Privacy Breach Response Policy

1. PURPOSE

The purpose of this Policy is to establish the Township's framework for identifying, containing, investigating, assessing, reporting, and responding to actual or suspected privacy breaches involving personal information. The Township is committed to protecting personal information entrusted to it and ensuring that privacy breaches are managed in a timely, consistent, transparent, and accountable manner.

This Policy is guided by:

- The Municipal Freedom of Information and Protection of Privacy Act (MFIPPA);
- Applicable regulations;
- Guidance and recommendations issued by the Information and Privacy Commissioner of Ontario (IPC); and
- Established privacy and information security best practices.

This Policy establishes procedures to:

- Minimize harm to affected individuals;
- Ensure prompt containment of privacy breaches;
- Assess whether a breach creates a real risk of significant harm;
- Determine notification and reporting obligations;
- Document decisions and response actions; and
- Implement corrective measures to prevent recurrence.

This Policy applies to:

- All Township employees;
- Members of Council;
- Appointed officials;
- Volunteers;
- Contractors, consultants, and service providers;
- All Township departments and operational units;
- All records containing personal information, including paper, electronic, audio, video, and cloud-based records; and
- All information systems, applications, artificial intelligence systems, automated tools, and third-party platforms used to process personal information.

This Policy applies to both suspected and confirmed privacy breaches.

2. DEFINITIONS

"Personal Information" means recorded information about an identifiable individual as defined under MFIPPA.

"Privacy Breach" means an incident involving the unauthorized collection, access, use, disclosure, retention, loss, or destruction of personal information contrary to MFIPPA, applicable law, Township policy, or established procedures.

Examples include:

- Unauthorized access to personal information;
- Unauthorized disclosure by email, mail, verbal communication, or electronic transmission;
- Lost or stolen documents, devices, or storage media;
- Cybersecurity incidents, including phishing, malware, ransomware, or hacking;
- Improper disposal of records;
- Unauthorized access by employees, contractors, or third parties;
- Improper use of personal information; and
- Unauthorized disclosure through artificial intelligence tools or automated systems.

A privacy breach may be accidental or intentional.

"Suspected Privacy Breach" is an event where there is reason to believe that personal information may have been accessed, used, disclosed, lost, or compromised without authorization.

"Real Risk of Significant Harm (RROSH)" means a real risk that a breach could result in significant harm to an affected individual, including bodily harm, humiliation, damage to reputation or relationships, loss of employment or business opportunities, or financial loss.

Potential harms include:

- Identity theft or fraud;
- Financial loss;
- Physical harm or safety risks;
- Emotional distress;
- Reputational harm;
- Discrimination or embarrassment;

- Loss of employment, professional, educational, or personal opportunities;
- Exposure of sensitive personal circumstances; or
- Increased risk to vulnerable individuals.

"Head" means the head of the institution as defined under MFIPPA, or an individual authorized to exercise delegated authority on behalf of the Head.

"Privacy Officer" is the Township official responsible for co-ordinating privacy compliance activities, including privacy breach response, investigations, documentation, and liaison with the IPC. The Privacy Officer acts in an advisory and co-ordinating capacity and does not replace the statutory authority or responsibilities of the Head under MFIPPA.

"Privacy Breach Response Team" is the group of Township personnel responsible for co-ordinating breach response activities. Membership may include:

- Privacy Officer;
- Clerk or designate;
- Information Technology representatives;
- Records management personnel;
- Communications personnel;
- Legal counsel; and
- Other subject matter experts as required.

3. PRIVACY BREACH RESPONSE PRINCIPLES

The Township shall respond to privacy breaches according to the following principles:

- Immediate containment of unauthorized access, use, or disclosure;
- Protection of affected individuals;
- Prompt assessment of risk and potential harm;
- Accountability and transparency;
- Compliance with MFIPPA and IPC guidance;
- Appropriate notification where required;
- Accurate documentation of all decisions and actions; and
- Continuous improvement of privacy safeguards.

4. REPORTING A PRIVACY BREACH

4.1 Duty to Report

All employees, Council members, volunteers, contractors, and service providers must immediately report any suspected or confirmed privacy breach.

Reports shall be made to:

- The employee's supervisor;
- The Privacy Officer; and/or
- Designated Information Technology or records management personnel.

Employees are not expected to determine whether a breach has occurred before reporting.

5. IMMEDIATE CONTAINMENT

5.1 Requirement to Contain

Upon discovery or suspicion of a privacy breach, immediate action shall be taken to contain the breach and prevent further unauthorized access, use, or disclosure. Containment shall begin without waiting for completion of the investigation.

5.2 Containment Measures

Depending on the circumstances, containment measures may include:

- Securing affected records or locations;
- Retrieving improperly disclosed information where possible;
- Requesting deletion or return of information disclosed to unauthorized recipients;
- Isolating affected systems;
- Disabling compromised accounts;
- Revoking access privileges;
- Changing passwords or credentials;
- Preserving evidence;
- Restricting further disclosure; and
- Notifying appropriate technical or administrative personnel.

6. PRIVACY BREACH INVESTIGATION

6.1 Investigation Responsibility

All suspected or confirmed privacy breaches shall be investigated under the direction of the Privacy Officer. The Privacy Officer co-ordinates the investigation and response process. Statutory responsibilities under MFIPPA remain with the Head of Institution.

6.2 Investigation Objectives

The investigation shall determine:

- What occurred and when;
- How the breach occurred;
- The type of personal information involved;
- The sensitivity of the information;
- The individuals affected or potentially affected;
- The extent of unauthorized access, use, disclosure, retention, copying, or distribution;
- Whether the information remains at risk;
- Whether unauthorized recipients have retained or further disclosed information;
- Whether notification obligations exist; and
- Required corrective actions.

