Town of South Bristol Information Security Policy

Adopted: May 2026

Last Reviewed: May 2026

Table of Contents

1. Purpose 3
2. Scope 3
3. Governance & Responsibilities 3
   3.1 Town Board 3
   3.2 Information Security Officer (ISO) 3
   3.3 Privacy Officer 4
   3.4 Managed IT Service Provider (MSP) 4
   3.5 All Users 4
4. Risk Management 5
5. Access Control & Remote Access 5
6. Data Protection & Backup 5
7. Incident Response & Breach Notification 6
   7.1 Internal Incident Reporting 6
   7.2 Reporting to NYS DHSES 6
   7.3 Breach Notification to Individuals 6
8. Vendor & Third-Party Management 6
9. Cybersecurity Training 7
10. Disaster Recovery 7
11. Policy Review 7

1. Purpose

The purpose of this Information Security Policy is to protect the Town of South Bristol's information systems and private data from unauthorized access, misuse, disruption, or loss, and to ensure compliance with applicable New York State laws.

2. Scope

This policy applies to:

- All Town Board members
- All Town employees and elected officials
- Volunteers and contractors
- Third parties accessing Town systems
- All Town-owned devices, systems, and data

3. Governance & Responsibilities

The Town of South Bristol recognizes that effective cybersecurity requires clear governance, defined roles, and accountability. The Town operates under a model in which policy oversight is maintained by the Town Board, while technical implementation is performed by a contracted Managed IT Service Provider (MSP). This section defines those responsibilities.

3.1 Town Board

The Town Board retains ultimate authority and oversight for information security governance. The Board is responsible for establishing policy direction and ensuring appropriate safeguards are in place to protect Town systems and data.

The Town Board shall:

- Adopt and maintain this policy
- Appoints an Information Security Officer (ISO)
- Appoints a Privacy Officer
- Provides oversight of cybersecurity risks
- Review periodic security reports

3.2 Information Security Officer (ISO)

The Information Security Officer (ISO) serves as the Town's designated oversight official for cybersecurity matters. The ISO provides coordination, monitoring, and reporting functions, but does not perform day-to-day technical system administration unless separately authorized.

The ISO shall:

- Oversee implementation of this policy
- Coordinate with the Town's Managed IT Service Provider (MSP)

- Review risk assessments and incident reports
- Ensure compliance with state reporting requirements
- Report cybersecurity matters to the Town Board

3.3 Privacy Officer

The Privacy Officer serves as the Town's designated lead for data identification and privacy coordination. Working with department heads, the Information Security Officer (ISO), and the Managed IT Service Provider (MSP), the Privacy Officer helps ensure the Town understands what private and sensitive information it maintains, where that information resides, and how it should be handled and protected.

The Privacy Officer shall:

- Identify and maintain an inventory of private, sensitive, and confidential data maintained by the Town
- Document where such data resides, is processed, or is transmitted across Town systems, devices, applications, paper files, and third-party services
- Coordinate with the ISO and MSP so administrative, technical, and physical safeguards align to the data and systems being protected
- Support development of data handling, retention, and privacy-related procedures
- Assist with breach response, notification, and privacy compliance as appropriate

3.4 Managed IT Service Provider (MSP)

The Town contracts with a Managed IT Service Provider (MSP) to implement and maintain technical safeguards. The MSP is responsible for the operational management and protection of the Town’s information systems under the direction of the Town Board and in coordination with the ISO.

The MSP shall:

- Monitor and maintain Town information systems and network infrastructure
- Maintain firewalls, endpoint protection, and system updates
- Implement and maintain secure authentication controls where feasible
- Maintain secure, regular data backups capable of supporting disaster recovery
- Assist with periodic risk assessments or vulnerability reviews
- Assist in incident investigation, containment, remediation, and recovery
- Support compliance with required state and federal cybersecurity reporting

3.5 All Users

All individuals who access or use Town systems share responsibility for protecting Town information and technology resources.

All users must:

- Comply with this Information Security Policy, the Employee Handbook, and related technology, acceptable use, and data handling procedures
- Use Town systems only for authorized and legitimate Town purposes
- Protect login credentials and not share passwords or authentication devices
- Complete required annual cybersecurity training
- Exercise caution regarding phishing emails, suspicious links, and unknown attachments
- Immediately report suspected cybersecurity incidents, data breaches, lost devices, or unusual system activity to the Information Security Officer or the Managed IT Service Provider

4. Risk Management

The Town shall take reasonable steps to identify and mitigate cybersecurity risks.

At minimum:

- Periodic risk assessments or vulnerability reviews shall be conducted
- Material risks shall be reported to the Town Board
- This policy shall be reviewed annually

5. Access Control & Remote Access

The Town of South Bristol shall implement reasonable access controls to ensure that information systems and data are accessible only to authorized individuals for legitimate Town purposes.

Accordingly:

- Access shall be limited to authorized users based on job responsibilities or official duties.
- User accounts shall be uniquely assigned to individuals; shared accounts shall be avoided unless operationally necessary and appropriately controlled.
- Access rights shall be reviewed periodically and removed promptly upon separation from service or change in role.
- Multi-factor authentication (MFA) shall be implemented where feasible, particularly for remote access and administrative accounts.
- Remote access to Town systems shall be secured through approved methods (e.g., VPN or equivalent secure connection) and managed in coordination with the Town's Managed IT Service Provider.

6. Data Protection & Backup

The Town shall implement reasonable safeguards to protect private and sensitive information.

At minimum:

- Anti-malware and endpoint protection shall be maintained

- Security patches shall be applied in a timely manner
- Secure, regular backups shall be maintained
- Backup systems shall support disaster recovery capability
- Backup data shall be stored securely and protected from unauthorized alteration

7. Incident Response & Breach Notification

7.1 Internal Incident Reporting

Any suspected or confirmed cybersecurity incident must be immediately reported to:

- The Information Security Officer (ISO)
- The Managed IT Service Provider (MSP)

7.2 Reporting to NYS DHSES

In accordance with New York State law:

- Cybersecurity incidents shall be reported to the New York State Division of Homeland Security and Emergency Services (DHSES) within 72 hours of discovery.
- Any ransomware payment shall be reported to DHSES within 24 hours of payment.

The ISO, in coordination with the MSP, shall ensure required reporting is completed.

7.3 Breach Notification to Individuals

If private information is compromised, the Town shall comply with New York State Technology Law §208 and other applicable laws.

The Information Security Officer, in coordination with the Managed IT Service Provider and legal counsel as appropriate, shall ensure:

- Timely notification to affected individuals
- Notification to required state agencies
- Documentation of the incident, investigation, and response actions

The Town Board shall be informed of any reportable breach and resulting notifications.

8. Vendor & Third-Party Management

Third parties with access to Town systems or private data must:

- Be authorized by the Town
- Maintain reasonable security safeguards
- Comply with applicable laws
- Enter into written agreements where appropriate

9. Cybersecurity Training

The Town shall provide ongoing cybersecurity awareness training to employees and officials, including annual training and additional updates or reminders as appropriate, consistent with New York State guidance.

Training shall include:

- Phishing awareness
- Password security
- Data handling best practices
- Incident reporting procedures

10. Disaster Recovery

The Town shall maintain a disaster recovery capability appropriate to its size and resources.

At minimum:

- Critical systems shall be backed up regularly
- Backup restoration capability shall be periodically tested
- The MSP shall assist in system recovery in the event of disruption

11. Policy Review

This policy shall be reviewed at least annually by the ISO and Town Board and updated as necessary.