**[Device Name]**

**Security Operations Manual**

**[Insert device image (optional)]**

**Applies to [Enter relevant part number and version for the product and its software, as applicable]**

This document was prepared by [**department/role name**] of Stryker’s [**division name**] division. See section 3.1 below for contact information.

**Table of Contents**

[1. PURPOSE 5](#_Toc59610132)

[2. DEFINITIONS 5](#_Toc59610133)

[3. PRODUCT DESCRIPTION 8](#_Toc59610134)

[3.1 Device and Manufacturer Identification (DOC-1, 2, 3, 5) 8](#_Toc59610135)

[3.2 Device Intended Use (DOC-6) 8](#_Toc59610136)

[3.3 Related Manufacturer Programs (DOC-8, DOC-9) 8](#_Toc59610137)

[3.4 System Characterization and System Assets 8](#_Toc59610138)

[3.5 System Security Context and Intended Environment (SGUD-4) 9](#_Toc59610139)

[3.6 Network, Data Flow Diagram (DOC-10) 10](#_Toc59610140)

[3.7 Setup of SaMD (DOC-11) 11](#_Toc59610141)

[4. MANAGEMENT OF PII and PHI (MPII-1) 11](#_Toc59610142)

[4.1 Authority to Collect PHI 11](#_Toc59610143)

[4.2 Purpose Specification for PHI Use 11](#_Toc59610144)

[4.3 PHI Data Quality and Integrity 11](#_Toc59610145)

[4.4 PHI Data Deletion and Minimization (SGUD-2) 11](#_Toc59610146)

[4.5 Legal Roles and Related Requirements for Privacy 11](#_Toc59610147)

[4.6 Handling of Patient Requests for their PHI Access 11](#_Toc59610148)

[4.7 Storage and Removal of PII (MPII-2) 11](#_Toc59610149)

[4.8 Transmitting, Importing/Exporting of PII (MPII-3) 11](#_Toc59610150)

[5. AUTOMATIC LOGOFF (ALOF-1, 2) 12](#_Toc59610151)

[6. AUDIT CONTROLS (AUDT) 12](#_Toc59610152)

[6.1 Device-Specific Audit Log Configuration (AUDT-1) 12](#_Toc59610153)

[6.2 Events and Attributes Recorded (AUDT-2, 3, 4) 12](#_Toc59610154)

[6.3 Audit Log Protection (AUDT-7) 13](#_Toc59610155)

[6.4 Log Export, Use, and Notification (AUDT-5, 6, 8) 13](#_Toc59610156)

[7. AUTHORIZATION (AUTH) 13](#_Toc59610157)

[7.1 Access Prevention (AUTH-1) 14](#_Toc59610158)

[7.2 Privilege and Access (AUTH-2, 3, 4, 5, SGUD-3, 3.1) 15](#_Toc59610159)

[7.3 System Use Notification 15](#_Toc59610160)

[8. CYBER SECURITY PRODUCT UPGRADES (CSUP) 15](#_Toc59610161)

[8.1 Secure Servicing and Security Upgrades Overview (CSUP-1) 15](#_Toc59610162)

[8.2 General Parameters for Updates (CSUP-7, 8, 9, 10, 11) 15](#_Toc59610163)

[8.3 Operating System Updates (CSUP-2) 15](#_Toc59610164)

[8.4 Driver, Firmware Updates (CSUP-3) 16](#_Toc59610165)

[8.5 Anti-Malware Software Updates (CSUP-4) 16](#_Toc59610166)

[8.6 COTS (non-OS) Updates (CSUP-5) 17](#_Toc59610167)

[8.7 Other Software Component Updates (CSUP-6) 17](#_Toc59610168)

[9. HEALTH DATA DE-IDENTIFICATION (DIDT-1) 17](#_Toc59610169)

[10. DATA BACKUP AND DISASTER RECOVERY (DTBK-1, 2, 3, 4, 5, 6) 17](#_Toc59610170)

[11. EMERGENCY ACCESS (EMRG-1) 17](#_Toc59610171)

[12. HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU-1, 2) 17](#_Toc59610172)

[13. MALWARE DETECTION/PROTECTION (MLDP-1) 17](#_Toc59610173)

[13.1 Support of Anti-Malware (MDLP-2) 18](#_Toc59610174)

