Town of Fulton
Information Technology Control Policy

1. Purpose

The aim of this policy is to govern the management, operation, and use of the Town of Fulton's ("Town") IT resources, guarantee data integrity, confidentiality, and availability, and meet compliance with relevant legislation, regulations, and best practice guidelines.

2. Scope

This policy applies to all hardware, software, networks, data, and information systems owned or managed by the Town of Fulton, and all users thereof including employees, contractors, consultants, and the contracted IT service provider.

3. Roles and Responsibilities

3.1. Town Management:

- Responsible for overall IT governance and policy compliance.

3.2. Contracted IT Service Provider:

- Manage all software.
- Executes routine IT services in accordance with the service level agreement (SLA).
- Develop and implement IT security measures and protocols.
- Ensures system availability, performance, and maintenance.
- Inform Town Management promptly of any security threats or breaches.

3.3. Users:

- Adhere to IT policy rules and regulations.
- Protect sensitive and confidential information from unauthorized access or disclosure.
- Notify IT service providers of any observed or suspected security incidents.

4. IT Service Management

4.1. The contracted IT service provider should adhere to the guidelines and standards outlined in the SLA.

4.2. All proposed changes to the IT infrastructure, systems, applications, or data must be approved by Town.

4.3. The IT service provider must maintain a comprehensive inventory of all IT assets.

5. Security Controls

5.1. User Access Control:
- Multi-factor authentication should be used where feasible.
- User access privileges should be granted based on roles and responsibilities and should be regularly reviewed.

5.2. Physical Security:
- Restricted physical access to IT assets like servers and network equipment.

5.3. Network Security:
- Implement network firewalls, intrusion detection and prevention systems.
- Regularly update anti-virus and anti-malware programs.

5.4. Data Protection:
- A disaster recovery plan should be in place.

5.5. Security Awareness:
- Regular training and awareness sessions should be conducted to educate users about IT security risks and best practices.
-

6. Compliance and Audit

The IT service provider must comply with applicable legal, regulatory, and contractual requirements, including those pertaining to data protection and privacy.

7. Policy Review and Amendments

This policy should be reviewed as needed, with amendments made as necessary following approval by Town Council.

Effective Date: April 16, 2025.

Approved by: Kelli Cole, Mayor

By adhering to this policy, the Town of Fulton strives to safeguard its IT resources, uphold the privacy and security of its data, ensure continuity of operations, and maintain the trust of its residents and stakeholders.