Vendor Privacy and Security Standard Policy

1. PURPOSE

The purpose of this Policy is to establish a comprehensive, risk-based framework governing all vendors, contractors, consultants, service providers, and technology partners (collectively "Vendors") who collect, access, store, process, transmit, or dispose of personal information or municipal records on behalf of the Township of Armour ("the Township").

2. SCOPE

This Policy applies to:

- Cloud service providers and SaaS platforms
- IT service providers and managed service contractors
- Professional consultants and operational contractors
- Communications, marketing, and social media service providers
- Any third-party handling records in the custody or control of the Township

This Policy is designed to ensure compliance with:

- The Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
- Applicable IPC guidance on third-party service providers
- Municipal procurement and accountability standards
- Privacy-by-design and security-by-default principles

3. DEFINITIONS

For the purposes of this Policy:

"Artificial Intelligence (AI)" means a machine-based system that uses data and computational methods to infer how to generate predictions, content, recommendations, decisions, or other outputs that can influence physical or digital environments. AI systems may operate with varying degrees of autonomy and may adapt after deployment. For the purposes of this Privacy Management Program, AI includes systems used to collect, analyze, infer, generate, or otherwise process personal information, including machine learning, generative AI, and AI-supported automated decision-making tools.

"Machine Learning" means technology that enables computer systems to identify patterns in data, learn from experience, and improve performance or make predictions without being explicitly programmed for each specific task. Examples include systems that automatically classify documents, identify trends in data, detect unusual activity, provide recommendations, or assist with tasks such as speech recognition and image analysis.

"Personal Information" means recorded information about an identifiable individual as defined by applicable privacy legislation.

"Records" means recorded information in any format, including paper and electronic records, created, received, or maintained by or on behalf of the Township.

"Real Risk of Significant Harm (RROSH)" means the threshold used to assess privacy breaches, defined as a real risk of significant harm—such as identity theft, physical harm, humiliation, damage to reputation or relationships, or financial loss—arising from the unauthorized access, use, or disclosure of personal information.

"Security Incident" means any event that compromises or may compromise the confidentiality, integrity, or availability of Township information or systems.

"Township Information" means all records and information created, collected, received, accessed, used, stored, processed, transmitted, retained, or disposed of by or on behalf of the Township.

"Vendor" means any contractor, consultant, service provider, supplier, technology provider, or subcontractor that provides services to the Township and has access to Township information or systems.

"Privacy Breach" means the unauthorized access, collection, use, disclosure, loss, alteration, retention, or destruction of personal information.

4. LEGISLATIVE AUTHORITY

This Policy is established pursuant to the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) and shall be administered in accordance with applicable legislation, regulations, municipal policies, records retention requirements, and guidance issued by the Information and Privacy Commissioner of Ontario.

Where legislation imposes more stringent privacy requirements, those requirements shall prevail.

5. RESPONSIBILITIES

Council approves this Policy.

Department Managers are responsible for identifying vendor engagements involving Township information and ensuring compliance with this Policy.

The Clerk/Privacy Officer provides privacy guidance, supports privacy risk assessments, and advises on compliance with MFIPPA.

Procurement ensures appropriate privacy and security requirements are incorporated into procurement documents and agreements.

Information Technology provides technical guidance on information security and technology risks, where applicable.

Vendors are responsible for complying with this Policy and all applicable contractual privacy, security, and confidentiality obligations.

6. VENDOR PRIVACY AND SECURITY PRINCIPLES

All Vendors shall conduct their activities in accordance with the following principles.

6.1 Accountability

Vendors are accountable for protecting all Township information entrusted to them and shall maintain appropriate administrative, technical, and physical safeguards throughout the duration of the contractual relationship.

Compliance with this Standard does not relieve a Vendor of any contractual, statutory, or professional obligations.

6.2 Authorized Collection, Use and Disclosure

Township information shall be collected, accessed, used, disclosed, processed, retained, and disposed of solely for the purposes authorized by the Township and only to the extent necessary to fulfill the applicable contractual obligations.

Information shall not be used for secondary purposes without the Township's prior written authorization.

