
- Political campaigning using town systems (Hatch Act violations)

### Inappropriate Content

- Accessing, storing, or distributing pornographic material
- Content that is discriminatory, harassing, or offensive

## 3.3 Email and Internet Usage

### Email Best Practices

- Use professional language and tone in all town email communications
- Remember that email may be subject to FOIL requests and become public
- Report suspicious emails (phishing attempts) immediately to IT
- Do not open attachments or click links from unknown senders

### What Never to Send via Email

Never send the following information via unencrypted email:

- Passwords or authentication credentials
- Credit card numbers or payment information
- Social Security numbers or tax identification numbers
- Personal health information protected under HIPAA
- CJIS-restricted criminal justice information

# SECTION 4: ACCESS CONTROL AND AUTHENTICATION

## 4.1 User Account Management

Access to town systems is controlled through individual user accounts. Each person must have their own unique account to ensure accountability and proper audit trails.

### Account Termination

Accounts must be disabled immediately upon:

- Employee termination or resignation
- End of elected official or board member term
- Contractor or vendor engagement completion

## 4.2 Password Requirements

Strong passwords are the first line of defense against unauthorized access.

### Password Complexity

Passwords must meet these minimum requirements:

- Minimum 12 characters in length (16+ recommended)
- Contain mix of uppercase and lowercase letters
- Include at least one number
- Include at least one special character (!@#$%^&*)
- Not contain username, town name, or common dictionary words

### Password Protection

- **NEVER share passwords with anyone**—including supervisors, IT staff, or colleagues
- Do not write passwords down or store in plain text files
- Do not send passwords via email, chat, or text message
- Do not reuse passwords across multiple accounts
- Change password immediately if compromise is suspected

**CRITICAL:** Town IT staff will NEVER ask for your password. If someone requests your password, report it immediately as a potential security incident.

## 4.3 Multi-Factor Authentication (MFA)

Multi-factor authentication adds an essential second layer of security beyond passwords.

### MFA is MANDATORY for:

- All town email accounts
- Remote access and VPN connections
- Administrative access to systems
- Access to financial systems
- Any system handling confidential or sensitive data

### MFA Best Practices

- Register multiple authentication methods for backup
- Keep authentication device secure and accessible
- Report lost or stolen authentication devices immediately
- Never share MFA codes with anyone
- Report any MFA prompts you did not initiate (may indicate account compromise)

# SECTION 5: DATA PROTECTION AND HANDLING

## 5.1 Data Classification Levels

The town uses three classification levels: Confidential, Internal, and Public (defined in Section 2.2).

## 5.2 Handling Requirements by Classification

### Confidential Data Handling

**Access Control:**

- Access limited to authorized personnel with business need
- Multi-factor authentication required
- Access logged and monitored

**Storage:**

- Encryption at rest required for electronic data
- Store only in approved secure locations
- Never store on personal devices or personal cloud accounts
- USB drives must be encrypted if containing confidential data

**Transmission:**

- Encryption in transit required (TLS/SSL, VPN)
- Never send via unencrypted email or messaging
- Verify recipient before sending

**Disposal:**

- Paper: Cross-cut shred all confidential documents
- Electronic media: Secure wipe or physical destruction
- Never place confidential documents in regular trash

## 5.3 Personally Identifiable Information (PII)

PII requires special protection under New York law. PII includes: Social Security numbers, driver's license numbers, account numbers with security codes, and biometric information.

**PII Protection Requirements:**

- All PII must be treated as Confidential
- Access restricted to personnel with business need
- Encryption required for storage and transmission
- Never email PII without encryption
- Report PII breaches immediately (NY Gen. Muni. Law § 18)

## 5.4 Data Storage Requirements

**Approved Storage Locations:**

- Town file servers and network storage
- Town-approved cloud storage platforms
- Town-issued devices with encryption enabled

**Prohibited Storage Locations:**

- Personal email accounts
- Personal cloud storage (Dropbox personal, Google Drive personal accounts)
- Unencrypted USB drives or external media
- Home computers not approved for remote work

