VELENTIUM
MEDICAL

TOTAL PRODUCT LIFE-CYCLE SECURITY GUIDE

SEC-GUIDE-07

Provided by:

VELENTIUM MEDICAL
CYBERSECURITY SERVICES

1.0 Introduction to Velentium Medical's Cybersecurity Approach

At Velentium Medical, cybersecurity isn't a checkbox – it's a commitment to improving and defending lives for a better world. Our Total Product Life-Cycle (TPLC) security process is purpose-built to align with the latest and most rigorous standards from the U.S. FDA, EU MDR/MDCG, IEC 81001-5-1, and more. Whether you're building a brand-new system or sustaining one already in the field, we provide a globally compliant, submission-ready pathway to securing your device from concept to end of support.

This guide outlines the phases, activities, and deliverables that make up Velentium Medical's Secure Product Development Framework (SPDF) for the TPLC. It reflects a proven approach trusted by hundreds of clients and backed by a 100% success rate in regulatory submissions. As a premier one-stop shop for medical device cybersecurity, we flex our services and pricing to meet your needs, whether you need full-service support or expert guidance on specific phases.

The table in Section 3.0 maps our security process to the IEC 62304 software development lifecycle. Use it as a practical reference to understand what "secure by design" truly means across every phase of your device's life.

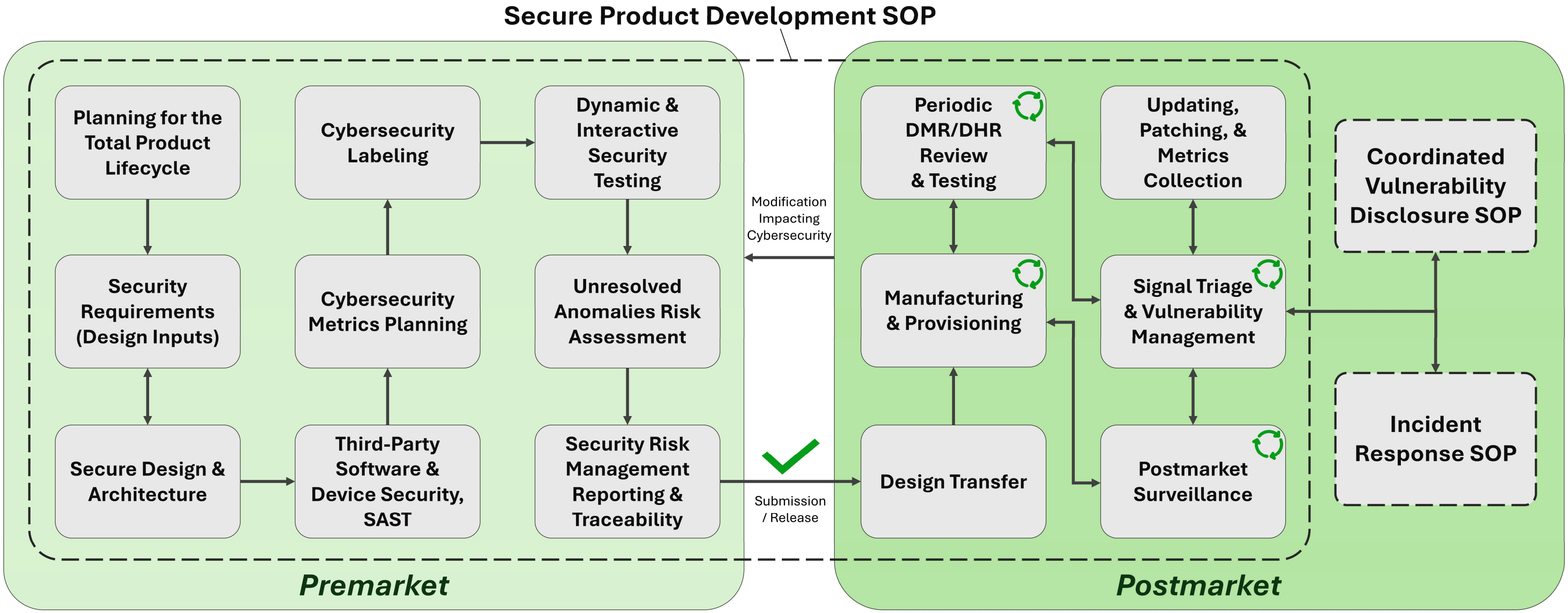
2.0 The Velentium Way

The Velentium Medical SPDF includes three Standard Operating Procedures (SOPs):