6.3 Data Minimization

Vendors shall limit the collection, access, use, retention, and disclosure of personal information to the minimum amount reasonably necessary to perform the contracted services.

Where practical, Vendors shall employ privacy-enhancing techniques including anonymization, de-identification, or masking to reduce privacy risks.

6.4 Need-to-Know Access

Access to Township information shall be restricted to personnel whose duties require such access. Vendors shall implement role-based access controls, least-privilege principles, and appropriate authentication mechanisms to prevent unauthorized access.

Access permissions shall be reviewed regularly and promptly revoked when no longer required.

6.5 Security Safeguards

Vendors shall implement safeguards appropriate to the sensitivity, volume, and risk associated with Township information.

Safeguards shall include administrative, technical, and physical measures designed to protect information against unauthorized access, collection, use, disclosure, alteration, destruction, loss, theft, or unavailability.

6.6 Transparency

Vendors shall maintain documented privacy, information security, records management, and incident response practices and shall provide relevant documentation to the Township upon reasonable request.

Vendors shall promptly notify the Township of any material changes to practices that could affect the privacy or security of Township information.

6.7 Privacy by Design and Security by Default

Where technologies or services are developed, implemented, configured, or maintained on behalf of the Township, Vendors shall incorporate privacy and security considerations throughout the system lifecycle.

Default configurations shall protect personal information to the greatest extent reasonably practicable without requiring unnecessary user intervention.

6.8 Risk-Based Information Management

Privacy and security safeguards shall be proportionate to the sensitivity of the information, the likelihood and severity of potential harm, operational requirements, and recognized industry practices.

Higher-risk information shall receive enhanced protection commensurate with the level of risk.

6.9 Continuous Improvement

Vendors shall periodically review and improve their privacy and information security practices to address evolving threats, technological developments, operational changes, and emerging risks.

Where deficiencies are identified, Vendors shall implement corrective measures within reasonable timeframes agreed upon with the Township.

7. VENDOR PRIVACY AND SECURITY REQUIREMENTS

7.1 Contractual Requirements

Vendor agreements involving Township information shall include appropriate privacy, security, confidentiality, and records management requirements based on the nature of the services provided and the sensitivity of the information involved.

7.2 Data Ownership and Control

All Township information remains under the custody and control of the Township. Vendors acquire no ownership rights or independent authority over Township information and shall retain such information only as necessary to provide contracted services or as otherwise required by law.

7.3 Security Safeguards

Vendors shall implement reasonable administrative, technical, and physical safeguards appropriate to the sensitivity and risk of Township information.

Safeguards shall include, where applicable:

- access controls based on least privilege;
- appropriate authentication measures, including multi-factor authentication where required;
- encryption of information in transit and at rest;
- security monitoring and audit logging;
- vulnerability management and security updates; and
- protection against unauthorized access, disclosure, alteration, loss, or destruction.

7.4 Vendor Personnel Requirements

Vendors shall ensure personnel with access to Township information:

- are authorized and require access to perform assigned duties;
- are subject to confidentiality obligations;
- receive appropriate privacy and security training; and
- have access removed promptly when no longer required.

7.5 Privacy Breaches and Security Incidents

Vendors shall notify the Township without undue delay, and no later than within 24 hours, upon becoming aware of any actual or suspected privacy breach or security incident involving Township information.

Vendors shall:

- provide comprehensive impact details, data volume metrics, and sufficient information necessary for the Township to conduct its Real Risk of Significant Harm (RROSH) assessment and satisfy mandatory reporting obligations to the Information and Privacy Commissioner of Ontario (IPC); co-operate with investigation, containment, and remediation activities;
- preserve relevant records, logs, and evidence; and
- provide documentation of actions taken.

7.6 Subcontractors

Vendors shall obtain approval before granting subcontractors access to Township information where required by contract.

Subcontractors shall be subject to privacy, security, confidentiality, and records management obligations equivalent to those imposed on the primary Vendor.

Vendors remain responsible for the actions and compliance of all approved subcontractors.

8. VENDOR RISK MANAGEMENT AND OVERSIGHT

8.1 Due Diligence

The Township may assess Vendor privacy and security practices before entering into an agreement or implementing a service.

