Medical Technology Company Standard Operating Policy Template

The following Product Security Standard Operating Policy (SOP) Template is provided below in furtherance of our commitment to transparency and collaboration with customers and industry stakeholders.

PURPOSE

1.1 The purpose of this SOP is to provide [insert company name] with the proper guidance for securing software-enabled commercial offerings by design, in use, and through partnership throughout the Product Lifecycle.

1.0 SCOPE

1.1 This SOP is applicable to functions that may take part in any aspect of the following:

1.1.1 Design, development, manufacturing, service and support of [insert company name] products that provide software or firmware solutions including medical devices, cloud-based solutions, and software-only products.

1.1.2 Third-Party Entities that [insert company name] collaborates with at any point in the Product Lifecycle including acquisition, development and servicing that do business with [insert company name] products or are in acquisition.

1.2 This document is not intended to provide guidance to update related business procedures, and is exempt from:

1.2.1 Standards or practices regarding concept feasibility, technical development, or products intended without software.

1.2.2 Standards or practices regarding security of [insert company name] internal assets and infrastructure.

2.0 DEFINITIONS / ACRONYMS

2.1 **Product Security:** Striving towards the adequate protection of product, customer and patient confidentiality, integrity, availability, and safety by design, in use, and through partnership with all stakeholders defined in the Responsibilities section below throughout the Product Lifecycle.

2.2 **Vulnerability:** A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a Threat Source.

2.3 **Threat Source:** The intent and method targeted at the intentional exploitation of a Vulnerability or a situation and method that may accidentally trigger a Vulnerability.

2.4 **Product Security Requirements (PSR):** A set of design-level requirements that address Product Security mitigations in both software and system components during Design Control of the secure development lifecycle (SDLC),

and are processed through Risk Management that comprise a product or other commercial offerings.

2.5 **Product Security Risk Assessment:** Overall process comprising a risk analysis and a risk evaluation for security issues found in [insert company name] products using impact to confidentiality, integrity, and availability of product to patients, customers, and [insert company name] to determine the acceptability of the risk.

2.6 **Product Security Management Plan:** Documents all Product Security activities carried out through the design process and post commercialization.

2.7 **Secure Coding Standards:** Guidelines for writing software code which mitigates common security flaws specific to a programming language or in general to all software.

2.8 **Static Code Analysis:** The automated analysis of software code for security flaws and adherence to a Secure Coding Standard.

2.9 **Hardening Standards:** A documented process or mechanism for securely configuring or implementing commonly used technologies.

2.10 **Vulnerability Scanning:** The automated analysis and detection of Vulnerabilities such as missing patches and misconfiguration in operating systems and other third-party software

2.11 **Penetration Testing:** A test methodology in which assessors, using all available documentation such as system design and working under specific constraints, attempt to circumvent the security features of an information system.

2.12 **Vulnerability and Patch Management:** The systematic monitoring, identification, assessment, remediation, deployment, and verification of 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.

2.13 **Third-Party Entities:** External individuals and organizations, such as vendors and suppliers that [insert company name] collaborates with at any point in the Product Lifecycle, including acquisition, development and servicing, that do business with [insert company name] in connection with its products.

2.14 [insert company name] **Assets and Systems:** Includes, but not limited to, equipment used by any function in any aspect of day-to-day business operations that is owned by [insert company name] . Examples such as development environments used by R&D, equipment used by Manufacturing to produce products or computers used to support products.

2.15 **Removable Media:** Portable electronic storage media such as magnetic, optical, and solid-state devices, which can be inserted into and removed from a computing device, and that is used to store text, video, audio, and image information. Such devices have no independent processing capabilities.

Examples include hard disks, floppy disks, zip drives, compact disks, thumb drives, pen drives, and similar USB storage devices.

2.16 **Product Lifecycle:** Managing the entire lifecycle of a product from inception, through engineering design and manufacture, to monitoring, service and disposal of manufactured products.