1. **Secure Product Development SOP** – Covers premarket new product development and a majority of postmarket activities, inclusive of surveillance and maintenance. Activities include planning, requirements derivation and analysis, threat modeling, cybersecurity risk assessment, architecture and controls reporting, Software Bill of Materials (SBOMs), labeling, metrics, security testing, security assessments of software bugs, traceability, and more.
2. **Coordinated Vulnerability Disclosure SOP** – Covers coordinated vulnerability disclosure during postmarket, beginning with the intake of security reports from external parties and ending with disclosure to customers, government agencies, and other stakeholders.
3. **Incident Response SOP** – Covers the response, recovery, and recording of security events deemed to be true security incidents happening during postmarket.

Velentium Medical offers access to these SOP templates and templates for regulatory artifacts, plus consulting and support for manufacturers so they can implement procedures in their QMS, train their personnel on operating within the procedures, develop safe and secure products, and create globally compliant DHF and DMR/DHR items.

The graphic below shows this holistic process in a simplified flow diagram, although the actual implementation may vary slightly per project and organization.


Secure Product Development SOP
Planning for the Total Product Lifecycle
Cybersecurity Labeling
Dynamic & Interactive Security Testing
Security Requirements (Design Inputs)
Cybersecurity Metrics Planning
Unresolved Anomalies Risk Assessment
Secure Design & Architecture
Third-Party Software & Device Security, SAST
Security Risk Management Reporting & Traceability
Modification Impacting Cybersecurity
Submission / Release
Periodic DMR/DHR Review & Testing
Updating, Patching, & Metrics Collection
Manufacturing & Provisioning
Signal Triage & Vulnerability Management
Design Transfer
Postmarket Surveillance
Coordinated Vulnerability Disclosure SOP
Incident Response SOP
Premarket
Postmarket

KEY: *SOP = Standard Operating Procedure, SAST = static analysis security testing, DHR = Design History Record, DMR = Device Master Record, ♻ = Continuous / Frequent Process*

The table in Section 3.0 below elaborates on the graphic above to expand each phase shown into activities and outcomes. Many of the outcomes include artifacts necessary for regulatory submission. Velentium Medical's *SEC-GUIDE-00 Navigating Cybersecurity during FDA eSTAR Submissions* discusses these submission requirements with annotated screenshots and actions to take to comply with the FDA's electronic submission process.

3.0 Velentium Medical Process Summary Table

This section outlines Velentium's complete TPLC-aligned security process. Each phase includes clear objectives, actionable activities, and concrete outputs—many of which are required regulatory artifacts marked with an asterisk (*). The SPDF is not just a checklist—it's an integrated set of practices that ensure your product is secure by design, defensible in audit, and safe in deployment.

