Rural Municipality of Wawken No. 93
Policy No. 200-27 Data Breach Policy
Effective July 16, 2026

1. Purpose

The Rural Municipality of Wawken No. 93 (RM) is committed to protecting the personal information, confidential information, and municipal records entrusted to it. This policy establishes procedures for identifying, responding to, containing, investigating, documenting, and reporting actual or suspected data breaches.

The objectives of this policy are to:

- Protect personal and confidential information.
- Minimize harm resulting from a breach.
- Meet obligations under Saskatchewan legislation.
- Ensure timely notification when appropriate.
- Reduce the likelihood of future breaches.

2. Scope

This policy applies to:

- Council members
- All municipal employees
- Contractors and consultants
- Volunteers
- Any third party with access to municipal information systems or records

This policy applies to information in any format, including:

- Electronic records
- Paper files
- Emails
- Databases
- Mobile devices
- Cloud-based systems
- USB drives
- Backup media

3. Legislative Authority

This policy is developed with consideration of:

- The Local Authority Freedom of Information and Protection of Privacy Act (LAFOIP), Saskatchewan
- The Municipalities Act
- Applicable cybersecurity best practices

4. Definitions

Personal Information

Information about an identifiable individual including, but not limited to:

- Name
- Home address
- Phone number
- Email address
- Financial information
- Tax roll information
- Employee records
- Utility account information
- Driver's licence information

Confidential Information

Information that is not intended for public disclosure, including:

- Personnel files
- Legal documents
- Financial records
- Vendor banking information
- Council confidential reports
- Passwords
- Security information

Data Breach

A data breach is any unauthorized:

- Access
- Collection
- Use
- Disclosure
- Modification
- Loss
- Theft
- Destruction

of municipal information.

Examples include:

- Lost laptop
- Stolen USB drive
- Ransomware attack
- Email sent to incorrect recipient
- Employee viewing records without authorization
- Hacked municipal account
- Lost paper files

5. Roles and Responsibilities

Council

Council shall:

- Support implementation of this policy
- Receive reports on significant breaches
- Approve corrective actions where necessary

Administrator

The Administrator is the Data Breach Coordinator and shall:

- Lead breach response activities
- Coordinate investigations
- Notify insurers where applicable
- Engage IT providers
- Determine notification requirements
- Maintain breach records
- Report significant breaches to Council

Employees

Employees shall:

- Immediately report suspected breaches
- Cooperate with investigations
- Protect confidential information
- Follow municipal cybersecurity procedures

Failure to report a breach may result in disciplinary action.

IT Service Provider

Where contracted, the IT provider shall:

- Assist with containment
- Preserve evidence
- Recover systems
- Conduct technical investigations
- Recommend security improvements

6. Identifying a Data Breach

A breach may be identified through:

- Employee reports
- Public complaints
- System alerts
- Antivirus software
- Ransomware notifications
- Missing files
- Lost devices
- Third-party notifications

All suspected breaches shall be treated seriously until investigated.

7. Data Breach Response Procedure

Step 1 – Report Immediately

Any employee who discovers a breach shall immediately notify:

- Administrator
- Reeve (if Administrator unavailable)

Information to provide:

- Date and time discovered
- Description of incident
- Type of information involved
- Individuals affected (if known)
- Actions already taken

Step 2 – Contain the Breach

Immediate actions may include:

- Disconnect affected computers from the network
- Disable compromised accounts
- Recover misplaced documents
- Change passwords
- Shut down unauthorized access
- Contact IT support
- Preserve evidence

Step 3 – Assess the Breach

The Administrator shall determine:

- What happened?
- When did it occur?
- What information was affected?
- Who was affected?
- Was personal information involved?
- Is the breach ongoing?
- What is the risk of harm?
- Has information been copied or disclosed?

Step 4 – Notify Appropriate Parties

Depending on the circumstances, notifications may include:

- Affected individuals
- Municipal insurer
- IT service provider
- Legal counsel
- Saskatchewan Information and Privacy Commissioner (where appropriate)
- Law enforcement (if criminal activity is suspected)

Notifications should occur as soon as practical after containment and assessment.

Step 5 – Investigate

The Administrator shall document:

- Cause of breach
- Timeline
- Information affected
- Number of affected individuals
- Actions taken
- Costs incurred

- Recommendations

Step 6 – Recovery

Recovery activities may include:

- Restoring backups
- Password resets
- Security updates
- Malware removal
- Monitoring systems
- Additional staff training

Step 7 – Prevention

Following every breach, the municipality shall review:

- Policies
- Procedures
- Staff training
- Physical security
- Cybersecurity controls
- Vendor practices

Corrective actions shall be documented.

8. Notification Guidelines

Affected individuals should be notified when the breach could reasonably result in:

- Identity theft
- Financial loss
- Fraud
- Harm to reputation
- Unauthorized access to accounts
- Loss of privacy

Notification should include:

- What happened
- Information affected
- What the municipality has done
- What individuals should do
- Contact information for questions

9. Documentation

The Administrator shall maintain a confidential Data Breach Register containing:

- Incident number
- Date
- Description
- Information involved
- Individuals affected
- Investigation summary
- Notifications made
- Corrective actions
- Date closed

Records shall be retained in accordance with the municipal records retention bylaw.

10. Training

Employees shall receive training:

- Upon hiring
- When policies change
- Following significant breaches
- At least annually where practical

Training should include:

- Password security
- Phishing awareness
- Safe email practices
- Confidential information handling
- Reporting procedures

11. Security Measures

The RM will implement reasonable safeguards including:

Administrative:

- Employee confidentiality obligations
- Access controls
- Staff training

Physical:

- Locked offices
- Secure filing cabinets
- Visitor controls

Technical:

- Multi-factor authentication where available
- Antivirus software
- Firewalls
- Regular backups
- Software updates
- Strong passwords
- Encrypted devices where practical

12. Policy Review

This policy shall be reviewed:

- Every two years
- Following a significant breach
- Following legislative changes
- As recommended by Council

Appendix A – Data Breach Reporting Form

Date of Incident: _____

Date Reported: _____

Reported By: _____

Department: _____

Description of Incident

Information Involved

☐ Employee Information
☐ Taxpayer Information
☐ Vendor Information
☐ Financial Records
☐ Email
☐ Paper Records
☐ Other

Number of Individuals Potentially Affected

Immediate Actions Taken

Was IT Contacted?

☐ Yes
☐ No

Administrator Signature: _____

Date: _____

Appendix B – Data Breach Investigation Checklist

Task	Completed
Breach reported	☐
Systems secured	☐
Passwords changed	☐
IT contacted	☐
Evidence preserved	☐
Risk assessed	☐
Individuals identified	☐
Notifications completed	☐
Insurer notified	☐
Investigation completed	☐
Corrective actions implemented	☐
Council informed (if required)	☐
Incident closed	☐

Appendix C – Employee Reporting Procedure

If you believe information has been lost, stolen, emailed incorrectly, accessed without authorization, or exposed in any way:

1. Notify the Administrator immediately.
2. Do not attempt to hide or delete evidence.
3. If electronic, disconnect the affected device from the network if safe to do so.
4. Preserve all emails and documents related to the incident.
5. Cooperate fully with the investigation.
6. Do not discuss the incident with anyone outside the investigation unless authorized.