[13.2 Other Compensation/Protection Controls (MDLP-3, 4, 5) **Error! Bookmark not defined.**](#_Toc59610175)

[14. NODE AUTHENTICATION (NAUT-1, 2, 3) 18](#_Toc59610176)

[15. CONNECTIVITY CAPABILITIES (CONN) 18](#_Toc59610177)

[15.1 Hardware Connectivity Capabilities (CONN-1) 18](#_Toc59610178)

[15.2 Communication Provisions (CONN-2, 3, 4, 5, 6, 7) 19](#_Toc59610179)

[16. PERSON AUTHENTICATION (PAUT) 19](#_Toc59610180)

[16.1 Password/ID Assignments (PAUT-1) 19](#_Toc59610181)

[16.2 User Account Management (PAUT-2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14) 19](#_Toc59610182)

[17. PHYSICAL LOCKS (PLOK-1, 2, 3) 20](#_Toc59610183)

[18. ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP) 20](#_Toc59610184)

[19. SOFTWARE BILL OF MATERIALS (SBoM-1, 3) 20](#_Toc59610185)

[19.1 SBoM Structure and Updates (SBoM-2, 4) 20](#_Toc59610186)

[20. SYSTEM AND APPLICATION HARDENING (SAHD) 20](#_Toc59610187)

[21. HEALTH DATA STORAGE CONFIDENTIALITY (STCF-1, 2, 3, 4) 21](#_Toc59610188)

[22. TRANSMISSION CONFIDENTIALITY (TXCF) 21](#_Toc59610189)

[23. TRANSMISSION INTEGRITY (TXIG-1, 2) 23](#_Toc59610190)

[24. REMOTE SERVICE (RMOT-1, 2, 3) 23](#_Toc59610191)

[25. SECURITY PROGRAM INTEGRATION 23](#_Toc59610192)

[25.1 Vulnerability Management 23](#_Toc59610193)

[25.2 Incident Response 23](#_Toc59610194)

[25.3 Security Testing 24](#_Toc59610195)

[25.4 Scanning 24](#_Toc59610196)

[25.5 Risk Management 24](#_Toc59610197)

[25.6 Training and Awareness 25](#_Toc59610198)

[26. SECURE DECOMMISSIONING 25](#_Toc59610199)

# PURPOSE

This Security Operations Manual (SOM) provides information that Stryker’s customers need to integrate a specific Stryker device or health IT solution into a customer’s IT network environment. It also supports a customer’s ability to perform risk management, to identify configurable security controls, and to better protect their systems and devices.

**Note**: This Manual is aligned with the structure of the Manufacturer Disclosure Statement for Medical Device Security (MDS2 form) in order to provide the supplemental information which is requested in the MDS2 form. The Question IDs from the MDS2 form are incorporated in the section headers to enable traceability between this document and the MDS2 form. There is no SGUD (Security Guidance) section in this document, as the entire document is the security guidance.

# DEFINITIONS

**AAMI – Association for the Advancement of Medical Instrumentation**: An organization for advancing the development, and safe and effective use of medical technology. AAMI publishes standards and technical reports related to various aspects of medical device development and use (e.g., AAMI TIR57). ~~See~~ [www.aami.org](http://www.aami.org/).

interface for computing that defines interactions between multiple software intermediaries.

**API – Application Programming Interface**: An interface for computing that defines interactions between multiple software intermediaries.

**COTS – Commercial off-the-shelf**: Software (or any other item) that is sold as a packaged solution which is then adapted to satisfy the needs of the organization purchasing the COTS. Some medical devices utilize COTS software in addition to or instead of software developed by the manufacturer. See third-party software.

**Customer**: The individual or organization responsible for procurement and operation of the device. See Owner and Operator.

**Device:** The item being integrated or used for a healthcare purpose. A Medical Device or other health IT product may be referred to as a Device or a Product in this document.

**DICOM (Digital Imaging and Communications in Medicine)**: Standard developed by NEMA and the American College of Radiology, used worldwide to store, exchange, and transmit medical images.

**FDA – U.S. Food and Drug Administration:** A federal agency of the United States’ Department of Health and Human Services. ~~See~~ [www.fda.gov](http://www.fda.gov).

**HDO – Healthcare Delivery Organization**: Also “Health Delivery Organization,” an organization or group of organizations that are involved with the delivery of healthcare services. A hospital is an HDO. If an HDO purchases and operates a Stryker device, the HDO is also the Customer, Owner, and Operator per the definitions of those terms.