Lifecycle Phases	Security Phases	Security Processes / Activities	Deliverables / Artifacts / Outcomes	Description
Software Development Planning	**Kickoff**	Company and System Information Gathering	• Cybersecurity Information Gathering Form	An informal document critical to Velentium understanding and documenting your project information needed for planning, threat modeling, cybersecurity risk assessment, attack surface analysis, and more.
	Governance	Generation of SOPs / WIs / FRMs / etc. for other processes and outcomes covered in this guide	• Security Procedures integrated within QMS and followed throughout TPLC	All premarket and postmarket activities require procedures integrated within a manufacturer's QMS aligned with global regulations, standards, and best practices for medical device cybersecurity, including IEC 81001-5-1, AAMI SW96, HSCC Joint Security Plan v2, US FDA, EU MDCG, and more.
	Security Planning	Security Risk Management Planning for Total Product Life-Cycle (TPLC)	• Security Risk Management Plan*	Contains a justification and description of the Secure Product Development Framework (SPDF) used with references to premarket and postmarket governance structures (above QMS items and standards), Security Goals, Roles and Responsibilities of the personnel involved, and security activities and outcomes for the system for the total TPLC.
Software Requirements Analysis	**Security Requirements**	Derive Security Requirements (may require updates following Threat Modeling and Cybersecurity Risk Assessment)	• Security Requirements included in System Requirements • Security Requirements included in Software Requirement / Specifications • Security content included in Detailed Design	Security content should be included in requirements and design inputs documentation. The threat models and cybersecurity risk assessment should inform the requirements and may require changes to the requirements. Ultimately, security requirements should be traced to security controls, and security requirements should be tested during Verification and Validation while security controls will be tested during vulnerability and penetration testing.
Software Architectural Design	**Secure Design and Architecture**	Threat Modeling and Generation of Security Architecture Views and Use Case Views	• Threat Modeling and Security Architecture Report*	Contains the system security risks and mitigations (both for design/architecture and processes such as updating and supply chain), methods used, assumptions made, and security architecture views and use case views.
		Cybersecurity Risk Assessment	• Cybersecurity Risk Assessment Report*	Summarizes pre- and post-mitigation assessment of security risks using CVSS or similar methods adequate for design security risk assessment of medical devices. Velentium Medical employs a modified version of CVSS version 2 due to the Collateral Damage Metric's ability to proxy for safety and severity and due to the ability to gear the methods for design-time assessments.
		Cybersecurity Controls Reporting	• Cybersecurity Controls Report*	Controls should be documented according to the FDA's Premarket Guidance Appendix 1. Control Categories. Using the Velentium Mitigation Inventory and our FDA eSTAR templates during threat modeling and risk assessment makes this document extremely simple, as our mitigations are already mapped to the control categories.

Lifecycle Phases	Security Phases	Security Processes / Activities	Deliverables / Artifacts / Outcomes	Description
Software Unit Implementation	**Third-Party Software and Device Security**	Generation and Maintainenance of Software Bill of Materials (SBOM)	• Machine-readable SBOMs in CycloneDX or SPDX format in JSON or XML*	SBOMs should be generated for all first-party software and firmware. SBOMs are inventories of third-party software components used in first-party software and firmware and are essentially data structures complying with the NTIA's SBOM minimum data elements and other standards. SCA can be leveraged as one potential way to generate SBOMs. Velentium Medical uses NetRise tooling to perform SCA, SBOM management, and SBOM monitoring. We are a reseller of other vendors, as well, to ensure complete coverage for our clients.
		Document SBOM Component Support Information	• SBOM Support Report*	Support status (e.g., deprecated, supported, end of life) of third-party software components in the SBOMs as well as end of support dates if available, should be documented in an FDA eSTAR artifact. The Velentium Medical template for the SBOM Support Report includes a human-readable SBOM table with this information. Contingency plans for components becoming unsupported during postmarket must also be included in this document.
		Monitor and analyze SBOM Vulnerabilities (NIST NVD, CISA KEV, other sources)	• Software Component Risk Management Report*	Known vulnerabilities from sources such as the NIST NVD, CISA KEV Catalogue, and other security advisories are identified in the software components contained in the SBOMs. These vulnerabilities must undergo root cause analysis or impact analysis to determine if they are real, exploitable, present vulnerabilities in the system based upon the implementation of the affected components. Present vulnerabilities must then undergo cybersecurity risk assessment. This is an ongoing activity from premarket through postmarket.
		Commercial "Off-the-Shelf" (COTS) Device / OS Hardening	• Captured in design and architecture documents and described in product Labeling	COTS devices should be hardened and securely configured for their intended use and environment of operation. This usually involves creating a policy or image with a reduced attack surface that only allows intended functionality that can be quickly provisioned onto devices during manufacturing. Baselines and implementation guides are available to make this process easier.
	Cybersecurity Metrics	Plan for Metrics gathering during Updating / Patching	• Cybersecurity Metrics Report*	During postmarket update and patch events, certain metrics should be gathered. An eSTAR artifact is required that summarizes these metrics for the system to be submitted and for any previous cyber medical device systems from your company during historical update and patch events, if available / applicable.
	Cybersecurity Labeling	Derive security content for IFU and Labeling	• Cybersecurity included in IFU/Labeling*	Security instructions and information should be communicated to users through labeling to comply with the FDA's 14 cybersecurity labeling requirements from the Premarket Cybersecurity Guidance. The labeling report details where in the IFU the 14 requirements are covered or why certain requirements may not be applicable with justifications.
		Complete Manufacturer's Disclosure Statement for Medical Device Security (MDS2) form	• MDS2 form	NEMA provides a templated excel spreadsheet to communicate cybersecurity information to users and customers in a standardized format consisting of many yes-or-no questions with optional notes allowed. This is optional for FDA submissions but required for procurement with many customers.