3.0 RESPONSIBILITIES

3.1 Product Security (PS):

3.1.1 Creation and maintenance of policies, procedures, tooling, guidance, training and awareness for Product Security across all [insert company name] Business Units and functions. PS will support Product Security Risk Assessments, automated security testing, Penetration Testing, and remediation planning services for R&D and complaint handling.

3.2 Product Security Governance Committee:

3.2.1 Cross-Functional group responsible within each Business Unit providing oversight of [insert company name] Product Security Policy adoption and exemptions documented in the Product Security Plan.

3.3 Corporate and Business Unit Quality:

3.3.1 Ensures the [insert company name] Product Security Policy is aligned and consistent with other [insert company name] corporate policies, as well as global regulations and standards, for product development, risk management, manufacturing, and support. Quality, jointly with the PS, will ensure adherence to the [insert company name] Product Security Policy.

3.4 Research and Development (R&D):

3.4.1 Incorporates Product Security in the budgeting, resource planning, design requirements in the development process, and throughout the Product Lifecycle including post-commercialization maintainability. R&D will maintain record of security defects in accordance with the business unit quality management systems including design control and risk management procedures.

3.5 Service and Support:

3.5.1 Ensure proper response to security incidents and events with products at customer sites, including proper documentation records as per business unit complaint handling procedures. Secure [insert company name] service assets, maintain validated security updates and ensure secure implementation, periodic reporting of security incidents and events and security update tracking.

3.6 Business Unit and Regional Leadership:

3.6.1 Responsible for communication, compliance and adherence of the [insert company name] Product Security Policy at the Regional and local

business levels. This may include the creation of local procedures that align with and supplement where needed, due to regional laws and regulation, the over-arching [insert company name] Product Security Policy.

3.7 Global Information Security (GIS):

3.7.1 Ensures [insert company name] managed assets, including but not limited to laptops, Removable Media, and networks that interact with [insert company name] products adhere to the [insert company name] Information Security Policy.

3.8 Third-Party Entities:

3.8.1 Adhere to requirements in the [insert company name] Product Security Policy and [insert company name] Information Security Procedure against entities external to [insert company name]. Any exemptions must be documented in the Product Security Management Plan.

4.0 REQUIREMENTS

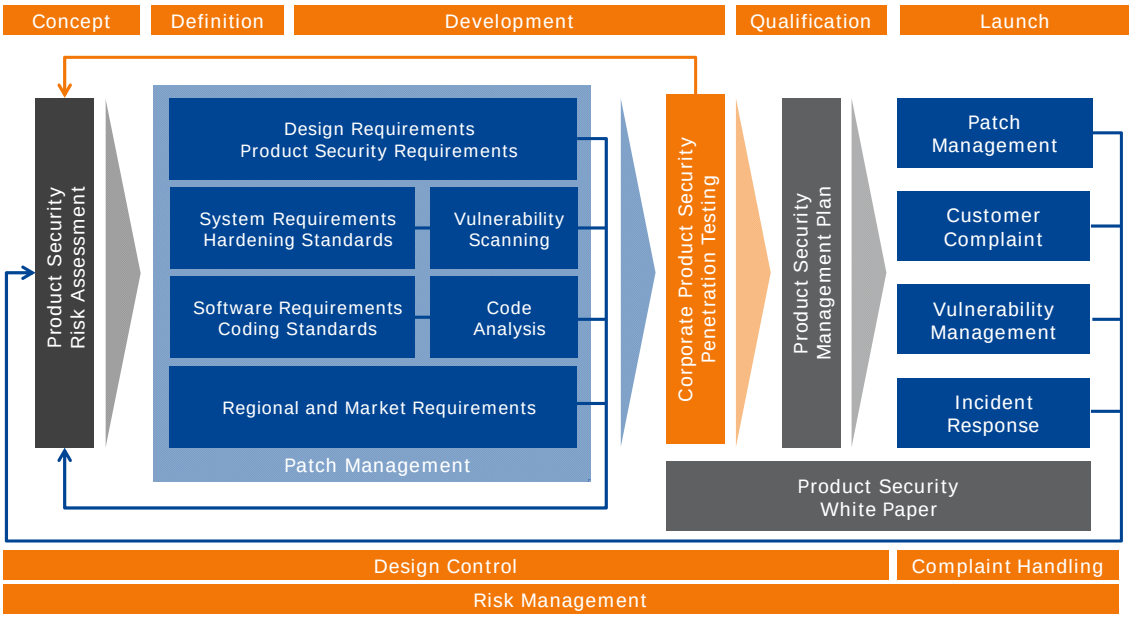
4.1 The following requirements must be considered during any design, development, manufacturing, service and support of [insert company name] products that provide software or firmware solutions including:

