Technical Support & Service Level Policy

Last Updated: 22 April 2025

1. Overview

This policy defines Niricson Software Inc.'s commitment to providing reliable, responsive, and secure technical support for its software platforms, including AUTOSPEX® and associated services.
Our goal is to ensure that all clients receive consistent, high-quality support that maintains system availability, data integrity, and operational efficiency.

2. Purpose

The purpose of this policy is to:

Establish the standards and processes governing technical support services.

Define the service levels, response times, and escalation procedures applicable to clients.

Reinforce Niricson's commitment to proactive system monitoring, client satisfaction, and service continuity.

This policy aligns with Niricson's Information and Data Protection Policy (DPP.001.000) to ensure all support interactions uphold strict data security and privacy standards.

3. Scope

This policy applies to:

All clients and users of Niricson's AUTOSPEX® platform and digital inspection solutions.

All Niricson employees, contractors, and support partners providing technical assistance or system maintenance.

All communication channels used for technical support, including email, ticketing systems, and service portals.

4. Support Commitment

Niricson is committed to delivering reliable service and transparent communication. Our support objectives include:

Maintaining consistent system uptime and data access.

Providing timely responses to technical inquiries and service requests.

Ensuring minimal disruption to client operations during troubleshooting or maintenance.

Continuously improving system stability, performance, and usability based on client feedback.

5. Service Availability

Niricson's AUTOSPEX® platform is designed for high availability, with redundant cloud infrastructure hosted in ISO 27001 and SOC 2-compliant environments.

Unless otherwise specified in a client agreement:

AUTOSPEX® services are available 24 hours a day, 7 days a week, 365 days a year.

Scheduled maintenance windows will be communicated at least 48 hours in advance.

Emergency maintenance may be performed as required to protect service integrity or security.

6. Support Channels

Clients can reach Niricson's technical support team through the following channels:

Email: support@niricson.com

Severity Level	Description	Resolution Target
Critical (P1)	Complete service outage, data access failure, or security incident impacting all users.	Within 24 hours or as continuously worked until resolution.
Moderate (P2)	Major feature malfunction or performance degradation impacting multiple users or core functionality.	2 business days.
Minimal (P3)	Minor issue, single-user problem, or feature not performing as expected without significant operational impact.	Within 5 business days.
Maintenance Activities and Updates (P4)	All other items. A change to the platform that is planned by Niricson.	Addressed in next scheduled update/release.

All response and resolution times are measured during standard business hours (Monday–Friday, 9:00 AM – 5:00 PM PST, excluding statutory holidays).

8. Client Responsibilities

To ensure efficient resolution, clients are expected to:

Provide accurate and detailed descriptions of issues, including steps to reproduce the problem.

Designate authorized points of contact for submitting and approving support requests.

Cooperate with Niricson's support team during diagnostic and troubleshooting processes.

Maintain their own internal connectivity and device configurations as per Niricson's technical requirements.**9. System Maintenance and Updates**

To maintain performance and security:

Niricson may deploy periodic software updates, security patches, or enhancements.

Maintenance is scheduled to minimize service impact and communicated in advance.

Updates follow a secure change management process aligned with Niricson's Secure Software Development Lifecycle (SDLC).

10. Incident Management

In the event of a major service incident:

Niricson will immediately investigate, isolate, and remediate the issue.

Clients affected by a critical or high-severity event will receive timely status updates.

Root cause analysis reports will be shared upon resolution when applicable.

11. Data Protection and Confidentiality

All support interactions are handled in accordance with Niricson's Data Protection and Cybersecurity policies.
Support staff are bound by confidentiality agreements and have access only to the systems and information necessary to resolve client issues.

Sensitive client data, such as inspection imagery or infrastructure models, is never copied, transmitted, or shared outside secure environments unless explicitly authorized.

12. Escalation Procedure

If an issue is not resolved within the target timeframe or requires additional attention:

Contact the assigned support representative or ticket owner.

Escalate to the Technical Software QA Lead if unresolved within the defined window.

Further escalation can be directed to Niricson's Chief Product Officer (CPO) for critical matters affecting service continuity.

Escalations are prioritized immediately upon receipt.

13. Service Review and Continuous Improvement

Niricson regularly evaluates its support performance against established metrics and client feedback.
We continuously improve our support processes through:

Post-incident reviews and lessons learned.

User feedback and feature enhancement requests.

Regular internal training and performance assessments.

14. Policy Review

This policy is reviewed annually or as required due to changes in:

Service offerings or infrastructure,

Regulatory or contractual obligations, or

Industry best practices.

15. Contact

For questions or assistance regarding technical support or service levels, please contact:
✉ info@niricson.com