# SECTION 6: ENDPOINT AND NETWORK SECURITY

## 6.1 Mandatory Security Tools

All town devices must have the following security controls enabled:

- Antivirus/anti-malware software (current and updated)
- Firewall enabled
- Full-disk encryption (BitLocker for Windows, FileVault for Mac)
- Automatic screen lock after 10 minutes of inactivity
- Operating system security updates enabled

**Strictly Prohibited:**

- Disabling or removing security software
- Bypassing security controls
- Tampering with security configurations

## 6.2 Software Installation and Management

Only approved software may be installed on town devices. Submit requests to IT Manager with business justification.

**Prohibited Software:**

- Pirated or unlicensed software
- Peer-to-peer file sharing applications
- Software from untrusted sources
- Unauthorized remote access tools
- Cryptocurrency mining software

## 6.3 Patch Management and Updates

Keeping systems updated is critical for security. Unpatched systems are vulnerable to known exploits.

- Enable automatic updates for operating systems
- Install critical security updates within 48 hours of release
- Restart devices when required to complete updates
- Do not postpone updates repeatedly

## 6.4 Mobile Device Security

**Town-issued mobile devices must meet these requirements:**

- Screen lock with PIN (minimum 6 digits) or biometric authentication
- Full device encryption enabled
- Operating system kept current
- Report lost/stolen devices immediately

# SECTION 7: REMOTE ACCESS AND TELEWORK

## 7.1 VPN Requirements

### When VPN is Required

Virtual Private Network (VPN) must be used when:

- Accessing internal town resources remotely
- Working on public WiFi networks
- Remote access from home offices
- Accessing confidential information remotely

## 7.2 Home Office Security

### Physical Security

- Work in private area with controlled access
- Position screens away from windows and common areas
- Lock screens when stepping away, even at home
- Do not allow family members to use work devices
- Use privacy screen if working in shared spaces

### Network Security

- Secure home WiFi with WPA2 or WPA3 encryption
- Use VPN when accessing town resources
- Keep home router firmware updated

## 7.3 Public WiFi Restrictions

Public WiFi networks are inherently insecure:

- Avoid accessing town systems on public WiFi when possible
- Always use VPN when connecting to public WiFi
- Verify network name with establishment staff (beware of fake networks)
- Consider using mobile hotspot instead

# SECTION 8: INCIDENT RESPONSE AND REPORTING

**(Refer to Cybersecurity Incident Notification Guide Resource)**

## 8.1 Security Incident Definition

A security incident is any event that compromises or threatens the confidentiality, integrity, or availability of town information assets.

### Examples:

- Confirmed or suspected malware infection
- Ransomware attack or file encryption
- Unauthorized access to systems or data
- Lost or stolen devices with town data
- Successful phishing attack
- Data breach or unauthorized disclosure

## 8.2 Incident Severity Levels

### CRITICAL (Severity 1) - Response: IMMEDIATE

- Active ransomware attack
- Confirmed breach of critical systems
- Large-scale data breach with PII

### HIGH (Severity 2) - Response: Within 1 hour

- Confirmed malware on multiple systems
- Unauthorized access to sensitive data
- Lost/stolen device with unencrypted confidential data

### MEDIUM (Severity 3) - Response: Within 4 hours

- Suspected malware on single system
- Minor unauthorized access attempt
- Lost/stolen device with encrypted data

## 8.3 Reporting Procedures

### IMMEDIATE REPORTING REQUIRED

If you suspect or discover a security incident, report it IMMEDIATELY. Do not wait.

**Primary Contact:**

- IT Manager: (845) 259-1700 / security@mcstechinc.com

**If IT Manager Unavailable:**

- Town Supervisor: [Phone] / [Email]

### What to Report

- What happened (description of the incident)
- When it occurred or was discovered
- What systems or data are affected
- What immediate actions have been taken
- Your contact information

### DO NOT Delay Reporting

Never delay reporting because:

- You're not sure if it's really an incident (let experts determine)
- You're worried about consequences (honest mistakes reported quickly are handled appropriately)
- You think you can fix it yourself (proper incident response is a team effort)

***When in doubt, report it. False alarms are better than missed incidents.***

## 8.4 Public Notification Requirements

Under NY General Municipal Law § 18, the town must notify residents if breach involves their private information (SSN, driver's license, account numbers with security codes). Notification must occur at most expedient time possible without unreasonable delay.

