GENERAL INSTRUCTIONS

This Product Security Incident Vulnerability Management Plan Template shall be used to establish a prescriptive plan for product teams to systematically monitor, identify, assess, remediate, validate, deploy, and report operating system and application software code updates. These updates are known as patches, hot fixes, and service packs to operating systems, third-party products and components, and [insert company name] developed software.

Medical Technology Company Product Security Incident Vulnerability Management Plan

[Insert Product Name]

1.0 Purpose

1.1 The purpose of this document is to formalize and communicate how incidents, vulnerabilities, and patches relating to [Insert Product Name] will be handled when reported by:

- Customers
- [insert company name] Associates
- Third-Party Component Vendors
- Security Researchers
- Other External Groups

1.2 Existing policy and procedures for complaint handling and defect tracking are reflected in this plan to showcase the cross-sections and relations with product security incidents, vulnerabilities, and patches.

2.0 Scope

2.1 The scope of this document is to provide instruction on specific aspects of product security incident, vulnerability, and patch management, including:

2.1.1 Monitoring and identifying vulnerabilities from various sources
2.1.2 Establish cross-functional teams per table below:

Name of Group(s) or Individual(s)	Email	Phone Number	Mandatory Participation
Product Security	[Insert email]	[Insert phone number]	Y
Business Unit Product Security [Insert group or name]	[Insert email]	[Insert phone number]	Y
Public Relations [Insert group or name]	[Insert email]	[Insert phone number]	N
Regulatory Affairs [Insert group or name]	[Insert email]	[Insert phone number]	N
Quality [Insert group or name]	[Insert email]	[Insert phone number]	Y
Legal [Insert group or name]	[Insert email]	[Insert phone number]	Y
Product Marketing & Management [Insert group or name]	[Insert email]	[Insert phone number]	N
Product R&D [Insert group or name]	[Insert email]	[Insert phone number]	Y
Product Support & Service [Insert group or name]	[Insert email]	[Insert phone number]	Y
Privacy Officer [Insert group or name]	[Insert email]	[Insert phone number]	N

2.1.3 Performing risk assessment for prioritization and remediation planning
2.1.4 Validating effectiveness and impact of remediation
2.1.5 Deploying remediation to affected products
2.1.6 Communication and reporting to various stakeholders

3.0 **Monitoring and Identification:** The following are sources for the identification of incidents and vulnerabilities.

3.1.1 Customers

3.1.1.1 [insert company name] Service and Support teams may be notified by customers of product security issues as the result of an incident or security testing and monitoring at their facility. In these circumstances, the [insert company name] Associate must document the product security issue in accordance with [Insert BU complaint handling procedure] for further analysis and evaluation.

3.1.1.2 In addition, customers may use the [insert company Product Security contact email] available on our company's public website to report security issues for their [insert company name] products. Security issues reported to this email will be forwarded to corresponding [insert company name] Service and Support teams and documented for further analysis and evaluation as per [Insert company complaint handling procedure].

3.1.2 Associates in Service and Support

3.1.2.1 During routine maintenance of products at customer sites [insert company name] Service and Support teams may encounter security incidents or vulnerabilities. In these circumstances, the [insert company name] Associate must document the product security issue in accordance with [Insert complaint handling procedure] for further analysis and evaluation.

3.1.2.2 During routine customer visits, [insert company name] Service and Support teams may use the following methods to manually identify product security issues that should be documented for further analysis and evaluation:

Description of product security issue	Instructions for identifying product security issues
[Insert issue description]	[Provide steps for identifying issue]

3.1.3 Associates in R&D

3.1.3.1 During routine development and testing of products, [insert company name] R&D may discover security vulnerabilities. In these circumstances, the [insert company name] Associate must document the product security issue in accordance with [Insert BU risk management procedure] for further analysis and evaluation.

3.1.4 Third-party Product and Component Vendors

3.1.4.1 The following third-party products and components are used in [insert product name]. For each third-party products and component, the version number and the vendor's source of security notifications is provided:

Name of Third-party Product or Component	Version Number	Source of Vendor Security Notifications
[Insert name of component]	[Insert version number]	[Insert URL]

3.1.4.2 The following group(s) or individual(s) will monitor these sources on a routine basis (weekly/bi-weekly/monthly):

Name of Group(s) or Individual(s) Monitoring	Email	Phone Number
[Insert name]	[Insert email]	[Insert phone number]

3.1.5 Security researchers

3.1.5.1 There may be vulnerabilities reported to [insert company name] from security researchers either to the [insert company name] Product Security email address, which is available on our company's public website or through other public-facing channels. In these circumstances, the product security incident must be documented for further analysis and evaluation as per [Insert complaint handling procedure]. Notification to the cross-functional team must be established in a timely manner.

