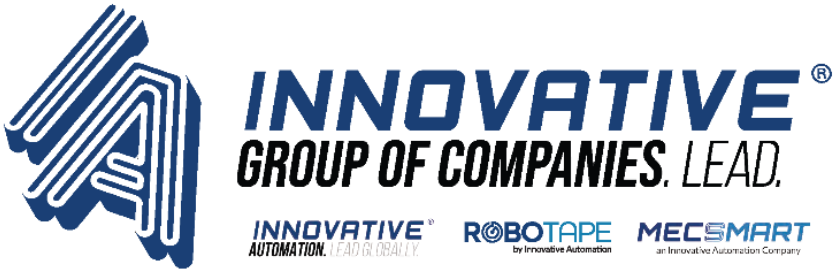

Supplier Information Security Policy

PL-3.6.1.0-21

Rev.: 1

Date: 20-Apr-26

Revision History		
Date	Rev.	Revision Description
15-Nov-24	0	Initial draft
20-Apr-26	1	Cleanup/Clarity; Added cloud services accountability section to clarify IGC responsibility

Contents

Purpose

This policy ensures that all suppliers comply with the organization's security policy, data protection, and operational requirements to safeguard company information, maintain service integrity and availability in alignment with ISO 27001:2022 and GDPR standards.

Scope

This policy applies to all suppliers providing goods or services to the organization, and to internal stakeholders involved in selecting, onboarding, and managing suppliers (including IGC Purchasing and IT). IT/Cloud suppliers are categorized based on risk, criticality, and access to sensitive information. Security requirements are tailored to the supplier's risk and the services provided.

Definitions

Confidential Data

Any information or material that is proprietary, commercially valuable, sensitive, or otherwise protected by the organization. This includes, but is not limited to, technical information, business plans, customer and supplier lists, financial information, and any other data whose unauthorized disclosure could adversely impact the organization's interests. Confidential data does not include information that is publicly available, lawfully acquired from other sources without restriction, or independently developed without reference to the organization's confidential information.

Personal Data

Any information relating to an identified or identifiable natural person ("data subject"). An identifiable person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

Personally Identifiable Information (PII)

Any information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. PII includes, but is not limited to, full name, home address, email address, social insurance number, passport number, driver's license number, biometric records, financial account numbers, and any other data that can uniquely identify an individual. PII is a subset of personal data and is subject to strict protection requirements under GDPR, PIPEDA and organizational policies.

General Data Protection Regulation (GDPR)

The European Union (EU) and European Economic Area (EEA) data protection law (Regulation (EU) 2016/679) that governs the processing of personal data, including requirements for lawful processing, data subject rights, security safeguards, breach notification, and cross-border data transfers.

Personal Information Protection and Electronic Documents Act (PIPEDA)

A Canadian federal privacy law that governs how private-sector organizations collect, use, and disclose personal information in the course of commercial activities, including requirements for consent, safeguarding, access and correction rights, and accountability.

Supplier Obligations

General Requirements (All Suppliers)

Information Handling & Confidentiality

- All organization information and data (in any form) must be treated as confidential unless the organization explicitly classifies it otherwise in writing.
- Suppliers must use organization information only for the purpose of providing the contracted goods/services and must restrict access to supplier personnel who have a legitimate need-to-know and are bound by confidentiality obligations.
- Suppliers must not disclose, share, sell, publish, or otherwise make organization information available to any third party, except to subcontractors engaged to perform the contracted services on a need-to-know basis. Any such subcontractor must be bound by written "flow-down" terms requiring confidentiality, restrictions on use and disclosure, and information security obligations at least as protective as those that apply to the supplier. The supplier remains responsible for the acts and omissions of its subcontractors.
- Suppliers must protect organization information using appropriate administrative, technical, and physical safeguards (e.g., secure storage, controlled access, secure transmission, and secure disposal) to prevent unauthorized access, use, disclosure, alteration, or loss.
- Suppliers must retain organization information (including technical data such as CAD drawings, specifications, and "math data") only as long as needed to perform the applicable work (e.g., a purchase order/work order) and in accordance with contract terms and applicable legal/regulatory requirements.
- Upon termination of the contract or completion of services, suppliers must securely destroy organization data and retain proof of destruction.
- Suppliers must report security incidents in accordance with the **Incident Management** section of this policy (including required timelines and contacts).
- Suppliers must cooperate with the organization to investigate, contain, remediate, and prevent recurrence of incidents, including preserving relevant logs/evidence where applicable.
- Suppliers must comply with applicable laws and regulations and any organization instructions relating to confidentiality, privacy, and secure handling of information.