# SECTION 9: BUSINESS CONTINUITY AND BACKUP

## 9.1 Backup Requirements

**What is Backed Up:**

- File servers and network storage
- Business applications and databases
- Financial system data

**Backup Frequency:**

- Critical systems: Daily backups
- Less critical data: Weekly backups minimum

## 9.2 3-2-1 Backup Strategy

Where possible, follow 3-2-1 backup rule:

- 3 copies of data (1 primary + 2 backups)
- 2 different storage media types
- 1 copy offsite (cloud or alternate physical location)

## 9.3 Disaster Recovery Priorities

Systems and services recovered in order of business criticality:

**Priority 1 (Immediate - within 4 hours):**

- Email and communication systems
- Phone systems

**Priority 2 (Urgent - within 24 hours):**

- Financial systems
- Resident services systems

# SECTION 10: ELECTRONIC MEDIA DISPOSAL

## 10.1 Electronic Media Disposal

- Hard drives: Secure wipe using approved software or physical destruction
- USB drives: Secure wipe or physical destruction
- Mobile devices: Factory reset after encryption enabled, or physical destruction
- CDs/DVDs: Physical destruction (shredding)
- Contact IT before disposing of any device containing town data

## 10.2 Document Shredding

- Confidential documents: Use cross-cut shredder
- Never place confidential documents in regular trash or recycling

# SECTION 11: EMAIL AND COMMUNICATION SECURITY

## 11.1 Phishing Awareness and Prevention

### Recognizing Phishing

Be suspicious of emails that:

- Create urgency or pressure to act quickly ('Account will be closed!')
- Request sensitive information or credentials
- Contain unexpected attachments
- Have suspicious links (hover to preview destination)
- Come from unknown senders or spoofed addresses
- Have poor grammar or spelling errors
- Use generic greetings ('Dear Customer' instead of your name)

### If You Receive Suspicious Email

**DO NOT:**

- Click links or open attachments
- Reply or provide any information

**DO:**

- Report to IT Manager immediately
- Delete after reporting

### If You Click Phishing Link

Act immediately:

- Report to IT Manager IMMEDIATELY
- Change your password right away
- Do not be embarrassed—report quickly to minimize damage

# POLICY ADMINISTRATION

## Policy Review and Updates

This policy will be reviewed annually by IT Manager and Town administration, with updates approved by Town Board.

## Training and Awareness

All users must complete information security awareness training:

- Upon hire or initial system access
- Annually as refresher training
- When policies are significantly updated

## Questions and Support

If you have questions about this policy or need guidance:

- IT Manager: [Contact Information] - Technical security questions
- Town Supervisor: [Contact Information] - Policy interpretation
- Town Clerk: [Contact Information] - FOIL and public records questions

*When in doubt about security, ask. It is always better to seek clarification than to make assumptions that could compromise security or violate public records laws.*

# POLICY ACKNOWLEDGMENT FORM

By signing below, I acknowledge that I have received, read, and understood the Town of Gardiner Information Technology Security and Usage Policy. I agree to comply with all provisions of this policy as a condition of my employment or affiliation with the town.

I understand that:

- This policy is mandatory and applies to my use of all town technology resources
- I have no expectation of privacy when using town systems
- My communications on town systems may become public records
- Violations may result in disciplinary action up to and including termination
- I am responsible for immediately reporting security incidents
- I am responsible for protecting passwords and town data

_____
Employee/User Name (printed)

_____
Employee/User Signature

_____
Date

_____
Department

_____
Position/Title

*For Office Use Only:*
*Received by:* _____ *Date:* _____
*Filed in personnel file: ☐ Yes*