

1. Purpose

- 1.1. What does this document do? MALLINCKRODT PHARMACEUTICALS is dedicated to maintaining the confidentiality, integrity, and availability of Mallinckrodt's products, systems, and information. We are committed to ensuring the security of our customers and associates by protecting their information from unwarranted disclosure by delivering safe and secure products and services. When security vulnerabilities are discovered, we work diligently to resolve them. This document describes MALLINCKRODT PHARMACEUTICAL's policy for receiving reports from security researchers or other third parties related to potential security vulnerabilities in its products and services and the company's standard practice about informing customers of verified security vulnerabilities.
- 1.2. This policy is also intended to give security researchers clear guidelines for conducting security research and to convey our preferences in how to submit discovered security vulnerabilities to us.
- 1.3. This policy describes what systems are covered and types of security research are permitted under this policy, how to send us security vulnerability reports, and how long we ask security researchers to wait before publicly disclosing security vulnerabilities.
- 1.4. We want security researchers to feel comfortable reporting security vulnerabilities they have discovered – as set out in this policy – so we can fix them and keep our users safe. We have developed this policy to reflect our values and uphold our sense of responsibility to security researchers who share their expertise with us in good faith.

2. Scope

- 2.1. This policy applies to all Mallinckrodt manufactured Cyber devices and Mallinckrodt public facing Internet websites and applications.
- 2.2. To verify whether a Cyber device or website is associated with Mallinckrodt, contact us at MPVR@mnk.com before starting your security research or at the security contact for the system's domain name listed in WHOIS for the applicable domain.
- 2.3. Mallinckrodt may pursue all appropriate actions, including, without limitation, referral to the appropriate legal, regulatory, or enforcement authorities, as a result of active security research and testing conducted on systems and services outside the guidelines of this policy.
- 2.4. Types of testing

The following test types are expressly not authorized. Mallinckrodt will pursue all appropriate actions available as a result of the use of any of these types of testing.

 - 2.4.1. Using social engineering.
 - 2.4.2. Using malware.
 - 2.4.3. Phishing Attacks.
 - 2.4.4. Changing the data accessed by exploiting the security vulnerability.
 - 2.4.5. Compromising the system and persistently maintaining access to it.
 - 2.4.6. Using brute force to gain access to systems.
 - 2.4.7. Sharing security vulnerability with third parties.
 - 2.4.8. Network denial of service (DoS or DDoS) tests.

- 2.4.9. Using the security vulnerability in any way beyond proving its existence. To demonstrate that the security vulnerability exists, the reporter could use non-intrusive methods. For example, listing a system directory.
- 2.4.10. Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical security vulnerability testing.

3. References

- 3.1. Federal Food, Drug, and Cosmetic Act (FD&C Act)

4. Definitions

- 4.1. "Security Vulnerabilities" means a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.
- 4.2. "Security Researcher" means a person or entity who researches security vulnerabilities that exist in software applications and hardware, attempts to discover and reverse engineer malware, and finds flaws in websites and commonly used Internet protocols.
- 4.3. "Security Research" means the systematic investigation into and study of materials and sources by security researchers to establish facts and reach new conclusions related to security vulnerabilities.
- 4.4. Cyber Device.
As defined in section 524B of the FD&C Act; the term 'cyber device' means a device that either (A) includes software; or (B) is intended to connect to the internet.

5. Responsibilities

- 5.1. Security researchers or other third parties reporting potential security vulnerabilities.
- 5.2. MALLINCKRODT PHARMACEUTICALS is dedicated to maintaining the confidentiality, integrity, and availability of Mallinckrodt's products, systems, and information. We are committed to ensuring the security of our customers and associates by protecting their information from unwarranted disclosure by delivering safe and secure products and services.

6. Policy

- 6.1. Guidelines - We request that you:
 - 6.1.1. Notify us as soon as possible after you discover a real or potential security issue.
 - 6.1.2. Provide us a reasonable amount of time to resolve the issue before you disclose it publicly.
 - 6.1.3. Avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
 - 6.1.4. Only use exploits to the extent necessary to confirm a security vulnerability's presence. Do not use an exploit to compromise or exfiltrate data, establish command-line access and/or persistence, or use the exploit to "pivot" to other systems.
 - 6.1.5. Once you have established that a security vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), you must stop your test, notify us immediately, and not disclose this data to anyone else.

6.1.6. Do not submit a high volume of low-quality reports. Mallinckrodt will consider reports to be of “low-quality” if, at a minimum, a report does not contain the information and detail set out in the “What we would like to see from you” section of this policy.

6.2. Authorization

6.2.1. If you make a good faith effort to comply with this policy during your security research, we will consider your security research to be authorized, we will work with you to understand and resolve the issue quickly, and MALLINCKRODT PHARMACEUTICALS will not recommend or pursue legal action related to your security research. Mallinckrodt Pharmaceuticals expressly reserves all rights in law and in equity in connection with any security research conducted by or on behalf of you, whether or not such security research complies with this policy and such security research is deemed “authorized.”

6.3. Reporting a vulnerability

6.3.1. Contact the Mallinckrodt Product Security Vulnerability Response Team by sending an email to MPVR@mnk.com and include "VULNERABILITY DISCLOSURE" in the email subject. If you have identified a potential security vulnerability with one of our products. After your incident report is received, the appropriate personnel will contact you to follow-up.

