TOWN OF GREENVILLE, FLORIDA
Cybersecurity Policy

I. PURPOSE

The Town of Greenville, Florida, recognizes the importance of safeguarding its data, information technology (IT), and IT resources. This Cybersecurity Policy establishes cybersecurity standards that ensure the availability, confidentiality, and integrity of the Town's information systems and data. The policy is consistent with generally accepted best practices, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

II. SCOPE

This policy applies to all employees, elected officials, contractors, vendors, and third parties who access, use, or manage the Town's IT systems, networks, and data.

III. CYBERSECURITY GOVERNANCE

A. Information Security Officer: The Town Manager or the Town Manager's designee shall serve as an Information Security Officer (ISO).

B. ISO Responsibilities: The Information Security Officer is responsible for implementing security measures and monitoring compliance.

C. Compliance: All employees and users are responsible for adhering to this policy and reporting potential security threats.

IV. CYBERSECURITY FRAMEWORK

A. NIST Cybersecurity Framework: The Town of Greenville shall adopt the Cybersecurity Framework (CSF), adopted by the National Institute of Standards and Technology, which consists of five key functions:

1. Identify

a. Maintain an inventory of IT assets, including hardware, software, and data systems.

b. Conduct cybersecurity risk assessments at least annually.

c. Identify and classify sensitive data based on confidentiality and regulatory requirements.

d. Develop and enforce access control policies.

2. Protect

a. Implement multi-factor authentication (MFA) for all Town IT systems.

b. Require strong passwords that meet complexity and expiration requirements.

c. Ensure all IT systems and devices receive regular security updates and patches.

d. Encrypt sensitive data at rest and in transit.

e. Restrict administrative access to IT systems based on the principle of least privilege.

f. Implement firewalls, antivirus software, and intrusion detection/ prevention systems (IDS/IPS).

g. Conduct cybersecurity awareness training for employees at least annually.

3. Detect

a. Implement 24/7 monitoring of network and system activities using a Security Information and Event Management (SIEM) system.

b. Establish an incident detection and alerting system for unauthorized access and anomalies.

c. Conduct regular vulnerability scans and penetration testing.

4. Respond

a. Develop an Incident Response Plan (IRP) that includes:

i. Procedures for detecting, reporting, and responding to cybersecurity incidents.

ii. Defined roles and responsibilities during a cybersecurity event.

iii. Communication protocols with law enforcement and state cybersecurity agencies.

iv. Data breach notification procedures in compliance with section 501.171, *Florida Statutes*.

b. Conduct cybersecurity incident response exercises at least twice per year.

5. Recover

a. Implement regular data backups stored in a secure, offsite location.

b. Ensure business continuity through a Disaster Recovery Plan (DRP).

c. Conduct annual disaster recovery testing.

d. Review cybersecurity incidents and apply lessons learned to improve security controls.

V. USER ACCESS AND AUTHENTICATION

A. Town-Approved Credentials: Employees and contractors must use Town-approved credentials to access IT systems.

B. Role-Based Access Controls: Role-based access controls (RBAC) shall be enforced to restrict data access.

C. Virtual Private Network: Remote access to Town systems requires a Virtual Private Network (VPN).

VI. THIRD-PARTY SECURITY

A. Cybersecurity Agreement: All vendors and contractors with access to Town IT systems must sign a Cybersecurity Agreement.

B. Security Standards: Vendors handling sensitive Town data must comply with NIST, ISO 27001, and other applicable security standards.

VII. DATA PROTECTION AND PRIVACY

A. Encryption: Personal Identifiable Information (PII) and Financial Data shall be protected using encryption.

B. Cloud Storage: Employees must use Town-approved cloud storage and avoid unauthorized external storage.

C. Public Records: Data retention and disposal shall follow Chap. 119, *Florida Statutes*, and Chap. 257, *Florida Statutes*, *respectively*, as well as the Town of Greenville Public Records, Record Retention and Disposition Policy.

VIII. CYBERSECURITY AWARENESS AND TRAINING

A. Annual Training: Mandatory annual cybersecurity training for all employees.

B. Awareness: Phishing simulations shall be conducted to test employee awareness.

C. Reporting Requirements: Employees must report suspicious emails and cyber threats immediately.

IX. POLICY ENFORCEMENT AND COMPLIANCE

A. Disciplinary Action: Violations of this policy will result in disciplinary action, up to and including termination.

B. Audits: The Town's IT consultant shall audit and assess cybersecurity compliance quarterly.

C. Reporting Violations: Non-compliance with this policy must immediately be reported to the Town Manager. However, if the non-compliance jeopardizes or compromises the Town's data, information technology, or information technology resources, it must also be reported to the Town Council.

X. AMENDMENTS AND REVIEW

This policy shall be reviewed annually and updated as necessary to address emerging cybersecurity threats.

Ryan D. Kornegay

Ryan Kornegay, Mayor

Kimberly M. Reams

Kimberly M. Reams
Town Clerk

ACTION	SECTION(S) AMENDED	RESOLUTION #	DATE
Adoption	n/a	2025-02	02/17/2025