Town of Wellesley – User Policies on Information Technology Resources

Aligned with NIST SP 800-53 Rev. 5 and CIS Controls v8

Version 1.0 – January 2026

1. History

This document is a living publication that is updated periodically to reflect changes in technology, regulatory requirements, and cybersecurity best practices. It is aligned with **NIST SP 800-53 Rev. 5** and **CIS Controls v8** to complement internal IT departmental policies and procedures.

2. Authority and Approval

Town Bylaw 19.32.g grants oversight of the Town's network and information systems to the Executive Director of General Government Services. Approval is required annually or upon significant modification.

Date	Version	Name	Title / Role	Status
1/8/26	1.0	Meghan Jop	Executive Director of General Government Services	Approved

3. Owner

Brian DuPont
IT Director, Town of Wellesley
781-431-1019 x2280
bdupont@wellesleyma.gov

4. Introduction

This document defines the user-facing policies governing the use of Information Technology Resources (ITRs) owned or operated by the Town of Wellesley. These policies are aligned with industry standards for security and privacy, including **NIST SP 800-53 Rev. 5 controls** (notably AC, AT, MP, PL, PS, SC, and SI families) and **CIS Controls v8**, to ensure appropriate protection of Town information and resources.

5. Purpose

The purpose of this policy is to:

- Establish user responsibilities and acceptable behavior related to Town ITRs.
- Protect Town information, systems, and services from unauthorized access, disclosure, alteration, or destruction.
- Ensure compliance with state and federal regulations, including **M.G.L. c. 93H** and **201 CMR 17.00**.

6. Scope

This policy applies to all ITRs, including on-premises and cloud-hosted systems, mobile devices, workstations, peripherals, software, and telecommunications equipment. It also applies to all employees, contractors, consultants, volunteers, and third parties granted access to Town resources.

7. Audience

All users of Town ITRs are responsible for understanding and complying with this policy. It may be shared with auditors, regulators, or external assessors to demonstrate control implementation. Use of Town resources constitutes acceptance of these requirements.

8. Responsibility

The IT Department (IT) is responsible for maintaining, updating, and enforcing this policy. All employees must exercise sound judgment and comply with these standards.

9. Definitions of Key Terms

This section explains technical or potentially confusing terminology used throughout this policy.

Information Technology Resources (ITRs) – All Town-owned or authorized devices, systems, software, networks, cloud services, and data used to conduct Town business.

Personally Identifiable Information (PII) – Information that can identify an individual, such as name, Social Security number, driver's license number, financial account information, or other sensitive identifiers.

Protected Health Information (PHI) – Individually identifiable health information that relates to a person's past, present, or future physical or mental health condition, the provision of healthcare, or payment for healthcare, and that can be used to identify the individual (e.g., medical record numbers, diagnoses, treatment details, test results, insurance information).

Multi-Factor Authentication (MFA) – A security method requiring two or more verification steps (e.g., password + mobile code) to confirm a user's identity.

Least Privilege – A security principle granting users the minimum access rights needed to perform their job responsibilities.

Privileged Account – An account with elevated permissions that allow administrative actions, typically restricted to IT staff.

Encryption – A method of protecting data by converting it into a secure, unreadable format unless unlocked with an authorized key.

Malware – Malicious software such as viruses, ransomware, and spyware that can damage, steal, or compromise data.

Phishing – Fraudulent attempts to trick users into revealing sensitive information or downloading harmful software.

Jailbroken / Rooted Device – A mobile device with manufacturer restrictions removed, often making it insecure and unsuitable for accessing Town systems.

Incident – Any event that could compromise the confidentiality, integrity, or availability of Town data or technology resources.

Breach – Confirmed unauthorized access, disclosure, or loss of sensitive or confidential information.

WPA2/WPA3 – Wireless security standards that use encryption to protect Wi-Fi networks with improved authentication.

10. Access Control

10.1 Accounts and Authentication

- Access to ITRs must be granted using unique user accounts.
- Shared or generic accounts are prohibited without written approval from the IT Director.
- Multi-Factor Authentication (MFA) is required for all remote access and applicable systems.
- Privileged access is restricted to authorized IT personnel.
- Accounts may be locked after repeated authentication failures.

10.2 Modifying Access

- All requests for access changes must be submitted via IT helpdesk ticket.
- Access approvals will follow a least privilege, role-based model.
- Access must be revoked immediately upon separation.
- Accounts inactive for 30 days will be disabled unless approval for extension has been granted by the IT Director.

11. Passwords

11.1 Requirements

- Minimum length: **16 characters**
- Must use upper/lowercase letters, numbers, and special characters (except !).
- Must be unique and not reused across systems.
- Must avoid common or easily guessable words.
- Password changes may be required periodically per IT direction.

11.2 Protection

- Passwords must not be shared or written down.
- Passwords must not be stored or transmitted unencrypted.

11.3 Notification

- Users must immediately report suspected password compromise to IT.
- IT may reset account passwords when compromise is suspected.

12. Acceptable Use

12.1 General Use Principles

- ITRs are for Town business only.
- Users must protect confidential and sensitive data.
- No expectation of privacy exists when using Town-managed ITRs.
- The IT Department may monitor systems for maintenance and security.

