Corporate Privacy Policy

Version 1.2.1[i]

1 Purpose/Objective

The SPD Privacy and Data Protection Policy:

- Supports decision-making at SPD ('SPD' or 'the Company') by establishing guiding principles for how the Company will protect privacy, and the confidentiality of personal information (PI) and personal health information (PHI);
- Establishes a culture of privacy protection and privacy compliance, including fostering the application of 'Privacy by Design'; and
- Identifies core privacy responsibilities for SPD personnel and partners to foster co-ordination in protecting privacy.

2 Scope

This Policy applies to SPD's personnel and partners. It applies to:

- Personal Information (PI) protected by the *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F. 31 (FIPPA);
- Personal Health Information (PHI) protected by the *Personal Health Information Protection Act*, 2004, S.O. 2004, c. 3 (PHIPA); and
- Any other information that the Chief Privacy Officer (CPO) determines that the Company shall treat as PI/PHI.

SPD maintains a comprehensive set of privacy and data protection policies that are subordinate and complementary to the *SPD Privacy and Data Protection Policy*. The subordinate policies, listed in section 7, define privacy roles, responsibilities, accountabilities and requirements relevant to a given context (e.g. for the management of PHI and for PI) and may apply not only to SPD but also third party service providers.

3 Context

The Context section explains why protecting privacy is critical at SPD and introduces the sources for the Company's privacy requirements.

3.1 Protecting Privacy is Central to SPD's Mandate

Protecting privacy is not only an obligation for the Company- it's also part of its mandate. Along with providing Services and support for the effective and efficient planning, management and delivery of technology services throughout Canada, and developing professional services, strategy and operational policy, the Company's goal is to: 'protect the privacy of individuals whose personal information and/or personal health information is collected, transmitted, stored or exchanged by and through the Company, in accordance with the *Freedom of Information and*

Protection of Privacy Act, the *Personal Health Information Protection Act, 2004* and any other applicable law.'1

3.2 Company Privacy Requirements

The Company's privacy requirements derive from many sources including:

- Laws, rules, orders, regulations and by-laws, particularly its Enabling Regulation, PHIPA, FIPPA and orders made by the Information and Privacy Commissioner/ Ontario
- The Company's Memorandum of Understanding with the Minister
- Government of Ontario Directives that apply to SPD[2]
- Company policies
- Agreements
- Industry best practices
- Stakeholder expectations

The regulatory requirements that apply to any given Company activity depend on the facts and circumstances involved. SPD's subordinate privacy policies and procedures explain the regulatory requirements in detail.

3.3 Fostering a Culture of Privacy Protection

The Company believes that protecting privacy effectively involves not only complying with applicable privacy requirements but also having a strong culture of privacy protection.

This Policy mandates the Company's Privacy Protection Program. The Privacy Protection Program comprises comprehensive safeguards for PI/PHI and programs, practices, processes, tools and techniques to protect privacy proactively. SPD establishes a culture of privacy protection by maintaining and continuously improving its Privacy Protection Program.

4 Policy

The Company has established Guiding Principles for its approach to protecting privacy. Section 4.1 articulates the Guiding Principles which also serve as an interpretative tool for the policy statements that follow in section 4.2.

4.1 Guiding Principles

1. By proactively protecting privacy and PI/PHI, and fostering a culture of privacy protection, SPD:
    - Demonstrates respect for individuals' privacy rights and for its stakeholders;
    - Reduces privacy, operational and other risks for the Company and for its stakeholders, particularly the public; and
    - Builds confidence in the Company.

2. Protecting PI/PHI in accordance with the Company's privacy requirements is a core SPD business practice. The Company's privacy requirements derive not only from legal requirements but also from Company policies, industry best practices and individuals' privacy preferences.
3. The Company proactively embeds privacy protections into the design and operation of its programs, services, systems, and processes. Privacy protections shall seek to prevent privacy invasive events from occurring and shall safeguard PI/PHI throughout its lifecycle.
4. SPD personnel all play a role in protecting privacy and PI/PHI, working under the leadership of the CPO. SPD managers, including the CPO, are responsible for making sure that SPD manages privacy protection consistently and in a coordinated manner.
5. The Company employs a risk-based approach to protecting privacy. Risk management practices provide the opportunity to establish the optimum level of oversight, control and discipline to enable the Company to manage risk in changing environments and help provide the proper level of assessment that business objectives and strategies, including privacy protection, are being met.
6. The Company will continuously improve its Privacy Protection Program. It will seek opportunities to do so by learning from its stakeholders' experience and results, and by encouraging feedback and suggestions, particularly from personnel.

