



## RESOLUTION 25-649

### A RESOLUTION OF THE TOWN OF MOUNT CARMEL, TENNESSEE ADOPTING A CYBERSECURITY POLICY

**WHEREAS**, pursuant to T.C.A. § 7-51-2302, utilities are required to prepare and implement a cybersecurity plan to protect their facilities from unauthorized use, alteration, ransom, or destruction of electronic data; and

**WHEREAS**, the Town of Mount Carmel desires to comply with state law and is committed to maintaining the confidentiality, integrity, and availability of its information systems and technology assets; and

**WHEREAS**, the cybersecurity policy establishes the minimum requirements for securing the Town's IT assets and aligns with the National Institute of Standards and Technology (NIST) Cybersecurity Framework to ensure consistency, resilience, and effective risk management; and

**WHEREAS**, this policy applies to all IT assets owned, leased, or operated by the Town of Mount Carmel and governs all employees, contractors, and third-party service providers who access or use the Town's IT systems, data, or infrastructure; and

**WHEREAS**, all Town departments are required to implement this policy in conjunction with industry-specific regulations and applicable state and federal laws.

**NOW THEREFORE, BE IT RESOLVED** by the Board of Mayor and Aldermen meeting at Mount Carmel, Tennessee, on this 27<sup>th</sup> day of March, 2025, that:

**SECTION 1.** The Cybersecurity Policy attached hereto as Exhibit A is hereby adopted and shall be implemented by all Town departments and personnel.

**SECTION 2.** Town Administration shall monitor adherence to this policy and enforce compliance through regular assessments and disciplinary actions consistent with the standard procedures outlined in the Personnel Policies and Procedures document.

**SECTION 3.** The policy shall be reviewed bi-annually and updated as needed to address changes in technology, regulations, or risks.

This Resolution shall take effect immediately, the public welfare requiring it.

ADOPTED this 27<sup>th</sup> day of March, 2025.

  
\_\_\_\_\_  
John Gibson, Mayor

Attest:

  
\_\_\_\_\_  
Tyler Williams, Town Recorder



## **Cybersecurity Policy**

### **1. Policy Statement**

The Town of Mount Carmel, Tennessee, is committed to maintaining the confidentiality, integrity, and availability of its information systems and technology assets. This cybersecurity policy establishes the minimum requirements for securing the Town's IT assets.

### **2. Purpose**

The purpose of this policy is to provide a baseline for managing and reducing cybersecurity risks to the Town of Mount Carmel's infrastructure, information systems, data, and services. This policy aligns with the National Institute of Standards and Technology (NIST) Cybersecurity Framework to ensure consistency, resilience, and effective risk management.

### **3. Scope**

This policy applies to all IT assets owned, leased, or operated by the Town of Mount Carmel. It governs all employees, contractors, and third-party service providers who access or use the Town's IT systems, data, or infrastructure.

All Town departments are governed by this policy. The following specific departments are required to implement this policy in conjunction with industry-specific regulations and applicable state and federal laws.

- Administration
- Fire Department
- Police Department
- Animal Control
- Public Works
- Wastewater Treatment Plant
- Library



## **Cybersecurity Policy**

### **4. Framework**

The Town of Mount Carmel adopts the core functions of the NIST Cybersecurity Framework

#### **a. Identify**

- Maintain an inventory of Town-owned IT assets, including hardware, software, and data.
- Prioritize critical assets and systems requiring protection based on risk assessments.

#### **b. Protect**

- Implement safeguards such as access controls, encryption, and secure configurations to protect IT assets and data.
- Establish and enforce user authentication mechanisms and role-based access controls.

#### **c. Detect**

- Deploy continuous monitoring tools to identify cybersecurity threats and anomalies.
- Perform regular vulnerability assessments and penetration tests to identify and address potential risks.

#### **d. Respond**

- Develop and maintain an incident response plan to mitigate the impact of cybersecurity incidents.
- Establish a communication process to notify relevant stakeholders in the event of an incident.

#### **e. Recover**

- Implement a business continuity and disaster recovery plan to ensure timely restoration of critical services.
- Conduct regular backups of critical data and verify the effectiveness of restoration processes.



## **Cybersecurity Policy**

### **5. Roles and Responsibilities**

- Designate cybersecurity roles or teams responsible for implementing this policy.
- Department Directors are responsible for ensuring compliance with this policy within their departments
- Ensure all employees complete cybersecurity awareness training and follow established guidelines.

### **6. Compliance and Enforcement**

- The Town of Mount Carmel Administration will monitor adherence to this policy and enforce compliance.
- Regular assessments will be conducted to ensure alignment with applicable regulations.
- Disciplinary action related to violations of this policy shall be consistent with the standard procedures outlined in the Personnel Policies and Procedures document.

### **7. Review and Updates**

This policy will be reviewed annually and updated as needed to address changes in technology, regulations, or risks.

### **8. Reference Documents**

- National Institute of Standards and Technology (NIST) Cybersecurity Framework (Public Document).



## Cybersecurity Policy

### Approval and Signature Page

John K. Gibson Date 03/25/2025

John Gibson, Mayor

Tyler Williams Date 3-27-25

Tyler Williams, Town Recorder

Allen J. Coup Date 3-28-25

Allen Coup, Town Attorney