Policy Name:	**Information Security Policy**	Effective Date:	August 5, 2026
Policy Number:	**GG-IT001**	Approval Date:	August 4, 2026
Policy Area:	General Government	Council Resolution	2026.170
Policy Section:	Information Technology	Replaces Policy:	
No. of Pages:	7		

POLICY STATEMENT

The Town of Rosthern is committed to protecting the confidentiality, integrity, and availability of its information assets through the implementation of appropriate administrative, technical, and physical security controls. Information security is essential to maintaining public trust, protecting personal information, ensuring effective municipal operations, and complying with applicable legislative requirements.

All users of municipal information systems are responsible for protecting information assets from unauthorized access, disclosure, alteration, destruction, or disruption.

PURPOSE

The purpose of this policy is to:

a) Protect municipal information assets and technology resources.
b) Safeguard personal, confidential, and sensitive information.
c) Reduce the risk of cybersecurity incidents and data breaches.
d) Support the continuity of municipal operations.
e) Establish roles, responsibilities, and security requirements for users.
f) Ensure compliance with applicable legislation, regulations, and contractual obligations.

SCOPE

1) This policy applies to:

   a) All Council members, employees, contractors, consultants, volunteers, and third-party service providers.
   b) All municipal information, whether stored electronically, physically, or verbally communicated.
   c) All municipal technology resources including computers, mobile devices, servers, networks, cloud services, applications, and storage systems.
   d) All information processed, transmitted, or stored on behalf of the Town of Rosthern.

DEFINITIONS

2) "**Access Control**" – the process of restricting access to information and systems to authorized individuals.

3) "**Confidential Information**" – information that could result in harm, legal liability, privacy breaches, or operational disruption if improperly disclosed.

4) "**Information Asset**" – Any information, system, application, device, record, database, or technology resource owned or managed by the municipality.

5) "**Information Security Incident**" – Any event that compromises, or has the potential to compromise, the confidentiality, integrity, or availability of information or information systems.

6) "**Multi-Factor Authentication (MFA)**" - An authentication method requiring two or more forms of verification.

7) "**Restricted Information**" – Highly sensitive information requiring enhanced protection due to legal, financial, privacy, or operational risks.

8) "**User**" – Any person authorized to access municipal information or technology resources.

RESPONSIBILITIES

9) Council shall:

   a) Support appropriate information security governance.
   b) Ensure staff compliance with this policy.

10) Chief Administrative Officer (CAO) shall:

   a) Ensure staff compliance with this policy.
   b) Allocate appropriate resources for information security.
   c) Support incident response and risk management activities.

11) Managers and Supervisors shall:

   a) Ensure staff comply with this policy.
   b) Promote information security awareness.
   c) Report security risks and incidents promptly.

12) Information Technology Service Provider shall:

   a) Implement and maintain security controls.
   b) Monitor technology infrastructure.
   c) Manage user access and authentication controls.
   d) Perform software updates and patch management.
   e) Assist in responding to information security incidents.

13) Employees and Authorized Users shall:

   a) Comply with all information security requirements.
   b) Protect passwords and access credentials.
   c) Use information systems responsibly
   d) Report actual or suspected security incidents immediately.
   e) Complete security awareness training, as required.

14) Third-Party Service Providers shall:

   a) Protect municipal information assets.

b) Maintain appropriate security controls.
c) Report incidents affecting municipal information without delay.

PROCEDURES & GUIDELINES

17) **Information Classification**

a) Municipal information shall be classified according to its sensitivity:

- **Public** - information approved for public release.
- **Internal** – information intended from municipal business use only.
- **Confidential** - Information that requires protection due to privacy, legal, operational, or financial considerations.
- **Restricted** – highly sensitive information requiring enhanced safeguards and limited access.

18) **Access Control**

a) The Town shall implement access controls based on the principle of least privilege. Requirements include:
   - Unique user accounts for all users.
   - Strong password requirements.
   - Multi-factor authentication where available.
   - Access approvals based on business requirements.
   - Review of user access permissions.
   - Timely removal of access upon termination or role changes.

19) **Acceptable Use**

a) User shall:
   - Use municipal technology resources primarily for authorized business purposes.
   - Protect devices against unauthorized use.
   - Lock workstations when unattended.
   - Refrain from installing unauthorized software or hardware.
   - Not share passwords or access credentials.
   - Avoid accessing inappropriate, malicious, or illegal content using municipal systems.

20) **Network and System Security**

a) The Town shall maintain appropriate technical safeguards including:
   - Firewalls and network security controls.
   - Endpoint protection and anti-malware software.
   - Security monitoring and logging.
   - Vulnerability management processes.
   - Secure system configurations.
   - Regular software and firmware updates.

21) **Data Protection**

a) The Town shall:
   - Protect personal, confidential, and restricted information.
   - Use encryption where reasonable and appropriate.
   - Secure information during storage and transmission.