4.2 Policy Requirements

4.2.1 Accountability

1. The Company's Board of Directors oversees the protection of privacy at SPD.
2. The Chief Executive Officer (CEO) is responsible for managing privacy protection at the Company, including ensuring that SPD complies with applicable privacy requirements and fostering a culture of privacy protection.
3. The CEO delegates responsibility to the CPO to:
   - Lead the design and operation of the Company's Privacy Protection Program, including privacy- related governance bodies;
   - Provide advice, support and direction to personnel about privacy matters applicable to their areas of responsibility; and
   - Monitor and report on privacy protection at SPD.
4. SPD managers are responsible for achieving and demonstrating compliance with privacy requirements applicable to their areas of responsibility.
5. SPD shall provide its personnel and subcontractors with formal direction on their accountabilities, roles and responsibilities for protecting privacy. Means of providing such direction may include: training and awareness programs, agreements and written policies and procedures and job descriptions.

4.2.2 Privacy Protection Program

1. The Company shall maintain a Privacy Protection Program that comprises comprehensive and aligned safeguards for PI/PHI, and programs, practices, processes, tools and techniques that enable it to:

- Protect individuals' privacy and the confidentiality of their PI/PHI proactively and respect their privacy preferences; and
- Comply with its privacy requirements, particularly those derived from its Enabling Regulation, from PHIPA and FIPPA and the Regulations made under those Acts, and from its policies.

2. The Privacy Protection Program shall include processes, practices and tools and techniques to:
   - Build privacy and security protection into the design and operation of the Company's programs, operations and services, including business practices, systems and physical design and infrastructure;
   - Safeguard PI/PHI throughout its lifecycle;
   - Achieve, monitor, assess and enforce privacy compliance;
   - Identify and manage privacy risks proactively;
   - Train personnel and third party service providers about protecting privacy;
   - Develop and implement privacy policies, practices and standards;
   - Provide privacy services such as Privacy Impact Assessments (PIAs);
   - Manage, investigate and respond to privacy- and security- related incidents, breaches, complaints and inquiries; and
   - Engage internal and external stakeholders about privacy matters.
3. The CPO shall lead the design, implementation and operation of the Privacy Protection Program, working collaboratively with personnel.
4. SPD managers shall design, implement and operate aspects of the Privacy Protection Program applicable to their areas of responsibility, working collaboratively and proactively with the CPO.
5. Personnel and third party service providers shall seek to design privacy-protective features, including privacy defaults, into Company products, services and operations.
6. The Company shall conduct privacy and security assessments to accompany any proposals for new initiatives or changes to existing initiatives that may affect individuals' privacy.
7. At the CPO or designee's direction, SPD may extend privacy protections to information that is not subject to privacy and data protection laws, regulations or similar requirements.

4.3 SPD Policies and Practices

1. SPD's policies and practices shall:
   - Protect privacy and the confidentiality of PI/PHI while achieving the Company's other business interests and objectives (e.g. effectively facilitating the delivery of services and programs and realizing value for money); and
   - Comply with all applicable privacy requirements, in particular the Guiding Principles and Policy Requirements articulated in the Privacy and Data Protection Policy.
2. The CPO shall:

- Advise SPD managers about the privacy implications of, and requirements for, policies and practices in their areas of responsibility;
- Provide advice and support to the Shareholder during Company Strategic Policy development initiatives; and
- Establish and maintain written policies and practices that direct the design and management of the Company's Privacy Protection Program.

3. SPD managers shall:
   - Confirm that policies and practices applicable to their areas of responsibility comply with the Privacy and Data Protection Policy and any applicable subordinate privacy policies;
   - Seek advice from the CPO about the privacy implications and requirements for their policies and practices, particularly at the design stage and when making significant changes; and
   - Establish, maintain and ensure compliance with written policies and practices that protect individuals' privacy and the confidentiality of PI/PHI applicable to their areas of responsibility.
4. The CPO and Chief Security Officer (CSO) shall ensure that the Company's policies and practices that protect individuals' privacy and the confidentiality of their PI/PHI are comprehensive, aligned and complementary.
5. The Company shall comply with its policies and practices that protect individuals' privacy and the confidentiality of PI/PHI.
6. The Company may consult with external and internal stakeholders in the development of its policies and practices that protect privacy and the confidentiality of PI/PHI.