**IEC – International Electrotechnical Commission**: A global organization whose work underpins quality infrastructure and international trade in electronic goods. IEC publishes thousands of international standards, including documents related to medical device software (e.g., IEC 62304). ~~See~~ [www.iec.ch](http://www.iec.ch).

**IFU – Instructions for Use**: Information provided by the manufacturer in document or electronic form, informing the user of a device’s intended purpose and proper use and of any precautions to be take.

**Integrator**: The individual or organization who installs and configures the device/system into the operator’s environment.

**ISAO – Information Sharing and Analysis Organization:** An ISAO is any entity or collaboration created or employed by public- or private sector organizations, for purposes of gathering and analyzing critical cyber and related information in order to better understand security problems and interdependencies related to cyber systems, so as to ensure their availability, integrity, and reliability (source: from NIST SP 800-150).

**ISO – International Organization for Standardization**: An international standard-setting body that promotes proprietary, industrial, and commercial standards, and publishes standards relevant for information technology, privacy, and security (e.g., ISO/IEC 27034). ~~See~~ [www.iso.org](http://www.iso.org).

**Manufacturer**: ~~The entity (Stryker) that builds the device and sells it to the customer.~~

**MDR – European Union (EU) Medical Device Regulation of 2017:** The European Union regulation concerning medical devices. ~~See~~ <https://ec.europa.eu/health/md_sector/overview_en>.

**MDS2 - Manufacturer Disclosure Statement for Medical Device Security**: A form created by the National Electrical Manufacturers Association (NEMA), intended to be completed by a medical device manufacturer and provided to customers, giving standardized information on security and privacy control features (ANSI/NEMA HN 1-2019). ~~See~~ [www.nema.org](http://www.nema.org).

**Medical Device:** ~~See the following sources if a precise definition is required: FDA, MDR (EU) 2017/745, ISO 14971:2007.~~

**NEMA – National Electrical Manufacturers Association**: ~~See~~ [www.nema.org](http://www.nema.org).

**NIST - National Institute of Standards and Technology**: A physical sciences laboratory and non-regulatory agency of the United States Department of Commerce. NIST has published comprehensive standards for the selection, implementation, and risk management of security and privacy controls (e.g., NIST SP 800-53). ~~See~~ [www.nist.gov](http://www.nist.gov).

**Operator**: The person(s) using the device for its intended purpose. This term may also sometimes refer to the person or organization responsible for procuring the device (owner, customer).

**OSS – Open Source Software**: Third party software licensed under an OSS license, in which the copyright holder grants users the rights to use, study, change, and distribute the software to anyone and for any purpose as long as the license terms are adhered to.

**Owner**: ~~See~~ Operator and Customer.

**PHI - Protected Health Information**: Individually identifiable health information (IIHI) that is transmitted by electronic media; maintained in electronic media; or transmitted, or maintained, in any other form or medium (source: extracted from 45 CFR Section 160). Note: This is a subset of PII.

**PII - Personally Identifiable Information**: Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity… and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information (source: from NIST SP 800-122).

**Product:** ~~See~~ Device.

**SaMD - Software as a Medical Device**: Software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device (source: from International Medical Device Regulators Forum).

**SBoM – Software Bill of Materials**: For a specific device, a listing of all software components that are incorporated into the final product. The SBOM may be used to assist with operational security planning by the HDO.

**SIEM – Security information and event management**: Software products and services in which security information management and security event management are combined, providing real-time analysis of security alerts generated by applications and network hardware.

**SiMD - Software in a Medical Device**: Software which is incorporated in a Medical Device and which is required for the medical device to fulfill a medical function, and/or software which is used to drive or control a hardware medical device.

**SOM - Security Operations Manual**: A product-specific guide to the secure integration of a product into a customer IT network (this document).

**Third-party software**: Third party software is software not developed by Stryker, and for which Stryker otherwise does not have complete ownership. ~~See COTS and OSS.~~

**User**: ~~See~~ Operator.

# PRODUCT DESCRIPTION

|  |  |
| --- | --- |
| **Manufacturer Name** |  |
| **Stryker Division** |  |
| **Address** |  |
| **Device Description** |  |
| **Device Model, Version** |  |
| **Manufacturer Contact Information** |  |

# Device and Manufacturer Identification (DOC-1, 2, 3, 5)

# Device Intended Use (DOC-6)

# Related Manufacturer Programs (DOC-8, DOC-9)

When Stryker obtains vulnerability information through surveillance or other sources, an assessment of the vulnerability’s exploitability and impact is conducted. Based upon this assessment Stryker determines if further actions are required like providing security updates and/or providing communication to the customer in a timely manner. Vulnerability information may also be requested from Stryker at any time.