Lifecycle Phases	Security Phases	Security Processes / Activities	Deliverables / Artifacts / Outcomes	Description
Software Unit Implementation and Verification	**Security Testing**	Attack Surface Analysis	• Cybersecurity Testing Report* summarizing all security testing and requirements verification • Independent reports for each testing activity to be appended to Cybersecurity Testing Report	Attack surface analysis is similar to and should start with threat modeling. During attack surface analysis, the digital assets within the system and interfaces with which those assets could be affected are enumerated. Attack vectors (interfaces or data flows that can impact digital assets) and threat scenarios are explored against mitigating security controls to determine if the attack surface is sufficiently managed and controlled or not.
		Static Analysis (SAST) of Source Code		All first-party source code should be analyzed for violations against well-vetted and industry-recognized secure coding standards. These violations should be triaged and mitigated or justified, and SAST should be performed iteratively throughout development and one final time on the final release code base.
		Software Composition Analysis (SCA)		SCA examines firmware and software files, software executables, and device images to identify dependencies, cryptographic issues, exposed or insecure credentials, and other misconfigurations. SBOMs are generated as a product of SCA. Velentium Medical uses NetRise tooling to perform SCA, SBOM management, and SBOM monitoring. We are a reseller of other vendors, as well, to ensure complete coverage for our clients.
		Vulnerability Scanning		Closed-box scanning for known vulnerabilities attempts to identify known vulnerabilities and misconfigurations on a live host via a network interface, such as WiFi and Ethernet, with a connectable IP address. Velentium Medical uses Tenable Nessus Pro for this.
		Fuzz Testing		Fuzzing involves stress testing digital communication interfaces with malformed, unexpected, and/or random input. Behavior and responses to the inputs are observed to determine if any unintended or unacceptable device or software behaviors occur. Velentium Medical uses Keysight IoT Security Assessment tool for fuzz testing and other security testing methods.
		Malformed Input Testing		Malformed input testing is similar to fuzzing with the exception being that the inputs under test are typically user inputs, although some software inputs may be applicable as well. User inputs should be stressed tested to ensure only intended inputs are accepted and others are not, similar to boundary analysis.
		Penetration Testing		Penetration testing should be performed by an experienced, objective, and qualified party independent from the design and development of the system under test. Penetration testing typically involves the following phases: 1) Planning and Scoping, 2) Intelligence Gathering, 3) Threat Modeling, 4) Vulnerability Analysis, 4) Exploitation, and 5) Reporting. Methods are subject to the tester's repertoire of tools and techniques.
Software Release	**Unresolved Anomalies Risk Assessment**	Security Assessment of SOFTWARE BUGS following Verification	• Unresolved Anomalies Risk Management Report*	Following the completion of final Verification and Validation, any software bugs that are residual in the final release should be assessed for security impact and relevance. Some bugs may be determined to be potentially exploitable as security vulnerabilities or have security impact, and therefore, may require further testing and assessment.
	Security Risk Management Reporting and Traceability	Summarize all Activities Performed Prior to Submission / Release	• Security Risk Management Report*	This report is the final report generated during premarket activities summarizing all activities performed and referencing DHF artifacts. Justifications for residual security issues are performed, and it includes traceability between risks, vulnerabilities, controls/mitigations, requirements (with Verification and Validation), and security testing.
		Cybersecurity Traceability		
Submission / Release				

