1. PURPOSE

The purpose of this document is to describe how cybersecurity risks shall be managed throughout the development lifecycle.

It describes the plan to monitor, identify, and address, as appropriate, in a reasonable time, postmarket cybersecurity vulnerabilities and exploits.

It describes the format and method for producing the software bill of materials.

Finally, it describes how and when postmarket updates and/or patches to the device and related systems will be made.

2. SCOPE

This plan applies to CT Cardiomegaly.

3. DEFINITIONS

Terms and abbreviations used within this document:

Term	Definition
CVSS	The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.
GitHub	A service for hosting software source code.
Hazard	Potential source of Harm
Intended Use	What the medical device is intended to do (i.e., view, analyze CT/MR medical images, fixate fractured bones)
Risk	Combination of the probability of occurrence of harm and the severity of that harm
Risk Assessment	overall process comprising risk analysis and risk evaluation
Risk Control	Process in which decisions are made and measures implemented by which risks are reduced to, or maintained within, specified levels.
Risk Management	Systematic application of management policies, procedures (3.13) and practices to the tasks of analyzing, evaluating, controlling and monitoring risk

Term	Definition
SBOM	Software Bill Of Materials
STRIDE	A model for identifying cybersecurity threats using the mnemonic for Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege.
System	Integrated composite consisting of one or more of the processes, hardware, software, facilities, and people that provides a capability to satisfy a stated need or objective.
System Image	An individual file which can be used to completely reproduce the state of a software system. E.g., including the operating system, system-dependencies, DLLs, configuration files, etc
User	Person who interacts with (i.e., operates or handles) the device.
Verification	Confirmation by examination and provision of objective evidence that specified requirements have been fulfilled (i.e., the requirements are met).

4. REFERENCES

References made within this document:

4.1. Guidance

- 2021 MITRE “Playbook for Threat Modeling Medical Devices”

4.2. Internal

- DOC-0007 Risk Assessment (Rev C)
- P-0002 Development Procedure

5. CYBERSECURITY RISK MANAGEMENT

5.1. Process

Hazard analysis, mitigations, and design considerations pertaining to intentional and unintentional cybersecurity risks associated with the device are documented in the DOC-0007 Risk Assessment (Rev C) alongside the safety risks.

5.2. Threat Modeling

Threat modeling shall be used to help identify cybersecurity risks. A Cybersecurity Engineer shall evaluate assets, and threats in conjunction with the rest of the risk management team to identify cybersecurity risks throughout the product development lifecycle.

Threat modeling was performed following guidelines and the STRIDE methodology described in the 2021 MITRE “Playbook for Threat Modeling Medical Devices”. These methodologies were selected because this document was developed along with the FDA specifically for medical devices.

Threat modeling shall capture cybersecurity risks introduced through the supply chain, manufacturing, deployment, interoperation with other devices, maintenance/update activities, and decommission activities that might otherwise be overlooked in a traditional safety risk assessment process.

5.3. Security Risk Verification

Cybersecurity risk control measures shall be designed, developed, and verified following our P-0002 Development Procedure.

6. SOFTWARE BILL OF MATERIALS

A software bill of materials (SBOM) shall be produced for every publicly released version of the CT Cardiomegaly software.

The SBOM shall follow the SPDX file format.

The SBOM shall include the direct and indirect software dependencies that are incorporated into the System Images, as listed in the .

The SBOM shall be automatically generated manually using syft via the command:

```
syft $LATEST_DOCKER_IMAGE_NAME \
--output syft-table=/tmp/sbom-cardiomegaly-${SOFTWARE_VERSION_NUMBER}_docker_syft_table.txt \
--output spdx-json=/tmp/sbom-cardiomegaly-${SOFTWARE_VERSION_NUMBER}_docker_spdx.json
```

7. VULNERABILITY MANAGEMENT

7.1. Vulnerability Monitoring

Cybersecurity vulnerabilities will be monitored automatically using GitHub’s Dependabot functionality. Dependabot shall be configured to monitor every version of the software that has been released and may still be in use.

7.2. Identification

Vulnerabilities alerts will be reviewed by a Cybersecurity Engineer at least once each month. The record of these reviews shall be stored in the resolution comments of the vulnerability alerts.

During the vulnerability reviews, every alert will be evaluated according to two metrics:

1. Its CVSS severity (Critical, High, Moderate, and Low), as indicated on the alert
2. The Safety-Severity Level of existing Risks identified in the DOC-0007 Risk Assessment (Rev C).

The risk associated with the alert shall then be evaluated as "Controlled" or "Uncontrolled" according to the following matrix:

CVSS \ Safety-Severity Level	**Negligible (1)**	**Minor (2)**	**Moderate (3)**	**Serious (4)**	**Catastrophic (5)**
Critical	Controlled	Controlled	Uncontrolled	Uncontrolled	Uncontrolled
High	Controlled	Controlled	Controlled	Uncontrolled	Uncontrolled
Moderate	Controlled	Controlled	Controlled	Controlled	Uncontrolled
Low	Controlled	Controlled	Controlled	Controlled	Controlled

If there is no existing Risk in the DOC-0007 Risk Assessment (Rev C) that can be used to determine the Safety-Severity Level, then the engineer must notify the Project Manager who will coordinate with the risk management team to update the DOC-0007 Risk Assessment (Rev C) as appropriate. The vulnerability alert shall not be resolved *until* the new risks have been added as appropriate.

Alerts with a CVSS severity of "Moderate" or "Low" may be ignored if there's no chance of Catastrophic safety risk.

Alerts with a CVSS severity of "Critical" or "High" must be resolved once either:

1. It's determined that the alert is not relevant. The "dismissal comment" must explain why the vulnerability won't lead to a safety risk.
2. The vulnerability fix has been entered into the issue tracking system with an appropriate priority set to ensure the vulnerability is addressed. The "dismissal comment" must include a link to the issue id so that the fix can be traced.

7.3. Addressing Vulnerabilities

All "Uncontrolled" risks must be addressed and patches released as quickly as possible.

"Controlled" risks with a "Critical" or "High" CVSS severity level should typically still be addressed and the update released as part of the normal update schedule.

All other risks will be addressed based on their prioritization and available resources.

The resolution of security issues, including fixes, patches, or mitigations implemented, will be thoroughly documented.

8. CYBERSECURITY INSTRUCTIONS AND LABELING

Device instructions for use and product specifications related to recommended cybersecurity controls appropriate for the intended use environment (e.g., anti-virus software, use of firewall) shall be included in the User Manual or other customer facing document (e.g., Release Note).

Information relating to vulnerabilities which have been determined to have the potential for creating unacceptable risk shall be communicated to users no later than 30 days after such determination has been made. The information will at a minimum describe the vulnerability and identify interim compensating controls (as applicable).

9. SOFTWARE UPDATES

Validated software updates shall be developed following the P-0002 Development Procedure, which includes a mechanism for patch releases.

10. DOCUMENT HISTORY

Revision	Date	Description
A	Sep-11-2023	Initial release
B	Nov-22-2023	Change SBOM format to SPDX