Stryker participates in the **MedTech Information Sharing and Analysis Organization** (ISAO), a part of **AdvaMed** (Advanced Medical Technology Association).

# System Characterization and System Assets

# System Security Context and Intended Environment (SGUD-4)



While there is no specific requirement for Kneebalancer application to be fully functional other than a usual iOS environment, however Stryker recommends the user to follow some of the best security standards in order to run the application in a safe and secure environment as follows:

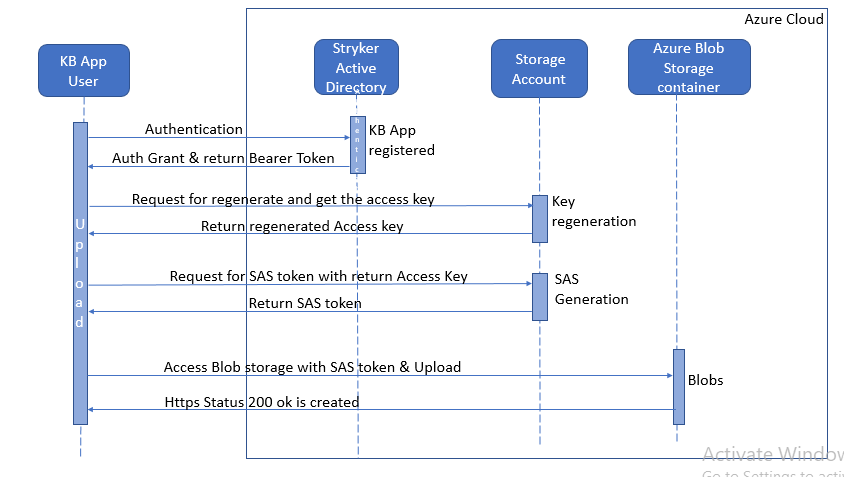
Devices operating in the intended use environment should consider that their IT infrastructure must obey different risk management approaches associated with their networks. Healthcare providers should adopt a risk management process adhering to general cybersecurity best practices to maintain the healthcare provider’s overall security status and their secure environment, as follows:

· Good physical security to prevent unauthorized physical access to device.  
· Access control measures (e.g., role based) to ensure only authenticated and authorized   
personnel are allowed access to network elements, stored information, services and   
applications.  
· General patch management practices that ensure timely security patch updates.

. Timely update of the devices and systems to prevent danger of using vulnerable software/OS  
· Malware protection to prevent unauthorized code execution.  
· Security awareness training.

# Network, Data Flow Diagram (DOC-10)

High level data flow diagram.



# Setup of SaMD (DOC-11)

# MANAGEMENT OF PII and PHI (MPII-1)

Kneebalancer application does not collect or ask user for any PII or PHI. Thus, no PII or PHI is created or stored in the device. This section is not applicable.

**Management of PII:**

Application read and process PII across the workflows. Application has the ability to import DICOM data containing PII. During the further workflow application have ability to update and include PII data in planning summary document. Application does not update the source DICOM data. As a part of safety measures application shows PII on each workflow step. Application also maintains the previous case lists on local drive. This case list file is encrypted and stored on windows user directory.

**Access control measure:**

PII data is stored in windows user directory and is not accessible to other users.

**Data Security measures:**

Files stored on the local drive containing PII is encrypted with 256-bit AES (Advanced Encryption Standard). Only authorized users having Thor Application can decrypt the files. Other users can use their key to decrypt files.

Audit logs containing the PII are encrypted. Decryption of the audit log is handled by Stryker on request from authorities.

**Data Anonymization measures:**

Application have ability to anonymize the PII shown on the application GUI on demand.

**Management of PHI:**

Application have ability to read, process and update the PHI. However, the application does not update the source DICOM data. PHI is stored in MITK files and planning summary files.

**Access control measure:**

PHI data is stored in windows user directory and is not accessible to other users.