Assessments may consider:

- sensitivity and volume of information involved;
- security safeguards;
- data storage and processing locations;
- subcontractor arrangements;
- incident response capabilities; and
- relevant certifications or independent assessments.

8.2 Privacy and Security Assessments

The Township may require a Privacy Impact Assessment (PIA) and/or other privacy, security, or technology assessments for services involving higher-risk information, new technologies, cloud services, artificial intelligence, automated processing, or significant changes to existing services.

Vendors shall provide information reasonably required to support such assessments.

8.3 Audit and Compliance Verification

The Township may conduct reasonable and proportionate compliance reviews to confirm Vendor adherence to contractual and policy requirements.

Oversight activities may include:

- review of relevant documentation;
- review of security certifications or assessments;
- verification of applicable controls; and
- review of records relating to Township information.

The Township shall exercise oversight in a manner that considers Vendor confidentiality, security requirements, and operational constraints. Where possible, the Township may rely on current third-party certifications, audit reports, or assessments provided by the Vendor.

8.4 Vendor Cooperation

Vendors shall cooperate with reasonable Township compliance reviews and address identified deficiencies within agreed timelines.

9. CLOUD SERVICES AND TECHNOLOGY PROVIDERS

9.1 General Requirements

Cloud service providers, SaaS providers, and technology Vendors shall ensure Township information is securely stored, processed, accessed, and protected.

Providers shall maintain:

- appropriate access controls;
- security monitoring and logging;
- system availability and reliability measures;
- backup and recovery capabilities; and
- processes supporting secure data export and transition.

9.2 DATA RESIDENCY AND CROSS-BORDER PROCESSING

The Township prefers that personal information be stored and processed within Canada where reasonably practicable.

Vendors shall disclose:

- locations where Township information is stored or processed;
- any cross-border data flows; and
- material changes to storage or processing locations.

9.3 Artificial Intelligence and Automated Processing

Vendors using artificial intelligence, machine learning, or automated processing involving Township information shall:

- disclose such use to the Township;
- protect Township information from unauthorized use or disclosure;
- not use Township information to train publicly available or shared models without written authorization; and
- provide reasonable information regarding how such technologies process Township information.

9.4 Business Continuity and Disaster Recovery

Technology Vendors shall maintain appropriate business continuity and disaster recovery measures to support the availability and recovery of Township information and services.

Where appropriate, Vendors shall periodically test recovery procedures and address identified deficiencies.

10. Records Lifecycle and Retention Requirements

10.1 Retention Requirements

Vendors shall manage Township information in accordance with applicable Township retention requirements and contractual obligations.

Where reasonably practicable, Vendor retention practices shall align with Township requirements.

10.2 Lifecycle Management

Vendors shall support the appropriate management of Township information throughout its lifecycle, including authorized use, retention, transfer, return, and disposal.

10.3 Backups and Replication

Vendors shall maintain reasonable controls for backup and replicated copies of Township information to support security, availability, and appropriate retention practices.

10.4 Legal Holds

Where the Township provides notice of a legal hold affecting Township information, Vendors shall take reasonable steps to preserve relevant information and suspend routine deletion processes as required.

10.5 Return and Disposal

Upon completion of services, termination of an agreement, or request by the Township, Vendors shall return or securely dispose of Township information in accordance with contractual requirements and applicable obligations.

Where appropriate, Vendors shall confirm completion of return or disposal activities.

11. COMMUNICATIONS AND SOCIAL MEDIA VENDORS

Vendors acting on behalf of the Township shall follow approved communications requirements, protect Township information, and promptly report any privacy, security, or communication incidents. Vendors shall not disclose personal information, confidential information, or represent personal opinions as official Township positions.

12. CONFIDENTIALITY

Vendors shall ensure that Township information is treated as confidential and accessed only by authorized individuals for approved purposes. Confidentiality obligations shall continue following completion or termination of services.

13. NON-COMPLIANCE

Failure to comply with this Standard or contractual obligations may result in corrective action, restriction of access, or other contractual remedies.

14. REVIEW

This Standard shall be reviewed periodically to ensure continued alignment with applicable privacy, security, records management, and technology practices.

15. EFFECTIVE DATE

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