1. Purpose

1.1. Therakos is committed to protecting the confidentiality, integrity, and availability of its products and information by delivering secure solutions and promptly addressing any identified vulnerabilities. This policy outlines how security researchers and third parties can report potential issues, and how Therakos communicates verified vulnerabilities to customers.

1.2. This policy establishes guidelines for conducting security research and outlines procedures for submitting security vulnerabilities discovered.

1.3. This policy outlines which systems and types of security research are permitted, how to report vulnerabilities, and the expected timeline before public disclosure. It encourages researchers to report issues responsibly and reflects our commitment to working with them in good faith to keep users safe.

2. Scope

2.1. This policy applies to all Therakos-manufactured medical devices and public-facing websites or applications. To confirm whether a system is covered, contact cybersec@therakos.com or check the domain's WHOIS record. Unauthorized testing outside these guidelines may result in legal or regulatory action.

2.2. The following types of testing are expressly not authorized.

2.2.1. Using social engineering.

2.2.2. Using malware.

2.2.3. Phishing Attacks.

2.2.4. Changing the data accessed by exploiting the security vulnerability.

2.2.5. Compromising the system and persistently maintaining access to it.

2.2.6. Using brute force to gain access to systems.

2.2.7. Sharing security vulnerabilities with third parties.

2.2.8. Network denial of service (DoS or DDoS) tests.

2.3. Using a vulnerability for anything beyond proving its existence is prohibited; only non-intrusive methods (e.g., listing a directory) may be used for a demonstration. Physical testing, social engineering (e.g., phishing, vishing), and other non-technical methods are also strictly forbidden.

3. Policy

3.1. Guidelines

3.1.1. We encourage researchers to notify us promptly upon discovering a real or potential security issue and to allow us a reasonable timeframe to investigate and resolve it before any public disclosure.

3.1.2. Please avoid actions that could compromise user privacy, disrupt services, or damage data. Use exploits only to the extent necessary to confirm a vulnerability — never to access, extract, or manipulate data, establish persistent access, or pivot to other systems. If you encounter sensitive information (e.g., personal, financial, or proprietary data), stop testing immediately and report the findings without sharing it further.

3.1.3. Additionally, we ask that you refrain from submitting large volumes of low-quality reports; submissions should include sufficient detail as outlined in our reporting guidelines.

3.2. Authorization and Reporting Process

3.2.1. If you conduct your security research in good faith and in line with this policy, we will treat your actions as authorized and will work with you to resolve the issue promptly. In such cases, Therakos will not pursue legal action. However, we reserve all legal rights for any activity that falls outside the scope of this policy.

3.2.2. To report a potential vulnerability, please contact the Therakos Product Security Vulnerability Response Team at cybersec@theakos.com, using the subject line **VULNERABILITY DISCLOSURE**. Once your report is received, our team will follow up with you directly.

3.2.3. For confidentiality, we encourage you to encrypt any sensitive information you share. Please note that this email address is intended solely for reporting product or service security vulnerabilities related to Therakos offerings.

3.3. What to Include in Your Report - To help us assess and address your submission efficiently, please include the following details in your report

3.3.1. A clear description of the security vulnerability, where it was found, and its potential impact.

3.3.2. Step-by-step instructions to reproduce the issue, including proof-of-concept code or screenshots, if available.

3.3.3. An explanation of how the vulnerability was discovered, with enough detail for us to replicate it.

3.3.4. Evidence confirming the vulnerability's existence (e.g., screenshots, links).

3.3.5. The date and time the issue was identified.

3.3.6. Any additional information that could help us locate and resolve the issue quickly.

3.3.7. If possible, please submit your report in English.

3.4. What You Can Expect from Us

3.4.1. If you choose to share your contact details, we commit to engaging with you openly and promptly. We aim to acknowledge receipt of your report within three business days and will keep you informed throughout the investigation and remediation process.

3.4.2. We'll confirm the vulnerability when possible and maintain transparent communication, including any challenges that may affect resolution timelines.

3.5. Severity Assessment

3.5.1. Therakos uses the Common Vulnerability Scoring System (CVSS) to evaluate and communicate the severity and potential impact of reported IT security vulnerabilities, in line with industry's best practices.

3.6. Security Advisories

3.6.1. When legally or regulatorily required, Therakos will report security research findings to the appropriate authorities.

3.6.2. If a third party reports a potential vulnerability in our systems, we will investigate and may coordinate a public disclosure with them. In cases where information is received under confidentiality or embargo — such as from a supplier — we will work with that party to encourage a timely fix, though we may be limited in what details we can share.

4. Attachments

4.1. N/A

5. Revision History

Revision No.	Change Description
1	• New Therakos document (ref. MNK POLICY-0295) – removed references to Mallinckrodt, improved overall language for conciseness, updated cyber team contact email.