# Authority to Collect PHI

Kneebalancer application do not collect or store any PHI of the user. Thus, this section is not applicable.

# Purpose Specification for PHI Use

Kneebalancer application does not collect or store any PHI data. This section is not applicable.

# PHI Data Quality and Integrity

Kneebalancer application does not collect or store any PHI data. This section is not applicable.

**PHI data access control measure:**

PHI data is stored in windows user directory and is not accessible to other users.

**PHI data validation:**

Application have ability to run the set of validation checks on the PHI data during import to application.

**PHI data backup and restore:**

Application does not have any mechanism to restore the lost or deleted data.

# PHI Data Deletion and Minimization (SGUD-2)

Kneebalancer application does not collect or store any PHI data. This section is not applicable.

Currently application does not have any policy defined to delete the PHI data.

Application stores the PHI data with the last update timestamp.

# Legal Roles and Related Requirements for Privacy

Kneebalancer application does not collect or store any PHI data. This section is not applicable

# Handling of Patient Requests for their PHI Access

Kneebalancer application does not collect or store any PHI data. This section is not applicable.

**Storage of PII:**

* PII is persistently stored on internal media with 256-bit AES encryption. Each licensed user has separate key and is managed internally by application.
* PII is not transferred or sent outside the operating system.

# Storage and Removal of PII (MPII-2)

Kneebalancer application does not collect or store any PHI data. This section is not applicable.**Storage of PII:**

* PII is persistently stored on internal media with 256-bit AES encryption. Each licensed user has separate key and is managed internally by application.
* PII is not transferred or sent outside the operating system.

**Storage of PII:**

* PII is persistently stored on internal media with 256-bit AES encryption. Each licensed user has separate key and is managed internally by application.
* PII is not transferred or sent outside the operating system.

# Transmitting, Importing/Exporting of PII (MPII-3)

Kneebalancer application does not collect or store any PHI data. This section is not applicable.

* The display of PII (e.g., video display, etc.)

Application displays PII information on workflow steps as a part of safety measures. Application have ability to anonymize the PII data on display.

* Generation of hardcopy reports or images containing PII

Application includes the PII data in planning summary document which can be printed or transmitted.

# AUTOMATIC LOGOFF (ALOF-1, 2)

Application do not lock the device after being idle for certain time period. ~~Customers~~ are advised to configure iOS device to automatically lock the screen after a reasonable period of time as per HDO IT policies.

# AUDIT CONTROLS (AUDT)

The Kneebalancer application have ability to capture and store important event and actions as part of audit logs. These logs are stored on the device in the application’s sandbox directories. These logs are accessible to Kneebalancer application only. Any other application installed on same device or user of the device cannot access or does not have control over these logs. Audit logs are an important part of any secure system, and they need to be carefully designed in order to give a faithful representation of past system activity.

The audit logs do not contain any sensitive information or PII or PHI. Users are not required to take any special measures to protect these logs but are not restricted from doing the same. The audit logs are uploaded along with case data and stored in Azure cloud with the security and encryption as provided by the Azure cloud. These logs are removed from the device within period of 30 days if not uploaded on storage server of Stryker. The logs are deleted from the device once they are uploaded to the cloud.

# Device-Specific Audit Log Configuration (AUDT-1)

The application captures the audit logs and stores in the specific secure location on the device. Audit logs are not configurable by user. No PII is logged in these audit logs.

# Events and Attributes Recorded (AUDT-2, 3, 4)

Application captures the errors and exceptions in JSON format. These logs only contain errors and exception occurred in device and the Kneebalancer application. Logs are pushed to cloud whenever the device comes online and if there is past case data waiting for upload. As soon as user provides his credentials and if past case data is available, all the logs are pushed to cloud. Any sort of user information is not logged in these events and attributes being recorded in these logs. Log details will be stored with combination of error details, crashing details, exception details, and event logs. The events and attributes recorded in these log files are as below:

* Application/Device errors
* Application/ Device exceptions
* Case data logs
* Event logs (Tracking)

# Audit Log Protection (AUDT-7)

The audit logs are captured and stored in the specific location in the device by the application. These logs are stored in special sandbox directory of the application inside iOS device’s local memory. The user of device or any other app installed on the same device do not have any control over these logs. These logs are not protected by any protection mechanism as they are stored in secure mechanism at first place. Moreover, these logs do not contain any sensitive or PII/PHI data.