IT Supplier Requirements

In addition to the general requirements above, these requirements apply to all suppliers providing IT-related goods or services.

Cloud Service Providers and Shared Responsibility

Where suppliers provide cloud-based services that process, store, or transmit IGC information, the cloud service provider is responsible for maintaining the confidentiality, integrity, and availability of services and data within the scope of their contractual and technical responsibilities, including the security of underlying infrastructure and provider-managed services.

IGC retains responsibility for the governance and oversight of information security risks associated with the use of cloud services. This includes, but is not limited to:

- Supplier due diligence and selection.
- Definition and maintenance of contractual information security requirements.
- Identity and access management within IGC-controlled environments.
- Data classification and determination of appropriate use of cloud services.
- Configuration decisions within tenant or customer-managed controls.
- Monitoring security notifications, advisories, and assurance reports provided by the supplier.
- Ensuring that any confidentiality, integrity, or availability incidents affecting IGC information are promptly disclosed by the supplier, assessed, and managed in accordance with IGC's incident management and legal or regulatory obligations.
- Outsourcing information processing or storage to cloud service providers does not remove IGC's responsibility to manage information security risk; however, it does not imply direct operational control over supplier-managed infrastructure or services.

Risk Assessment

- Suppliers shall be assessed for risk prior to engagement. IT/Cloud supplier risk assessments are performed by IT.
- Assessment includes security controls, certifications (ISO 27001, SOC 2), incident history, and compliance status.
- Suppliers are reviewed for risk annually and after any security incidents.

Service Level Agreements (SLAs)

- SLAs must meet organization's operational requirements for uptime and support

Data Requirements

- Suppliers must have a signed NDA and/or contractual confidentiality provisions that (at a minimum) restrict use to the contracted purpose, prohibit unauthorized disclosure to third parties, and require secure handling, storage, transmission, and secure disposal/destruction of organization data.

- Data residency (including cloud services):
  Organization data must be stored on servers physically located in Canada. Exceptions may be granted only for specific use, subject to approval. Exceptions must be documented, risk-accepted by the IT Manager (and Privacy/Legal if personal data/PII is involved), and reviewed annually. If the nature, type, or use of the data changes after an exception is granted, the exception must be re-evaluated and re-approved before any further processing or storage outside Canada. Cross-border transfers of personal data must comply with GDPR requirements (e.g., Standard Contractual Clauses).

- Only data necessary for service delivery should be collected and retained.

Asset Management

- Maintain inventory of all assets (hardware, software, data) handled on behalf of the organization.

Personnel Training

- Provide regular security awareness and GDPR training for supplier personnel.

Security Standards

- Secure backup processes with encryption and physical security.
- AES-256 or better for data at rest, TLS 1.2+ for data in transit.

System Development & Maintenance

- Suppliers must follow secure development practices and ensure systems are regularly updated and patched, including 3rd party development libraries.
- API keys, database connection credentials or other passwords must never be hard coded or included in source code.