Lifecycle Phases	Security Phases	Security Processes / Activities	Deliverables / Artifacts / Outcomes	Description
Postmarket	**Design Transfer**	Software, firmware, configurations, designs, etc. transferred to manufacturing with confidentiality, integrity, and authenticity ensured		Integrity, version control, and confidentiality should be ensured as designs are transferred to manufacturing. Future modifications or updates may require returning to development processes through release to transfer new software or firmware to manufacturing. Build environments and source code must also be maintained and protected to ensure future modifications can occur if needed to fix security or other issues.
	Manufacturing and Provisioning	Manufacturing	• Devices securely programmed with Executables, Binaries, Configurations, Images, etc.	Integrity should be maintained through manufacturing via cryptographic hash verification, at a minimum, and other considerations exist for intellectual property protection and operational technology cybersecurity concerns within the manufacturing environment. Programming and debugging interfaces should be disabled as a final manufacturing step of hardware and electronics.
		Device Provisioning		Devices must also be provisioned with hardening schemes, security secrets (keys, credentials, etc.) for backend interactions, device management solutions, and secure configurations prior to being deployed to users.
		Deployment to Customers	• Devices integrated within operating environments	Devices are then provided to customers and may require integration within the intended operating environment, such as if local PACS/DICOM and other servers are to be connected to within a hospital or if cloud connectivity is required through a hospital network.
		Device Management and Administration	• Long-term administration and monitoring of devices	Once fielded, certain devices may require management via a mobile device management or enterprise asset management solution to offer remote support, updating and patching pathways, monitoring and detection capabilities, metrics gathering, and other capabilities.
	Periodic DMR / DHR Review	Review and Potential Updates to Planning, Threat Modeling and Security Architecture Report, Cybersecurity Risk Assessment, Cybersecurity Controls Report, and Attack Surface Analysis	• Potential updates to DMR / DHR • May lead to Vulnerability Triage and Management	Artifacts and documents generated as DHF items during premarket and maintained as DMR/DHR items during postmarket should be reviewed during the entire postmarket phase, as the threat landscape impacting a system likely changes over time. Postmarket signals gathered during other postmarket phases should feed into this process. For example, security testing may reveal vulnerabilities or threats that were not considered during premarket, and device modifications may result in changed architecture.
	Periodic Security Testing	Static Analysis (SAST) of Source Code	• Updates to Cybersecurity Testing Report • Independent reports for each testing activity to be appended to Cybersecurity Testing Report • Findings may lead to Vulnerability Triage and Management	Security testing is required to be performed on a periodic basis. The FDA guidance recommends an annual frequency, but the cadence is subject to the device/system and its risk profile, in addition to what the FDA reviewer determines is sufficient. Some testing may need to occur on every release or code change, while other testing can be performed on an annual or other periodic basis. The Cybersecurity Testing Report can be a living document that is updated every time testing is performed to capture the latest testing results and historical data.
		Software Composition Analysis (SCA)		
		Vulnerability Scanning		
		Fuzz Testing		
		Malformed Input Testing		
		Penetration Testing		