12.2 Internet and Email

- The Town may block malicious or inappropriate content.
- All employees must use their assigned wellesleyma.gov address.
- Users must not forward Town data or use auto-forwarding to external email accounts.
- Emails are public records under M.G.L. c. 66 § 10 and will be retained in accordance with the Municipal Records Retention Schedule.
- Users must use caution with unknown attachments or URLs.

12.3 Unacceptable Uses

Prohibited activities include but are not limited to:

- Violations of copyright or software licensing.
- Introduction of malware or unauthorized software.
- Unauthorized access or attempts to circumvent security controls.
- Sending spam, phishing emails, or fraudulent messages.
- Harassment, threats, or creation of a hostile environment.

13. Data Classification and Handling

13.1 Classification Levels

- **Restricted:** Highly sensitive or confidential information (security plans, financials)
- **Personal:** Data regulated by state/federal law (PII, PHI)
- **Public:** Records subject to disclosure under MA Public Records Law

13.2 Handling Requirements

Users must follow these handling requirements:

- Access, share, and store only the minimum data necessary to perform job duties.
- Store Restricted and Personal information only on Town-approved systems.
- Transmit Restricted and Personal information only through encrypted channels approved by IT.
- Do not store Town data on personal cloud devices (e.g. personal Google Drive, Dropbox, iCloud)

13.3 Removable Media

- Use of USB drives or external storage devices is prohibited unless specifically authorized by the IT Director.
- Approved storage devices must always be encrypted and remain in the user's control.

14. Workstations and Devices

14.1 General Requirements

- Town-owned devices are for authorized use only.
- Workstations must be locked when unattended.
- Portable devices must be secured and encrypted.
- Personal devices may be used only where approved.

14.2 Endpoint Protection

Users must not disable, circumvent, or interfere with:

- Antivirus or Endpoint Detection and Response (EDR) software.
- Automatic security updates.
- Device encryption.

14.3 Software Requests

Requests for new software must:

- Be submitted via IT helpdesk ticket.
- Include business justification.
- Undergo security and licensing review.
- Receive written approval from the IT Director prior to installation.

14.4 Mobile Devices

- Must not access Town data without IT authorization.
- Must not be jailbroken or rooted.
- Must be encrypted and auto-lock within one minute.
- Must use strong PINs (6+ digits, non-sequential).
- Must apply timely system updates.
- Town may wipe lost/stolen devices remotely.

15. Remote Access and Remote Work

15.1 Authorization

Remote access to Town systems is a privilege and must be approved by a supervisor and the IT Director. Unauthorized remote access to any Town resource is strictly prohibited.

15.2 Security Requirements for Remote Work

Users must adhere to the following:

- Only Town-managed or IT-approved devices may access Town systems remotely.
- Home or remote networks must use secure Wi-Fi configurations (WPA2/WPA3 encryption and non-default passwords).
- Remote sessions must be conducted in private locations where screens cannot be viewed by unauthorized individuals.
- Users must lock or log off devices when not in use, even in a home environment.

15.3 Prohibited Practices

Users may not:

- Allow family members or others to use Town devices.
- Access Town resources from shared, public, or untrusted computers.

16. Incident Reporting & Response

16.1 Mandatory Reporting Requirements

Users must immediately report:

- Suspicious emails, phishing attempts, or unexpected attachments/links.

- Lost or stolen devices.
- Unauthorized access or attempted access.
- Malware alerts or unusual system behavior.
- Accidental disclosure of Town information.
- Lost badges, keys, or access credentials.

16.2 User Actions During an Incident

Until IT arrives or provides instructions, users must:

- Stop using the affected device immediately.
- Do not attempt to investigate, delete files, or "fix" the issue.
- Do not shut down the computer.
- Preserve any evidence (e.g. suspicious emails, screenshots).

16.3 How to Report

- Incidents and suspected breaches must be reported via email to the IT Department at IT@wellesleyma.gov or phone call to 781-431-1019 x2288.
- Suspicious emails, phishing attempts, or unexpected attachments/links must be reported via the Phish Alert Button or screenshot.
- The notification must include a description of what occurred and all surrounding circumstances.

17. Security Training

17.1 Applicability

All employees who use ITRs or access sensitive data must complete IT security training.

17.2 Frequency

Training occurs at least quarterly.

17.3 Topics

Training will cover:

- Policies and acceptable use
- Passwords and access controls
- Phishing and social engineering
- Malware dangers
- Data protection
- Incident reporting

17.4 Monitoring

The IT Department will track compliance and maintain records for at least one year.

18. Exemptions

Exemptions from all or some of these policies may be granted in writing by the IT Director only when the benefits outweigh the risks.

19. Compliance

- The IT Department may audit and monitor systems to ensure policy compliance.
- Violations may result in disciplinary action up to termination and/or referral to law enforcement.
- Users must report suspected violations to their supervisor and IT.
- The IT Department enforces this policy.

20. Acknowledgement

By signing below, the employee acknowledges understanding and acceptance of these policies.

Employee Name: ____

Employee Signature: ____ Date: __________