Personal Data and Personally Identifiable Information (PII)

- If working with PII the supplier must comply with the requirements of the GDPR and PIPEDA.
- Suppliers must support data subject rights, including access, rectification, erasure, restriction, and portability.
- Suppliers must process personal data lawfully, fairly, and transparently, and provide clear privacy notices.
- Suppliers must ensure that all processing of personal data is based on a valid legal basis as defined by GDPR Article 6. Acceptable legal bases include: consent, contract, legal obligation, legitimate interests, vital interests, and public task. The chosen legal basis must be documented and communicated to the organization.
- Suppliers must maintain records of the legal basis for each processing activity involving personal data and provide these records to the organization upon request. Where consent is used, suppliers must ensure it is freely given, specific, informed, and unambiguous, and maintain evidence of consent.
- Supplier contracts must specify the legal basis for processing personal data and include provisions for updating the organization if the basis changes.
- Suppliers must maintain a Record of Processing Activities (ROPA) in accordance with GDPR Article 30. This record must include all required details about the processing activities performed for the organization. The record must document the name and contact details of the supplier and the organization, the purposes of processing, categories of data subjects and personal data processed, categories of recipients, data retention periods, description of technical and security measures in place. The record must be made available to the organization and relevant supervisory authorities upon request.

Access Control

- Access shall follow least privilege principles.

- Implement strict access controls and authentication measures.
- Multi-factor authentication (MFA) is required for all accounts when accessing or providing services remotely.
- No unauthorized third-party access to organization's data.
- Maintain detailed access logs

Data Protection

- No sale or sharing of organization data with third parties.
- For legal basis and transparency requirements related to personal data/PII (including GDPR Article 6), see the **Personal Data and Personally Identifiable Information (PII)** section.
- Cloud services: Business continuity and disaster recovery plans must be tailored for cloud environments.
- Cloud services (personal data): Suppliers processing personal data must sign a Data Processing Agreement (DPA) that defines security measures, confidentiality, breach notification, audit rights, and compliance with GDPR Article 28. Alternatively, at the discretion of the IT department, if the supplier's contract contains provisions that fully address the requirements of the GDPR—including but not limited to security measures, confidentiality, breach notification, audit rights, and lawful processing—then a separate DPA may not be required.

Sub-Processing

- Where suppliers engage sub-processors who will access, process, or store organization data, suppliers must ensure those sub-processors are bound by written agreements with confidentiality, restrictions on use and disclosure, and information security obligations at least as protective as those required of the supplier. The supplier remains responsible for the acts and omissions of its sub-processors.
- The Suppliers' obligations under this policy also apply to their sub-processors as well as any specific Data Processing Agreements (DPAs).
- Suppliers must conduct due diligence on sub-processors, including incident history, compliance status, regulatory requirements, security certifications etc.
- Suppliers must maintain a register of approved sub-processors, including their roles and the types of data they handle.
- Suppliers must ensure sub-processors report security incidents or data breaches within the same timeframes as required for suppliers.
- Suppliers must coordinate with sub-processors to investigate and remediate incidents.
- Upon termination of the contract or sub-processing arrangement, suppliers must ensure sub-processors securely destroy organization data and retain proof of destruction.

Incident Management

- Suppliers must report security incidents within 24 hours by contacting the IGC Purchasing contact via email and/or phone, or IT directly.
- Suppliers must cooperate in investigations and remediation.

Compliance Monitoring

- Provide evidence of compliance upon request (e.g., certifications, logs, audit reports).
- The organization reserves the right to request evidence of assurance on an annual basis, including a current SOC 2 Type II report and/or ISO 27001 certification (or equivalent), as applicable to the services provided.
- The organization reserves the right to conduct, or to require the supplier to complete, a security questionnaire and/or audit activities proportionate to the supplier's risk category and the nature of services provided.

Penalties & Enforcement

- Non-compliance may result in financial penalties up to 10% of contract value, suspension of services, or termination for cause. The organization reserves the right to seek damages for breaches.

Roles and responsibilities

IT is responsible for IT/Cloud supplier risk assessment, onboarding due diligence (technical/security), compliance monitoring, continuous improvement, and incident management. The IGC Purchasing Department coordinates supplier onboarding and serves as the primary contact for supplier incident notifications and related communications.

Policy Ownership & Review

The policy and supplier security practices will be reviewed annually or upon significant changes to regulatory requirements, changes in risk, or business operations.