4.4 Privacy Training and Awareness

1. The CPO shall provide a foundational privacy training program suitable for all personnel and subcontractors. The CPO shall review and update the program annually at a minimum to address any substantive changes to SPD's privacy requirements and any other relevant matters.
2. The CPO, supported by the Privacy Office, shall develop and provide role-based privacy training for personnel commensurate with their responsibilities and whether or not personnel may have access to PI/PHI.
3. The Privacy Office shall deliver or make available role-based privacy training for personnel and subcontractors with access to, or the potential to access PI/PHI on the SPD network, in accordance with the SPD Personnel Information Protection Privacy Policy and the SPD Personnel Health Information Protection Privacy Policy.
4. Personnel shall:
   - Agree to the SPD Privacy and Security Acknowledgement and Agreement prior to commencing their work with the Company;
   - Complete foundational privacy training, Privacy and Security Fundamentals, within thirty (30) days of beginning work at SPD, and annually thereafter; and
   - Undertake role-based privacy training as directed by SPD managers.

5. Subcontractors shall:
    - Agree to the SPD Privacy and Security Acknowledgement and Agreement prior to commencing their work with the Company;
    - Complete privacy training as directed by SPD managers.
6. The Vice President, Human Resources shall:
    - Implement procedures to enable personnel and third party service providers to agree to the SPD Privacy and Security Acknowledgement and Agreement and complete required privacy training in a timely manner; and
    - Provide regular compliance reports to SPD managers and to the CPO.
7. SPD managers shall ensure that personnel or third party service providers reporting to them meet their privacy training requirements.

4.5 Working with Subcontractors

1. SPD shall enter into signed, written agreements with Subcontractors that include appropriate privacy requirements prior to the Subcontractors providing services or goods to the Company.
2. With guidance from the CPO, shall maintain standard content about privacy for procurement templates (e.g. privacy requirements, assessment and scoring criteria) and for agreements with Subcontractors. The CPO shall periodically review and update the standard content.
3. The Company shall modify the standard content to reflect the nature of the services or goods that a subcontractor will deliver, any specific privacy requirements arising and the associated privacy-related risks.

4.6 Protecting PI/PHI

1. SPD shall protect PI/PHI with technical, administrative, and physical safeguards that:
    - Are appropriate to the information's sensitivity, the format in which it is held, and the related privacy risks; and
    - Secure the PI/PHI against: theft, loss, unauthorized access, collection, use or disclosure and unauthorized copying, modification, retention or disposal.
2. Personnel and third party service providers shall not access PI/PHI unless:

4.7 Openness

1. Access is necessary in order to perform their roles;
    - They have been authorized to do so by their SPD manager, the system owner and with the requisite authority from the Privacy Office and Security Services;
    - They agree to the SPD Privacy and Security Acknowledgement and Agreement and completed applicable privacy training;
    - They have formally agreed to comply with any additional privacy-related requirements and restrictions established by SPD; and
    - They are in compliance with all applicable Company policies.

2. The Company shall publish its privacy policies and practices on its website and make copies of them available through the Privacy Office. For the benefit of clarity, the Company shall not publish or make available policies or practices if doing so could compromise the security of PI/PHI or would reveal a trade secret or confidential scientific, technical, commercial or labour relations information.
3. SPD shall publish the CPO or designee's name, title and contact information on its website and advise individuals of this information on request.
4. SPD shall publish summaries of the results of privacy assessments carried out on SPD's services when SPD is providing services.

4.8 Monitoring Compliance and Performance

1. SPD shall conduct privacy compliance reviews and maintain privacy-related performance metrics on a basis and schedule set by the CPO. Regular reports will be provided to the CEO and a report shall be provided not less than annually to the Company's Board of Directors.

4.9 Complaints and Inquiries

1. The CPO shall manage and respond to complaints, questions and feedback about the Company's privacy practices.
2. The Company shall review, investigate and document every complaint received and shall monitor for any trends arising.
3. If the sender provides contact information, the Company shall:
   - Acknowledge the complaint, question or feedback within five (5) business days of receipt and provide information about any relevant internal and external complaint mechanisms;
   - Respond to the sender's question, feedback or complaint within thirty (30) business days of receipt; and
   - Notify the sender of its expected timeframe for responding if it anticipates a delay arising.
4. The Company shall take appropriate measures to respond to complaints and feedback, which may include changing its policies and practices.
5. The Company shall provide a means for personnel to share privacy-related concerns in confidence and shall ensure that reporting personnel suffer no reprisals.

4.10 Non-Compliance

1. SPD shall take appropriate remedial action to address non-compliance with its privacy requirements.
2. The consequences of non-compliance or for failing to take appropriate remedial action shall be consistent with the Company's disciplinary and procurement policies and procedures and may include invoking measures up to and including dismissal or termination of contract.

[i] This policy is a subset of and subordinate to: Corporate Privacy and Data Protection Policy Ver. 1.2