These logs get uploaded on the Stryker’s storage server along with the case data. Once they are uploaded on the storage server, they are removed from the local memory of the device. The logs also contain debug errors and reports of the device and the application which also gets removed once uploaded on the Stryker’s server. The audit logs are transmitted and stored in Azure cloud with the security and encryption as provided by the Azure cloud. These logs are deleted from the device within period of 30 days if not uploaded on storage server of Stryker.

# Log Export, Use, and Notification (AUDT-5, 6, 8)

Kneebalancer application does not have any built-in feature to store backup of logs (like in case of data deletion). It is also not possible to export these logs using any wireless or physical media as these logs are only accessible to Kneebalancer application only.

The logs contain specific actions of the application, crash reports, debug reports and errors, application’s behavioral reports which are stored on the local storage on the device in specific location assigned to Kneebalancer application only. These logs are isolated from users of device and any other app on same device and are limited to Kneebalancer application only. These logs get deleted from the device within period of 30 days if not uploaded on storage server of Stryker.

# AUTHORIZATION (AUTH)

Kneebalancer application can be installed via authorized entity of Stryker. Once installed, application does not enforce any authorization mechanism to access the application. The application is installed on Stryker’s authorized devices via Stryker’s app store only and Stryker admin must approve the installation of the Kneebalancer application on Stryker’s device. A single user can log in via *Microsoft Authentication Library (MSAL)* mechanism on the device to upload case data to the Stryker’s storage servers.

Authorization in system security is the process of giving the user permission to access a specific resource or function. In secure environments, authorization must always follow authentication. In order to upload the case data on the server, the user is required to login into the application via Single sign on authentication mechanism with their own account.

# Access Prevention (AUTH-1)

This section is not applicable as a single user can be logged in into the application via single sign on authentication mechanism to use features of the application such as case data upload.

However, taking steps to prevent unauthorized access to the device and its software components is important for a wide number of reasons, including preventing unauthorized malicious actors from installing spyware, malware and deleting your important files, or further creating viruses. By making changes to your iOS devices to prevent unauthorized access, you are also protecting your personal privacy. Here are some steps to take to properly secure your iOS device and prevent others from accessing or modifying your application data:

* Set password/pin protection for unlocking the device: The iOS device must be protected with password, pin, or any other kind of authentication to prevent unauthorized parties from unlocking the device.
* Strong password/pin protection for device: The implemented authentication mechanism such as password, pin etc. must be set in such way that it must not be easy to guess.
* Install any applications from Appstore of Apple only. This will ensure installation of un-tampered applications. Additionally, install only required applications in your iOS device. This will also prevent any malicious or spyware application installation which are usually bundled or hidden in the normal applications.
* Restrict the access to your iOS device only to limited number of trusted peoples. This can help the installed application to be accessed only by an authorized individual.
* Keep your Apple ID secure. Your iCloud data and account details for services like the App Store and Apple Music are accessible through your Apple ID. Keep your Apple ID secure on iPhone to prevent any unauthorized access to data on iCloud and access to some of the features of device such as location information, notifications, personal information etc.
* Do not connect to any open or public wireless network. Always connect and use application while connecting to trusted wireless network. Do not connect to wireless network with misconfigured or old configuration such as WPS enabled, use of WEP, WPA1 mechanism in wireless network.
* Do not connect to any untrusted Bluetooth devices. Further keep Bluetooth option disabled if not being utilized.

# Privilege and Access (AUTH-2, 3, 4, 5, SGUD-3, 3.1)

Privilege, in the context of security, is the concept of only allowing users to do certain things. For example, an ordinary user is typically prevented from changing operating system files, while a system administrator is typically permitted to do so. As the Kneebalancer application do not have multiple access roles, this section is not applicable.*, I If the device is integrated with enterprise or upstream identity and access management capability, describe that here.*

# System Use Notification

Note - This section is not applicable

*If the device is integrated with enterprise or upstream identity and access management capability, describe that here.*

# CYBER SECURITY PRODUCT UPGRADES (CSUP)

***Existing Security Features:***The Kneebalancer application does not have any updates installation policy implemented. Hence, the users don’t get any notification of online updates. If Stryker identifies any potential vulnerabilities which require an update at the customer site, a new version of the application will be released, and customers will be informed about the action to be taken at their end.