3.1.6 Other External Groups

3.1.6.1 Information Sharing And Analysis Organizations

3.1.6.1.1 [insert company name] Product Security participates in healthcare industry Information Sharing and Analysis Organizations (ISAOs), which routinely meets and discuss emerging threats and share intelligence on those threats. In the event that a potential vulnerability or incident is identified from an ISAO, the [insert

company name] Product Security office will contact the following individual(s) or group(s):

Name of Group(s) or Individual(s) Monitoring	Email	Phone Number
[Insert group or name]	[Insert email]	[Insert phone number]

3.1.6.2 Secure Coding And System Hardening Standards Organizations

3.1.6.2.1 New or updated standards for software coding and system hardening may become available over the course of the product lifecycle. The following standards are applicable to [Insert product name]:

Name of Standard	Version Number	Source of Standard
[Insert name of standard]	[Insert version number]	[Insert URL]

3.1.6.2.2 The following group(s) or individual(s) will monitor these sources on a routine basis (weekly/bi-weekly):

Name of Group(s) or Individual(s) Monitoring	Email	Phone Number
[Insert group or name]	[Insert email]	[Insert phone number]

4.0 Risk Assessment and Remediation

4.1 Risk Assessment

4.1.1 Product security incidents, vulnerabilities, and patches may require risk assessment as described in [insert company Product security policy and procedure number] to determine the level of risk and prioritization for response. Refer to the [insert company name] Product Security White Paper for [Insert product name] to determine if there are security controls and considerations associated with this product security issue.

4.2 Classification

4.2.1 Product security issues that are reported to [insert company name] may be classified to ensure proper documentation, triage, and trending. The following classifications are for common product security issues for [Insert product name]:

examples shown below may or may not be applicable to each product, add or delete as necessary.

Sub Component	**Descriptor**	**Root Cause**
Operating System	Denial of Service	Malicious Code/Malware
	Security Update	Scans/Probes/Attempted Access
	Inappropriate Usage	Unauthorized Access
	Unknown	Request Security Change/Information
		Unknown

Sub Component	Descriptor	Root Cause
Third-party Software	Denial of Service	Malicious Code/Malware
	Security Update	Scans/Probes/Attempted Access
	Inappropriate Usage	Unauthorized Access
	E-PHI/PII Disclosure	Request Security Change/Information
	E-PHI/PII Destruction	Unknown
	E-PHI/PII Modification	
	Unknown	
Product Software	Denial of Service	Malicious Code/Malware
	Security Update	Scans/Probes/Attempted Access
	Inappropriate Usage	Unauthorized Access
	E-PHI/PII Disclosure	Security Agreement/BAA
	E-PHI/PII Destruction	Request Security Change/Information
	E-PHI/PII Modification	Unknown
	Unknown	
Removable Media	Inappropriate Usage	Malicious Code/Malware
	E-PHI/PII Disclosure	Unauthorized Access
	E-PHI/PII Destruction	Request Security Change/Information
	E-PHI/PII Modification	Unknown
	Unknown	
Documentation	Security Update	Unauthorized Access
	Inappropriate Usage	Security Agreement/BAA
	E-PHI/PII Disclosure	Request Security Change/Information
	E-PHI/PII Destruction	Unknown
	E-PHI/PII Modification	
	Unknown	
[Insert sub-component]	[Insert Descriptor]	[Insert Root Cause]

4.3 Remediation

4.3.1 In order to respond to product security incident, vulnerabilities, and patches immediate and permanent remediation planning may be required. The goal of an immediate remediation may be to achieve issue containment, temporarily workaround, or permanent fix.

4.3.2 Some product security issues may be remediated immediately by simply using the [insert company name] Product Security White Paper for [Insert product name] to determine if there are security controls and considerations associated with this product security issue.

4.3.3 In addition, the [insert company name] Product Security White Paper may be used to provide answers to customer security questionnaires. For additional information on completing the customer security questionnaire please contact Product Support & Service representative identified in the cross functional team table.

