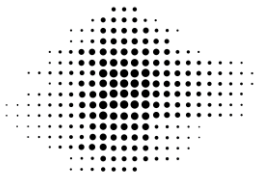

NIRICSON

# Data Protection Policy

| | |
|---|---|
| **POLICY NUMBER** | DPP.001.100 |
| **EFFECTIVE DATE** | October 2025 |
| **SUPERSEDES** | DPP.001.000 |

## Contents

## 1. Purpose

At Niricson, we are committed to protecting the data entrusted to us by our clients, partners, employees, and third parties. This Data Protection Policy outlines our principles and practices for the responsible collection, use, storage, and protection of personal data and sensitive client data. Our goal is to ensure compliance with applicable privacy laws and contractual obligations while upholding the highest standards of data security.

## 2. Scope

This policy applies to all Niricson employees, contractors, systems, and services that handle:

- Personal data
- Client-provided infrastructure data, including 2D/3D models and defect vectors
- Geospatial or structural information collected or processed through our AUTOSPEX™ platform and related services

## 3. Data We Collect

We may collect and process the following categories of data:

### 3.1 Personal Data

- Name, email, phone number, and job title
- Employment or organization-related information
- Account credentials and authentication details
- System usage data (e.g., logs, preferences, IP address)

### 3.2 Infrastructure and Inspection Data

- 2D and 3D models of physical assets
- Defect vector data and annotations
- Geotagged images and structural metadata

## 4. Lawful Basis for Processing

We only process personal data when there is a lawful basis to do so, including:

- Consent of the data subject
- Performance of a contract
- Compliance with legal obligations
- Legitimate interest pursued by Niricson that does not override individual rights

## 5. Use of Data

We use data solely for the purposes for which it was collected, including:

- Delivering and improving our services
- Responding to client and user inquiries
- Managing user accounts and access permissions
- Fulfilling legal, contractual, and security obligations

## 6. Data Sharing and Third Parties

We do not sell or rent personal or client data. Data may be shared with:

- Partners or subcontractors as needed to deliver services, under strict confidentiality obligations
- Third-party service providers under contractual data protection agreements
- Legal authorities when required by law

## 7. Protection of Client Infrastructure and Inspection Data

Although 2D/3D models and defect vector data processed by Niricson do not contain personal data, they represent sensitive infrastructure information related to assets such as dams, bridges, tunnels, and airfields.

To protect this data, Niricson:

- Enforces role-based access controls and user authentication
- Encrypts data in transit and at rest
- Adheres to secure data handling and processing procedures
- Requires personnel and third-party providers to comply with confidentiality agreements and data security protocols

This ensures we meet all regulatory, contractual, and ethical obligations for handling sensitive infrastructure data.

## 8. International Data Transfers

When transferring personal or sensitive data across borders, Niricson ensures appropriate safeguards are in place, such as adequacy decisions and standard contractual clauses.

## 9. Data Security

We apply technical and organizational controls to protect all forms of data, including:

- Encryption
- Secure network architecture
- Multi-factor authentication for privileged access
- Vulnerability scans and threat assessments

For more detailed measures, refer to Niricson's Cyber Security Policy.

## 10. Mobile Device Security and Incident Response

Niricson ensures that mobile devices used to access Niricson's corporate systems, including email, are protected with appropriate security controls and that any loss or theft of such devices is promptly reported and managed to prevent unauthorized access to company data. This subsection applies to all Niricson employees and authorized contractors who access Niricson's corporate email, files, or systems using a mobile device, whether company-issued or personally owned (BYOD).

**Device Security Controls**

- All mobile devices used to access Niricson systems must have the following security features enabled:
    - A device-level PIN, password, or biometric authentication (e.g., fingerprint or facial recognition).
    - Automatic screen lock enabled after a maximum of five (5) minutes of inactivity.
    - Full device encryption enabled.
- Access to corporate email and data must be performed exclusively through Microsoft Outlook via Microsoft 365, protected by enforced **Multi-Factor Authentication (MFA)**.
- Subcontractors are not permitted to access Niricson's corporate email or systems unless specifically authorized by the CTO.

**Lost or Stolen Device Protocol**

- If a mobile device with access to Niricson's systems is lost or stolen, the user must:

1. **Immediately report** the incident to the **People & Culture** and **Product** departments.
2. **Change their Niricson account password** from another secure device.
3. **Provide details** of the lost or stolen device, including type, ownership (company or personal), and last known location.

- The IT Cloud department will:

  - **Remotely wipe** the device via Microsoft 365 (if enrolled or connected).
  - **Revoke access** to Niricson email and other systems.
  - **Document the incident** for internal tracking and audit purposes.

**Compliance and Enforcement**

Employees must comply with this subsection when using mobile devices for any work-related purpose.

Failure to follow these requirements may result in revocation of mobile access privileges and/or disciplinary action, up to and including termination of employment.

## 11. Data Retention

We retain personal and infrastructure data only for as long as necessary to fulfill its purpose or meet regulatory requirements.

## 12. Data Subject Rights

Under applicable privacy laws, individuals may have the right to:

- Access their personal data
- Correct inaccuracies
- Request deletion of their data

Requests can be submitted to support@niricson.com

## 13. Roles and Responsibilities

All Niricson personnel are responsible for protecting data. Key roles include:

- Department Heads: Ensuring team adherence to policies
- Employees and Contractors: Following approved procedures and reporting concerns

## 14. Policy Review

This policy is reviewed annually or as needed to reflect regulatory changes, business needs, or evolving risks.

For questions about this policy or our data protection practices, please contact:
support@niricson.com