Lifecycle Phases	Security Phases	Security Processes / Activities	Deliverables / Artifacts / Outcomes	Description
	Postmarket Surveillance	Continuous SBOM Monitoring and Maintenance Field Reports (Complaints, Incidents, Service Records) Device Security Events and Log Analysis Threat Intelligence and Alerts from CERT/ISAC/ISAO and Suppliers	• Potential updates to SBOMs, Software Component Risk Management Report, and SBOM Support Report • New signals and vulnerabilities lead to Vulnerability Triage and Management	Many sources can be monitored during the postmarket to detect potential security vulnerabilities, threats, and events (which can be assessed to be real security incidents), including user complaints, SBOM related activities, device and user behaviors, and intelligence from the community. SBOMs should be maintained to be accurate during updates and patches and should be monitored for newly disclosed vulnerabilities that may impact the system, and the third-party software used within the fielded system. As signals arise, they should be triaged and documented, as well as potentially remediated and disclosed.
	Coordinated Vulnerability Disclosure (CVD)	Preparation Receipt Verification Remediation Development Release Post-Release	• CVD process documented as a SOP in QMS with roles, responsibilities, activities, outcomes, ecosystem and resources required, etc. • Vulnerability triage and management, CAPA, IR, updating and patching, and other processes may need to be performed	Manufacturers should be ready to receive security reports from external parties via a confidential and managed process. Once received, reports should be tracked, verified, remediated, and results should be communicated to reporting parties. Lastly, regardless of how an issue is found, vulnerabilities that are uncontrolled and/or having critical or catastrophic severity should be disclosed to users and the US government (FDA and/or other groups). Press and public interaction may also be required. Security vulnerabilities discovered in the postmarket should be disclosed within 30 days of their discovery.
	Vulnerability Triage and Management	May involve verification of issue / impact analysis / root cause analysis, assessment of exploitability and severity, mitigation / remediation, and tracking of issues and assessments; similar / redundant with other postmarket processes		As signals are detected and gathered during postmarket processes, especially during Postmarket Surveillance, Coordinated Vulnerability Disclosure and Periodic Security Testing, they should be assessed for accuracy, applicability, exploitability, and severity. An impact analysis or root cause analysis first determines if a signal is a real security vulnerability, threat, or incident impacting the system. True positive signals then are assessed to determine the exploitability of the issue (typically based on CVSS), the severity of the issue (negligible to catastrophic), and if the issue is controlled/mitigated or not. All issues should be documented and tracked over time, and the assessment will determine if further action is required, which may include disclosing the issue to customers and government agencies, as well as security updates or patches to apply new controls and resolve issues.

Lifecycle Phases	Security Phases	Security Processes / Activities	Deliverables / Artifacts / Outcomes	Description
	Incident Response (IR)	Preparation	• IR process documented as a SOP in QMS with roles, responsibilities, activities, outcomes, ecosystem and resources required, etc. • Awareness and training performed to SOP • CAPA, CVD, updating and patching, and other processes may need to be performed	Response teams are established, including defining appropriate lines of communication, articulate services necessary to support response activities, and procure the necessary tools, including secured communication between team members and secured file storage for use by the team.
		Identification		Identifying an event and conducting an assessment are required to confirm the existence of an incident. The assessment should include determining the scope, impact, and extent of the damage caused by the incident. In the event of possible legal action, digital evidence should be preserved, and forensic analysis may be conducted in compliance with legislative and legal requirements.
		Containment		Containment of the incident is necessary to minimize and isolate the damage caused. Steps should be taken to ensure that the scope of the incident does not spread to include other systems and products. Root cause analysis should be required prior to moving beyond the Containment phase and may require expertise from outside parties.
		Eradication		Eradication shall require the removal or addressing of all components and symptoms of the incident, including creating workarounds and patches.
		Recovery		Recovery shall involve the steps required to restore data and systems to a healthy working state allowing business operations to be returned, as well as updating or patching products in the field to return them to their original essential performance. Recovery isn't merely a return to the status that existed pre-incident, but improving the security posture to prevent a secondary incident to these newly restored systems.
		Lesson Learned		Includes post-incident analysis on the system(s) that were impacted by the incident and other potentially vulnerable systems, including assessments for any undetected occurrence of the same root cause of the vulnerability in other parts of the product or other product models. Lessons learned from the incident are communicated to executive management and may include updating process / QMS structures to improve future incident management practices and reduce risk exposure.
	Updating and Patching	Security Updates of First-Party Devices	• Defined process part of QMS and capabilities designed and implemented within the system during premarket; • Verified and Validated Updates and Patches ready for Deployment	Security updates are performed to first-party firmware and software (e.g., remediating security vulnerability in an application running on Windows created by you the manufacturer), and security patches are applied to third-party software used within a system (e.g., patching Windows, other operating systems, or third-party applications). The authenticity and integrity of update payloads and their sources, confidentiality of the update payload, and version control and rollback prevention should be ensured during such events, and users should be aware of these events and be able to control when they occur to prevent updates during critical operations. Development of patches and updates must occur within 60 days of postmarket vulnerability discovery. Release of updates and patches may vary, as some issues can be corrected during normal periodic maintenance, while others may require more urgent releases.
		Security Patches of Third-Party Devices		
		Collection and tracking of Cybersecurity Metrics	• Updates to Cybersecurity Metrics Report as needed	