4.3.4 The following immediate remediation actions may be considered during specific product security issues:

Description of product security issue	Instructions for immediate remediation of product security issue
Malware detected by antimalware solution	1. Report to customer IT 2. Advise disconnecting from network 3. (High priority) - Advice disconnecting device from network 4. (High priority) - Report incident to the local IT Support Team and advice if any PII/PHI resides in the device. 5. Follow SOP to deal with malware as per [company] Policy if available 6. [Insert additional steps for forensic analysis and recovery]
Phishing	1. (High priority) - Advice to avoid opening the email or clicking/hovering over any links or attachments. 2. (High priority) - Report incident to the local IT Support Team and advice what steps were taken by you. 3. Follow SOP to deal with the issue as per [company] Policy if available
SQL Injection Attack	
Cross-Site Scripting (XSS)	
Denial of Service (DoS)	
Session Hijacking and Man-in-the-Middle	
Credential Reuse	
[Insert issue description]	[Provide steps to remediate issue]

4.3.5 Permanent remediation may be in the form of compensating controls and instructions which customers can use to avoid, reduce, or accept risk. In addition, based on risk assessment and corresponding level of risk described in [insert company procedure documentation number] the development of a patch may be necessary.

5.0 Validation

5.1 Based on the analysis performed during Risk Assessment, criteria for validating effectiveness and impact of a remediation for this product security issue may be established.

5.2 For routine patches for third-party products and components provided by the vendor, a smoke test procedure may be performed to assess impact. Refer to [insert company Design Control Policy number] and [Insert procedure for product smoke testing, verification and validation] for instruction on proper verification and validation.

6.0 Deployment

6.1 At least one of the following methods will be made available for commercialized products to apply validated security patches. *Examples shown below, select all that apply and delete any that are not applicable.*

6.1.1 Customer Administered

6.1.1.1 Validated patches will be made available for customer retrieval and installation from a [insert company name] source or direct download from the third-party entity that provides the product or component.

6.1.2 Ad-Hoc Patching

6.1.2.1 Customers may accept risk for all other deployment mechanisms and/or application of security patches not validated by [insert company name].

6.1.3 Remote Update

6.1.3.1 Patches applied via authorized remote service and support platforms.

6.1.4 Service Visit

6.1.4.1 Local service administered security patches.

7.0 Communication and Reporting

7.1 Timely information must be provided to all stakeholders impacted by vulnerabilities and incidents for commercialized products.

7.1.1 Internal

7.1.1.1 The following individual(s) or group(s) must notify the [insert company name] Product Security Governance Committee of Medium to Critical Risks within three (3) days of initial discovery and provide an update every seven (7) days thereafter until closure.

- Product & Portfolio Management, Core Team lead or equivalent
- Legal

7.1.2 Regulatory and External Agencies

7.1.2.1 Medium to High Risks must be reported to regulatory agencies unless implemented product changes and/or compensating controls bring the residual risk to an acceptable level and users are notified within 30 days of initial discovery. Critical Risks must be reported to regulatory agencies within 30 days of initial discovery.

7.1.2.2 The following individual(s) or group(s) must provide the decision on regulatory notification and deliver the notification:

- Regulatory
- Quality

7.1.2.3 The following individual(s) or group(s) representing Regulatory Agencies must be notified upon decision to do so (disclaimer, may be regional contacts for the product not identified in the cross functional team):

Name of Group(s) or Individual(s) to be Notified	Email	Phone Number
[Insert name]	[Insert email]	[Insert phone number]

7.1.3 Customers and Third-Parties

7.1.3.1 Targeted customer bulletins or notifications posted to the public [insert company name] Product Security webpage must be delivered to customers within 30 days of initial discovery.

7.1.3.2 [insert company name] Product Security Webpage: [insert company website]

7.1.3.3 In addition to the [insert product name] Customer Service and Support portal if one exists: [Insert URL for customer service and support portal]

7.1.3.4 Updates to related Product Security White Papers should be evaluated.

7.1.3.5 Customers and third-parties reporting vulnerabilities and incidents should be provided in a routine cadence status updates while complaint handling investigation is in progress.

7.1.3.6 The cross functional team must provide the decision on notifying customers and other third-parties.

8.0 Exemptions

8.1 Any deviation from this plan will require documentation of the risk assessment performed, the remediation planning that was not pursued, or other component of this plan.