- Maintain backup and recovery procedures.
- Ensure disposal of records and media occurs securely and in accordance with retention requirements.

22) **Mobile Devices and Remote Access**

a) Authorized users accessing municipal systems remotely shall:
   - Use approved devices whenever practical.
   - Maintain current security updates.
   - Report lost or stolen devices immediately.
   - Utilize secure remote access methods.
   - Comply with municipal security requirements regardless of location.

23) **Physical Security**

a) The Town shall:
   - Restrict access to facilities and secure areas.
   - Protect technology assets from theft, damage, and unauthorized access.
   - Secure paper records containing confidential information.
   - Escort visitors in restricted areas when appropriate.

24) **Security Awareness**

a) The Town recognizes the importance of cybersecurity awareness and will make reasonable efforts to educate employees and officials on:
   - Password management.
   - Phishing and social engineering threats.
   - Protection of personal information.
   - Safe use of technology resources.
   - Incident reporting procedures.

25) **Information Security Incident Management**

a) All users must promptly report suspected or actual information security incidents to their supervisor or designated Town contact.

b) The Town will maintain a reasonable process for responding to information security incidents that may include:
   - Recording and assessing reported incidents.
   - Determining appropriate actions to limit or reduce potential impacts.
   - Escalating significant incidents to management, Council, legal counsel, law enforcement, or service providers as appropriate.
   - Retaining relevant information and records related to the incident when necessary.
   - Implementing corrective measures to address identified issues and reduce the likelihood of recurrence.
   - Providing notification where required by applicable legislation or regulatory requirements.

c) Examples of reportable incidents include:
   - Malware infections.
   - Unauthorized access attempts.
   - Lost or stolen devices.
   - Data breaches.
   - Fraudulent or suspicious emails.

d) Information Security Incident Response Process is as follows:

   - Incident Information

     i) Any employee, official, contractor, or user who becomes aware of a suspected or actual information security incident shall report it immediately to their supervisor, the CAO, or designated Town contact.

     ii) Examples of incidents include suspicious emails, lost or stolen devices, unauthorized access to systems or information, malware infections, or suspected privacy breaches.

   - Initial Assessment

     i) The CAO, designated manager, and/or the Town's IT service provider will review the reported incident to determine its nature, scope, and potential impact.

     ii) The incident will be assessed to determine whether immediate action is required.

   - Containment

     i) Appropriate measures will be taken to limit or prevent further impact from the incident.

     ii) Actions may include disconnecting affected equipment from the network, changing passwords, disabling user accounts, restricting system access, or engaging the Town's IT service provider.

   - Documentation

     i) All identified incidents shall be documented and Council shall be notified.

     ii) Documentation should include:

     - Date and time of the incident.
     - Description of the incident.
     - Individuals involved or affected.
     - Systems or information impacted.
     - Actions taken to contain and address the incident.

   - Resolution and Recovery

     i) The Town and/or its IT service provider will take appropriate steps to restore services, recover affected systems, and address vulnerabilities or deficiencies identified during the investigation.

     ii) Corrective actions will be implemented to reduce the likelihood of a similar incident occurring in the future.

- Notification

  i) Where required by applicable legislation, contractual obligations, or regulatory requirements, affected individuals, law enforcement agencies, regulators, insurers, or other relevant parties will be notified in a timely manner.

- Review and Follow-Up

  ii) Following resolution of the incident, the Town will review the circumstances surrounding the incident to identify lessons learned and opportunities for improvement.

  iii) Any necessary changes to policies, procedures, training, or technical controls will be considered and implemented as appropriate.

26) **Business Continuity and Disaster Recovery**

a) The Town shall:
- Maintain backup procedures for critical systems and information.
- Support disaster recovery planning.
- Test recovery capabilities periodically.
- Review continuity planning following significant changes or incidents.

27) **Third-Party Security**

a) Service providers accessing municipal information shall:
- Adhere to contractual security requirements.
- Protect information from unauthorized access.
- Maintain appropriate security controls.
- Notify the municipality immediately of any security incidents affecting municipal information.

28) **Legislative Compliance**

a) The Town shall comply with applicable legislation and regulatory obligations, including:
- The *Local Authority Freedom of Information and Protection of Privacy Act* (LAFOIP).
- Applicable records management requirements.
- Applicable contractual obligations relating to information protection.

29) **Policy Compliance**

a) Failure to comply with this policy may result in:
- Removal of system access.
- Disciplinary action.
- Contract termination.
- Legal action where appropriate.

30) **Exceptions**

a) Requests for exceptions to this policy must:
- Be documented.
- Include a risk assessment.

- Be approved by the CAO or designate.
- Be reviewed periodically.

HISTORY

Revision Date	***Description***
August 4, 2026	*New Policy Approval*

<END>