6.4. To ensure confidentiality, we encourage you to encrypt any sensitive information you send to us.

6.5. The MPVR@mnk.com email address is intended ONLY for the purpose of reporting product or service security vulnerabilities specific to our products or services.

6.6. What we would like to see from you

To help us triage and prioritize submissions, a report detailing your security research should include, at a minimum, the following:

6.6.1. Describe the security vulnerability, where it was discovered, and the potential impact of exploitation.

6.6.2. Offer a detailed description of the steps needed to reproduce the security vulnerability (for example proof of concept scripts or screenshots).

6.6.3. A clear and detailed description of the security vulnerability.

6.6.4. Clear and detailed information about how the security vulnerability has been discovered. The objective is to be able to reproduce it.

6.6.5. Proof of the existence of the security vulnerability (screenshot, link, etc.)

6.6.6. A timeline or other information about the moment (date and time) the security vulnerability was discovered.

6.6.7. All information necessary for locating and resolving the security vulnerability in the fastest and most efficient way possible.

6.6.8. Be in English, if possible.

6.7. What you can expect from us

When you choose to share your contact information with us, we commit to coordinating with you as openly and as quickly as possible.

6.7.1. Within three business days, we will use our best efforts to acknowledge that your report has been received.

6.7.2. To the best of our ability, we will confirm the existence of the security vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including issues or challenges that may delay resolution.

6.7.3. We will maintain an open dialogue to discuss issues.

6.8. Severity

6.8.1. Mallinckrodt Pharmaceuticals follows standard industry best practices in scoring or rating security vulnerabilities' potential impact by adopting the Common Vulnerability Scoring Systems (CVSS) framework for communicating the characteristics and impacts of its IT security vulnerabilities.

6.9. Security Advisories

6.9.1. In cases where there are regulatory or legal requirements to report security research findings, Mallinckrodt will report such findings to the appropriate regulatory, legal, or enforcement agencies.

6.9.2. In cases where a third party notifies Mallinckrodt of a potential security vulnerability found in our systems and services, we will investigate the finding and may publish a coordinated disclosure along with the third party. In some instances, Mallinckrodt may receive information about a security vulnerability from a supplier subject to a confidentiality obligation or under embargo. In these cases, Mallinckrodt will work with the applicable supplier to request that a security fix is released although we may not be able to provide details about the security vulnerability.

7. Attachments

7.1. N/A

8. Revision History

Revision No.	Change Description
1	New
2	Updates to include cyber devices

Signature Manifest

Document Number: POLICY-0295
Title: Vulnerability Disclosure Policy
Effective Date: 16 Feb 2024

Revision: 2

All dates and times are in UTC.

POLICY-0295

DCC Review

Name/Signature	Title	Date	Meaning/Reason
Megan Vernak (MEGAN.VERNAK)	Sr Dir, Prod Monitoring&QA Sys	08 Feb 2024, 01:39:36 PM	Approved

Create/Revise

Name/Signature	Title	Date	Meaning/Reason
Dan Curran (DAN.CURRAN)	CIO, Security Infrastructure	08 Feb 2024, 03:26:53 PM	Complete

Peer Collaboration

Name/Signature	Title	Date	Meaning/Reason
Dan Curran (DAN.CURRAN)	CIO, Security Infrastructure	08 Feb 2024, 03:29:59 PM	Complete

Doc Control Review

Name/Signature	Title	Date	Meaning/Reason
Kimberly Miller (KIMBERLY.MILLER)	Document Control Specialist	08 Feb 2024, 06:05:12 PM	Complete

Manager Training Approval

Name/Signature	Title	Date	Meaning/Reason
Dan Curran (DAN.CURRAN)	CIO, Security Infrastructure	08 Feb 2024, 06:30:43 PM	Approved
Michael Acque (MICHAEL.ACQUE)	Exec Dir, Info Technology	13 Feb 2024, 01:13:11 AM	Approved

Author/Department Approval

Name/Signature	Title	Date	Meaning/Reason
Michael Acque (MICHAEL.ACQUE)	Exec Dir, Info Technology	13 Feb 2024, 01:14:03 AM	Approved
Dan Curran (DAN.CURRAN)	CIO, Security Infrastructure	13 Feb 2024, 04:07:11 PM	Approved

Final QA Approval

Name/Signature	Title	Date	Meaning/Reason
Megan Vernak (MEGAN.VERNAK)	Sr Dir, Prod Monitoring&QA Sys	13 Feb 2024, 04:23:20 PM	Approved

Training

Name/Signature	Title	Date	Meaning/Reason
Constance Butler (CONSTANCE.BUTLER)	Quality Systems Training Assoc	16 Feb 2024, 09:30:14 PM	Approved

Change Control Approval

Name/Signature	Title	Date	Meaning/Reason
Kimberly Miller (KIMBERLY.MILLER)	Document Control Specialist	16 Feb 2024, 09:59:04 PM	Approved

Set Dates

Name/Signature	Title	Date	Meaning/Reason
Kimberly Miller (KIMBERLY.MILLER)	Document Control Specialist	16 Feb 2024, 10:00:12 PM	Approved

Notification

Name/Signature	Title	Date	Meaning/Reason
Dan Curran (DAN.CURRAN)	CIO, Security Infrastructure	16 Feb 2024, 10:00:12 PM	Email Sent