6.3 Investigation Activities

The investigation may include:

- Interviews with individuals involved;
- Review of system logs and access records;
- Examination of emails and electronic records;
- Review of physical record handling procedures;
- Consultation with IT security personnel;
- Consultation with vendors or service providers;
- Legal review where appropriate; and
- Assessment of existing privacy and security controls.

6.4 Investigation Documentation

The investigation record shall include:

- Date and time the breach occurred, if known;
- Date discovered;
- Timeline of events;
- Nature and scope of the breach;
- Information involved;
- Individuals affected;
- Evidence reviewed;
- Decisions made;
- Notifications issued; and
- Corrective actions taken.

7. PRIVACY BREACH RISK ASSESSMENT

7.1 Assessment Requirement

Every confirmed privacy breach shall be assessed to determine:

- Whether a real risk of significant harm exists;
- Whether affected individuals should be notified;
- Whether notification to the IPC is required or appropriate; and
- Whether additional mitigation measures are required.

7.2 Assessment Factors

The Township shall consider:

- Sensitivity of the personal information;
- Number of individuals affected;
- Likelihood that the information has been, is being, or will be misused;
- Nature of the unauthorized access, use, or disclosure;
- Whether the information has been recovered or contained;
- Whether the breach resulted from unauthorized internal or external activity;
- Availability of measures individuals can take to reduce harm;
- Whether the breach is systemic or recurring; and
- Applicable MFIPPA requirements and IPC guidance.

7.3 Risk Assessment Record

The Privacy Officer shall maintain documentation of the assessment, including:

- Summary of the incident;
- Risk analysis;
- RROSH determination;
- Notification decision;
- Reasoning supporting the decision; and
- Approval or review by appropriate Township officials.

8. NOTIFICATION REQUIREMENTS

8.1 Notification to the IPC

Where a privacy breach involves a real risk of significant harm (RROSH), the Township shall legally notify the Information and Privacy Commissioner of Ontario (IPC) as soon as practicable.

The Privacy Officer, or designate, shall complete the IPC's *Report a Privacy Breach at Your Organization* form and provide all available information regarding the breach.

The notification shall include available information regarding:

- The nature of the breach;
- Personal information affected;
- Number of individuals affected;
- Circumstances of the breach;
- Containment measures;
- Corrective actions; and
- Contact information for Township representatives.

8.2 Notification to Affected Individuals

Where a privacy breach creates a real risk of significant harm, the Township shall notify affected individuals as soon as reasonably practicable.

Notification shall include:

- A description of the breach;
- Date or timeframe of the breach, where known;
- Type of personal information involved;

- Steps taken to contain and address the breach;
- Recommended actions individuals may take to reduce potential harm;
- Township contact information; and
- Information regarding the right to make a complaint to the IPC.

Notifications shall be written in clear and plain language.

8.3 Method of Notification

The Township shall generally provide direct notification to affected individuals.

Indirect notification may be considered only where direct notification is impractical or inappropriate, including situations involving:

- Large numbers of affected individuals;
- Inability to identify affected individuals;
- Inaccurate or unavailable contact information; or
- Other exceptional circumstances.

The rationale for indirect notification shall be documented.

9. THIRD-PARTY AND VENDOR BREACHES

Where contractual arrangements permit, the Township shall require third-party service providers, contractors, or vendors involved in a privacy breach to:

- Immediate notification to the Township (without undue delay);
- Co-operation with investigation activities;
- Disclosure of the scope and impact of the breach;
- Preservation of evidence;
- Assistance with notification requirements; and
- Implementation of corrective measures.

Contracts should include appropriate privacy, confidentiality, security, and breach notification obligations.

10. CORRECTIVE AND PREVENTATIVE MEASURES

10.1 Remediation

Following investigation, the Township shall implement appropriate corrective actions, which may include:

- System security improvements;
- Access control changes;
- Credential resets;
- Data recovery or secure destruction;
- Policy updates;
- Process improvements; and
- Additional safeguards.

10.2 Prevention of Recurrence

Preventative measures may include:

- Privacy and security training;
- Updated procedures;
- Enhanced monitoring;
- Improved vendor controls;
- Technology upgrades;
- Encryption improvements; and
- Additional audits or reviews.

10.3 Disciplinary Measures

Where a breach results from negligence, misconduct, or failure to follow Township requirements, appropriate disciplinary or contractual action may be taken.

10.4 Post-Incident Review

Significant breaches shall undergo a post-incident review to evaluate:

- Root causes;
- Effectiveness of the response;
- Adequacy of safeguards;
- Employee awareness and training;
- Vendor controls;
- Policy effectiveness; and
- Required improvements.

11. PRIVACY BREACH RECORDS AND ACCOUNTABILITY

The Township shall maintain a confidential Privacy Breach Log. The log shall document:

- Date and nature of the breach;

- Personal information involved;
- Individuals affected;
- Risk assessment;
- Notifications provided;
- Response actions;
- Corrective measures; and
- Final outcome.

Records shall be retained in accordance with Township retention schedules, MFIPPA requirements, and applicable records management practices.

12. POLICY REVIEW

This Policy shall be reviewed periodically to ensure continued alignment with MFIPPA, Information and Privacy Commissioner of Ontario (IPC) guidance and decisions, privacy protection requirements, cybersecurity best practices, emerging technologies, and municipal operational needs. The Township shall update this Policy as required to maintain effective privacy breach management practices.

13. EFFECTIVE DATE

This Policy comes into effect on the date approved by Council.