Town of Greentown
112 N. Meridian St. P.O. Box 247
Greentown, IN 46936
Phone (765) 628-3263 Fax (765) 628-4002

Town of Greentown – Cybersecurity Policy

1. Purpose & Scope

Purpose: Protect Greentown's digital infrastructure, data integrity, and ensure compliance with SEA 472.

Scope: Applies to all technology systems (servers, networks, endpoints, cloud services, mobile devices, and connected IoT systems) and all users (employees, elected officials, contractors, and vendors).

2. Governing Framework

This policy is based on Indiana Office of Technology (IOT) standards and guidelines in accordance with SEA 472 (effective July 1, 2025; compliance by December 31, 2027).

3. Responsibilities

The Town Council or designated CIO/CISO oversees implementation, compliance, and updates of this policy.

4. Risk Management & Incident Response

Conduct regular risk assessments to identify threats, vulnerabilities, and potential impacts.

Maintain an incident response plan with defined roles and responsibilities.

Cybersecurity incidents will be reported to the IOT within two business days (as applicable under SEA 472).

5. Access & Authentication

Principle of least privilege applies to all accounts.

Multi-factor authentication (MFA) is required for remote or privileged access.

Passwords must follow strong security standards and be rotated regularly.

6. Network & Endpoint Security

Implement firewalls, intrusion detection/prevention systems, and network segmentation.

All systems must be kept up-to-date with vendor-supported patches and updates.

Town of Greentown
112 N. Meridian St. P.O. Box 247
Greentown, IN 46936
Phone (765) 628-3263 Fax (765) 628-4002

7. Data Governance

Classify data as public, internal, or restricted.

Encrypt sensitive data both at rest and in transit.

Implement secure backup and recovery procedures.

8. Third-Party Security

Vendors must be vetted for security posture.

Contracts must include cybersecurity provisions.

Conduct regular reviews of third-party security practices.

9. Monitoring & Audits

Maintain secure logs for critical activities.

Conduct periodic audits and reviews of cybersecurity practices.

10. Training & Awareness

Provide mandatory cybersecurity training at least biennially.

Maintain training records and update training content regularly.

11. Disciplinary Measures

Policy violations may result in disciplinary action up to and including termination or legal action.

12. Review & Updates

Review this policy at least annually or following significant incidents, technology changes, or updated IOT guidance.

13. Submission

Submit this policy to the Indiana Office of Technology (IOT) by December 31, 2027, and every two years thereafter.

14. Definitions

Public Entity: Includes the Town of Greentown and all associated departments.

Technology Resources: Includes all hardware, software, networks, cloud services, and IoT devices owned or managed by the Town.

Cybersecurity Incident: Any event that threatens confidentiality, integrity, or availability of systems or data.