



Information Security Policy

for conducting business with Natural



Information Security Policy
Version 1.0
Sep 2025

Control Sheet

Approved by:
Principal

Last Review:
Sep 2025

Next Review:
Sep 2026

Revision History:

| Version | Approved / Reviewed / Revised / Rescinded by: | Date | Comments |
|---------|---|----------|--------------------|
| 1.0 | Principal | Sep 2025 | Inaugural Version. |
| | | | |
| | | | |
| | | | |
| | | | |

** For any updates, improvement suggestions or broken links, please contact Natural.

1 Information Security Policy

Information is one of Natural's most valuable assets. This Information Security Policy establishes the principles and responsibilities required to protect the confidentiality, integrity, and availability of data managed by the company, ensuring compliance with legal obligations and maintaining the trust of clients, partners, and employees.

1.1 Purpose

The purpose of this Information Security Policy is to safeguard all data and information assets owned by or entrusted to Natural, including those of clients, employees, partners, and third parties. "Information" refers to any data received, stored, processed, created, or transmitted by Natural in the course of its operations. This policy outlines the principles and responsibilities governing the secure handling, use, and disposal of information across Natural's operations in Canada and abroad.

1.2 Audience

This policy applies to all individuals who access or manage information on behalf of Natural, including full-time and part-time employees, consultants, contractors, and third-party service providers. All parties are expected to comply with the principles and procedures outlined herein, regardless of their location or contractual status.

1.3 Policy Objectives

Natural is committed to the following objectives:

- Information shall be protected against unauthorized access, disclosure, alteration, destruction, or misuse.
- Access to information will be granted only to authorized users and approved in accordance with Natural's access control procedures.
- All staff must comply with Natural's [General Business Principles](#) and related data handling protocols, including Natural's [Use of Artificial Intelligence policy](#).
- Information will be managed in compliance with applicable legal, regulatory, and contractual obligations, including Canadian privacy laws (e.g., PIPEDA) and international standards where relevant.
- Confidentiality, integrity, and availability of information will be maintained to support service delivery and stakeholder trust.
- Information will be classified according to sensitivity and stored only in secure, approved environments.
- Personally identifiable information (PII) will be handled with strict confidentiality and in accordance with Canadian privacy standards.
- Physical and digital security measures will be implemented and maintained across all operational sites and systems.
- All information security incidents must be reported immediately to Natural.
- Employees and third parties are expected to periodically review and uphold the principles of this policy in all work activities.

1.4 Governance and Compliance

This policy is subject to regular review and updates in response to evolving cybersecurity risks, technological changes, and regulatory developments. Any breach of this policy may result in disciplinary action, up to and including termination of employment or legal proceedings.



Natural E&S Consulting Inc.
1751 Sheppard Ave East, Suite 502
Toronto, M2J 0A4
ON, Canada

 natural-consulting.ca

 [/naturalconsulting](https://www.linkedin.com/company/naturalconsulting)