# Acceptable Use Policy

Last Updated: 22 April 2025

### 1. Overview

This Acceptable Use Policy (AUP) defines the standards of conduct required when accessing or using Niricson Software Inc. systems, networks, and services — including the AUTOSPEX® platform, associated web applications, and client data environments.

By using Niricson systems or services, users agree to comply with this policy to ensure the confidentiality, integrity, and availability of information managed within our ecosystem.

### 2. Purpose

The purpose of this policy is to:

Establish clear expectations for the appropriate use of Niricson's technology and data assets.

Protect clients, partners, and employees from security, privacy, and reputational risks.

Ensure compliance with applicable laws, regulations, and contractual obligations.

This policy supports our broader Information and Data Protection Policy frameworks.

### 3. Scope

This policy applies to:

All Niricson employees, contractors, consultants, partners, and authorized users.

Any device or network accessing Niricson resources or AUTOSPEX® systems.

All data, including personal, operational, and infrastructure inspection data processed through Niricson platforms.

## 4. General Responsibilities

Users of Niricson systems must:

Access systems and data only for authorized business purposes.

Protect login credentials and never share passwords or authentication tokens.

Report suspected security incidents, data breaches, or unauthorized access immediately.

Ensure that personal devices used for work meet Niricson's security standards (e.g., encryption, updated antivirus software).

Follow all corporate policies regarding cybersecurity, privacy, and data protection.

## 5. Prohibited Activities

To maintain the security and integrity of Niricson's systems, the following activities are strictly prohibited:

5.1 Unauthorized Access or Misuse

Gaining or attempting to gain unauthorized access to Niricson systems or client environments.

Circumventing authentication or security controls.

Using another user's credentials or sharing account access.

5.2 Malicious or Illegal Conduct

Uploading, transmitting, or storing malware, ransomware, or other harmful code.

Conducting penetration testing, scanning, or probing of Niricson networks without written authorization.

Engaging in activities that violate applicable laws, including data protection or export control regulations.

5.3 Misuse of Client Data

Downloading, copying, or sharing client infrastructure or inspection data for non-business purposes.

Disclosing confidential or proprietary information without authorization.

Using client data to train external AI models or third-party analytics tools without consent.

5.4 Misuse of Resources

Using Niricson systems for personal commercial ventures or political activities.

Excessive personal use of company networks that interferes with business operations.

Introducing unapproved software or hardware into production environments.

## 6. Data Handling Requirements

All users are responsible for ensuring that data handled within Niricson's systems is managed securely and in accordance with:

Encryption requirements for data at rest and in transit.

Access controls based on least privilege principles.

Retention limits and secure deletion procedures outlined in our Data Protection Policy.

## 7. Third-Party and Client Access

Where Niricson provides clients, partners, or third parties with access to AUTOSPEX® or related services:

Access is granted only for legitimate, contractually defined purposes.

Users must comply with this AUP and all relevant data-protection and confidentiality obligations.

Unauthorized sharing, sublicensing, or resale of access credentials is prohibited.

## 8. Monitoring and Enforcement

Niricson reserves the right to:

Monitor network traffic and system activity for security and compliance purposes.

Investigate potential violations of this policy.

Suspend or terminate accounts found to be in breach.

Report unlawful activities to regulatory or law enforcement authorities as required.

Violations may result in disciplinary action, up to and including termination of employment or contract, and potential legal action.

**9. Reporting Security Incidents**

All users must immediately report:

Suspected or confirmed data breaches.

Lost or stolen devices containing company or client information.

Phishing attempts, suspicious emails, or unauthorized access.

Reports should be sent promptly to info@niricson.com