1. Purpose

This Vulnerability Disclosure Policy ("Policy") outlines Stereotaxis's approach to receiving, evaluating, and addressing cybersecurity vulnerabilities related to its medical devices and associated systems. This Policy may be updated at any time at Stereotaxis's sole discretion. It is based on ISO/IEC 29147:2018 and reflects our commitment to transparency, patient safety, and continuous product security improvement.

2. Scope

This policy applies to:

- All software-enabled medical devices developed and distributed by Stereotaxis
- Companion software (e.g., mobile apps, cloud platforms)
- Embedded firmware and network interfaces
- Third-party security researchers, customers, healthcare providers, or any individuals reporting cybersecurity vulnerabilities related to our products

3. Principles

Stereotaxis adheres to the following vulnerability disclosure principles, as outlined in ISO/IEC 29147:

- **Coordination:** Cooperate with researchers, regulators, and partners to address reported vulnerabilities.
- **Transparency:** Provide acknowledgments and remediation updates in a timely and responsible manner.
- **Responsibility:** Protect users from potential harm by verifying and addressing valid reports efficiently.

4. Reporting a Vulnerability

Individuals or organizations who discover a potential security vulnerability must promptly report it to Stereotaxis's Product Security Team. Any delay in reporting that results in harm to patients or systems may void safe harbor protections under this policy.

Reporting Channels

- **Phone:** (314) 678-6200
- **Email:** tst@stereotaxis.com

Information to Include

Please provide the following:

- Product name, version, and model number (if applicable)
- Description of the vulnerability and its potential impact
- Your contact information (optional, but recommended)

5. Our Commitment

Upon receiving a report:

- **Acknowledgment:** We will acknowledge receipt within **5 business days**.
- **Triage:** Vulnerabilities will be assessed based on severity (using CVSS v3.1 or newer), exploitability, potential impact on patient safety or product performance, and other factors as determined by Stereotaxis in its sole discretion.
- **Response:** We will communicate remediation plans and timelines. Updates will be provided at key milestones.
- **Resolution:** Valid vulnerabilities will be addressed through security patches, product updates, or mitigation guidance.
- **Lifecycle Patch Commitment:** Stereotaxis is committed to providing timely security patches, mitigations, or updates throughout the supported lifecycle of our medical devices, consistent with regulatory requirements and patient safety obligations.

6. Coordinated Disclosure

Stereotaxis supports **coordinated vulnerability disclosure (CVD)** with researchers and regulatory bodies such as:

- **FDA** (for medical devices in the U.S.)
- **ICS-CERT** (for vulnerabilities in networked medical technologies)
- **National CERTs** or healthcare ISACs (as appropriate)

Researchers must allow Stereotaxis a **minimum 90-day window** to develop and deploy mitigations before any public disclosure. Additional time may be required for complex issues, to be determined at Stereotaxis's sole discretion.

7. Legal and Safe Harbor

We value collaboration and responsible research. Subject to compliance with all terms of this policy, Stereotaxis agrees not to initiate or recommend legal action against security researchers who:

- Follow this disclosure policy
- Conduct research in good faith

- Do not intentionally harm users or access patient data
- Refrain from exploiting vulnerabilities beyond necessary testing

8. Contact

For questions related to this policy, please contact:
Stereotaxis Call Center
Stereotaxis
Email: tst@stereotaxis.com
Phone: +1 (314) 678-6200

Last Updated: 01 October 2025