Lifecycle Phases	Security Phases	Security Processes / Activities	Deliverables / Artifacts / Outcomes	Description
	Customer Communications	Although involved in other activities and phases above, customer communications are essential during postmarket, beginning with sales and procurement discussions. Up-to-date and version-controlled SBOMs, MDS2 forms, testing reports, and more may need to be made available to customers, IR and updates / patches must be communicated, uncontrolled and severe vulnerabilities must be disclosed, and security reports and field reports must be received and managed. EOS / EOL timelines, decommissioning guidance, and potentially reporting to government agencies are also required.		
End of Support or Use	**Device Retirement and Decommissioning**	Plan and execute secure decommissioning and EOL activities	• EOL Notice • Device Decommissioning and Disposal Records • Archived Security Deliverables	Ensure device is securely decommissioned at end-of-life. Remove sensitive data and credentials, communicate end-of-support status to users, and confirm safe disposal. These activities reduce the risk of postmarket exposure.

4.0 Next Steps

Velentium Medical can help you implement cybersecurity governance within your organization, develop secure products, generate submission-ready artifacts, maintain and sustain medical devices during postmarket, and train your personnel, all based on the latest, state of the art standards and best practices for medical device cybersecurity. We can either offer templates and be your guides, we can be your outsourced testing partner, or we can do everything for you with in-house experts and engineers.

Contact us and learn more at www.VelentiumMedical.com/EmbeddedCybersecurity.

5.0 Revision History

This guide has been revised as described below:

- Version 0: Initial Release
- Version 1: Updates corresponding to release of FDA eSTAR v5.5
- Version 2: Updates corresponding to release of FDA 2025 Premarket Cybersecurity Guidance and eSTAR v5.6
- Version 3: Minor changes to formatting and content

6.0 Abbreviations

The table below provides terms for the abbreviations used within this guide.

Abbreviation	Term
AAMI	Association for the Advancement of Medical Instrumentation
CAPA	Corrective and Preventive Action
CISA	Cybersecurity and Infrastructure Security Agency
COTS	Commercial Off-The-Shelf
CVD	Coordinated Vulnerability Disclosure
CVSS	Common Vulnerability Scoring System
DHF	Design History File
DHR	Device History Record
DICOM	Digital Imaging and Communications in Medicine
DMR	Device Master Record
EOL	End of Life
EOS	End of Support
eSTAR	FDA Electronic Submission Template and Resource
EU	European Union
FDA	U.S. Food and Drug Administration
HSCC	Health Sector Coordinating Council
IEC	International Electrotechnical Commission
IFU	Instructions for Use
IP	Internet Protocol
IR	Incident Response
JSON	JavaScript Object Notation
KEV	Known Exploited Vulnerabilities
MDCG	Medical Device Coordination Group
NEMA	National Electrical Manufacturers Association
NIST	National Institute of Standards and Technology
NTIA	National Telecommunications and Information Administration
NVD	National Vulnerability Database
PACS	Picture Archiving and Communication System
QMS	Quality Management System
SAST	Static Application Security Testing
SBOM	Software Bill of Materials
SCA	Software Composition Analysis
SOP	Standard Operating Procedure
SPDF	Secure Product Development Framework
SPDX	Software Package Data Exchange
TPLC	Total Product Life-Cycle
US	United States of America
XML	Extensible Markup Language