- Medical devices
- Cloud-based solutions
- Software-only products

4.2 Exemptions and Vulnerabilities not being addressed will be documented in the Product Security Management Plan.

4.3 The flowchart below is used to illustrate how Product Security may be incorporated within existing [insert company name] design control, quality

systems and release processes.



4.4 Risk Management for Product Security: There are specific considerations necessary for ensuring Product Security risks identified during Design Control and Complaint Handling are properly analyzed, evaluated, and documented.

4.4.1 Product Security Risk Assessments for Product Security findings identified in Design Control or Complaint Handling must be assessed for severity and documented accordingly.

4.4.2 Remediation Planning must be carried out for products in development as well as products within scope of this policy.

4.4.3 Exemptions for potential risks that are identified but which are addressed in subsequent releases or patch updates will require documentation of the risk assessment performed and the remediation planning that was not pursued in accordance with the [insert company name] Product Security Procedure.

4.5 Product Security controls and potential Vulnerabilities identified during Design Control will be incorporated per the relevant design control policy/procedure. The following should be used as additional requirements to be considered and implemented as part of product development.

4.5.1 A Product Security Risk Assessment and remediation plan must be performed to determine prioritization and subsequent actions for any potential security Vulnerabilities identified.

4.5.2 Products under development will require review of high-level security requirements based on authoritative sources as well as customer feedback.

4.5.3 System Requirements, including third-party components used in the product, shall also be subject to Product Security Requirements such as Hardening Standards, System Patching and Vulnerability Scanning.

4.5.4 Static Code Analysis and robust testing shall be performed throughout the development cycle to ensure Secure Coding Standards are followed.

4.5.5 A Product Security Incident & Vulnerability Management Plan must be established to identify, evaluate, and respond to any incident or Vulnerability, including routine patching, throughout the Product Lifecycle.

4.5.6 Additional Product Security Requirements will be produced prior to release or commercialization, including: Product Security Incident & Vulnerability Management Plan, Product Security White Paper, Penetration Testing Summary and Product Security Management Plan shall be established.

4.6 Complaint Handling for Product Security: Complaint evaluation or investigation shall include steps to determine if there is a Product Security event or question. [insert company name] Product Security will be notified if a complaint is determined to have a Product Security issue.

4.7 Peripheral factors impacting Product Security are identified as external components outside of the product design and implementation that shall also be assessed for risk.

4.7.1 [insert company name] assets and/or infrastructure used to support R&D, Supply Chain, Manufacturing, Service and any other functions to produce and procure [insert company name] products and services must adhere to [insert company name] Information Security Policy and Standards. These may include work computers and networks used during any stage of the Product Lifecycle.

4.7.2 [insert company name] Service and Support activities should include guidance regarding Service Access (remote and local), Customer Data Handling, Removable Media, and Decommissioning of [insert company name] products when applicable.

4.7.3 [insert company name] IT creates, supports and maintains infrastructure required by the business functions to develop, manufacture and support [insert company name] products in adherence to [insert company name] Information Security Policy and Standards.

4.7.4 Third-Party Assets and Systems shall be assessed and adhere to [insert company name] Information Security Policy and Standards.