Information and Data Protection Policy

Last Updated: 22 April 2025

1. Overview

At Niricson Software Inc., we are committed to safeguarding the confidentiality, integrity, and availability of all data entrusted to us.
This policy (DPP.001.000) outlines how we protect information assets, manage cybersecurity risks, and ensure compliance with data protection laws and contractual obligations.

Our security practices are built into every layer of our operations—from how we design and deploy our AUTOSPEX® platform to how we manage client infrastructure data and internal systems.

2. Purpose

The purpose of this policy is to define Niricson's approach to protecting client, employee, and partner information from unauthorized access, loss, or misuse.
We maintain a security-by-design philosophy to ensure that data protection is embedded into our technology, processes, and people.

3. Scope

This policy applies to all Niricson employees, contractors, and systems involved in the collection, processing, or storage of:

Personal information (e.g., names, contact details, login credentials)

Client-provided infrastructure data (e.g., 2D/3D models, defect vectors, geospatial metadata)

Inspection and operational data captured or processed via AUTOSPEX®

Internal corporate systems and cloud environments supporting these services

4. Core Principles

Our information and data security framework is guided by the following principles:

Confidentiality: Only authorized users can access sensitive data.

Integrity: Data is accurate, complete, and protected against unauthorized alteration.

Availability: Systems and information remain accessible to authorized users when required.

Accountability: Access and actions are logged and auditable.

Continuous Improvement: Security practices are regularly reviewed, tested, and enhanced.

5. Data Classification

All data managed by Niricson is categorized as one of the following:

Public: Information approved for external publication.

Internal: Business data not intended for external sharing.

Confidential: Client data, inspection data, or personal information.

Restricted: Highly sensitive data requiring enhanced access control and encryption.

Appropriate handling, storage, and transmission controls are applied to each classification level.

6. Security Governance

Security oversight is led by Niricson's executive and technical leadership teams.
We ensure:

Defined ownership for all systems and datasets

Documented access control policies

Regular security and privacy training for employees and contractors

Internal audits and compliance checks aligned with ISO 27001 and SOC 2-equivalent standards

7. Cybersecurity Controls

Niricson employs a layered security approach that includes:

Firewalls, VPNs, and network segmentation

Multi-factor authentication and strong password policies

Encryption of data in transit and at rest

Secure Software Development Lifecycle (SDLC) practices

Continuous vulnerability scanning and patch management

Separation of production and non-production environments

Incident response planning and threat monitoring

8. Cloud and Data Center Security

All third-party data centers and cloud platforms used by Niricson:

Comply with internationally recognized standards (ISO 27001, SOC 2, or equivalent)

Provide redundancy, fault tolerance, and high availability

Undergo security and compliance reviews prior to engagement

9. Data Sharing and Third Parties

We do not sell or rent any personal or client data.
When data is shared with trusted vendors or partners, we:

Conduct due diligence and security assessments

Require signed data protection and confidentiality agreements

Limit access to only what is necessary to perform contracted work

Monitor ongoing compliance with Niricson's standards

10. Data Protection and Privacy

Niricson’s Data Protection Policy (DPP.001.000) governs how we collect, use, store, and protect personal and client data.
We adhere to all applicable privacy laws and contractual obligations and support data subject rights, including access, correction, and deletion requests.

For more information, refer to our Privacy Policy