***Recommendation for ~~customer (HDO):~~*** Any information regarding cyber security product upgrades can be requested from Stryker.

# Secure Servicing and Security Upgrades Overview (CSUP-1)

The application does not have any updates installation policy implemented at the time of release. Users will not get any online updates in fixed cycle. The application update is possible only at the next release of the application which depends on major/minor changes such as features, security fixes, etc. However, it is recommended for the users to apply their operating system patches and their third-party components (if any) to maintain the system security.

Apple usually release security updates for iOS as soon as issues are patched. These updates address various bugs and vulnerabilities which are being exploited in the wild. Security updates are just patches which comes with feature enhancements, performance improvement, bug fixes, etc. General bug fix update is usually between 6 months and the major update in iOS generally pushed every 1-1.5 years.

On patching these security updates, your device will become more secure with enhanced protection as well as performance.

# General Parameters for Updates (CSUP-7, 8, 9, 10, 11)

# Operating System Updates (CSUP-2)

Outdated operating system is the weakest links. When you have outdated OS, you aren’t only missing out on few new features or a slightly faster program. You’re also exposing your business to vulnerabilities and security risks.

It is recommended for the users to keep your Apple iOS updated to ensure the device running smoothly and securely. When you update, you’ll get the latest fixes and security improvements, helping your device run efficiently and stay protected. Important and high-priority updates are critical to the security and reliability of your iOS device. Updates offer the latest protection against malicious online activities. Not keeping your operating system up to date can result in serious issue, affecting both your device and your own personal security. These include:

* Vulnerable OS components due to missing patches.
* Crashing, lagging, basically poor performance.
* Various viruses, spyware, malicious threat actors and other malwares
* Various cybercrime attacks
* Incompatibility for certain security features which are available in antivirus apps but unable to implement due to old and incompatible OS version.

# Driver, Firmware Updates (CSUP-3)

**Note: This section is Not Applicable**

# Anti-Malware Software Updates (CSUP-4)

Kneebalancer application does not contains any malware protection embedded. Thus, users are expected to take care of the installations and configuration of anti-malware software themselves. An anti-malware is a software/application that protects the device from various malware such as adware, worms, crypto mining malware, spyware, etc. Anti-malware application scans the device and OS components for all types of malicious software applications, outdated software, among all of the installed applications or hidden inside any application which manage to reach to the device.

The software updates of anti-malware comprise of latest files needed to combat the latest threats and safeguard your device. Hence, it is really important to update these applications as soon as updates are available for them. If these applications are not updated for long time, it is like not having them on the device.

As the database of anti-malware application is regularly gets updated with signatures and information of latest threats, malware, spywares etc. Thus, updating these applications also helps you to detect any recent malware installed into your iOS device. As iOS itself offers lots of security features to battle against those malwares however, it is highly recommended to purchase and use any good anti-malware application to avoid any slip of malware due to misconfiguration of security feature offered in iOS.

# COTS (non-OS) Updates (CSUP-5)

**Note: This section is Not Applicable**

# Other Software Component Updates (CSUP-6)

**Note: This section is Not Applicable**

# HEALTH DATA DE-IDENTIFICATION (DIDT-1)

Kneebalancer application does not collect or store any sensitive information or PII or health data of the user. Thus, this section is not applicable.

# DATA BACKUP AND DISASTER RECOVERY (DTBK-1, 2, 3, 4, 5, 6)

The application does not contain any online or offline mode of data on device or its recovery. The purpose of the backup is to create a copy of data that can be recovered in the event of a primary data failure. The case data gets uploaded on the azure storage server of Stryker once, user is logged-into the application.

# EMERGENCY ACCESS (EMRG-1)

**Note: This section is Not Applicable**

# HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU-1, 2)

The application does not store any sensitive information on the iOS device or on the Stryker’s server. Thus, this section is not applicable.

# MALWARE DETECTION/PROTECTION (MLDP-1)

By default, the standalone Kneebalancer application does not have any malware detection features and requires the user to have some malware detection in place in their iOS device. Due to the ubiquity of malware, malware detection is essential since it serves as an iOS device’s early warning system for malware and cyberattacks. It stops hackers from remotely accessing the device and guards against data breaches. To do this, an iOS device and its files must be scanned for malware. To protect against the malwares below points are recommended:

* Keep your iOS device and installed application updated. Auto update feature must be enabled in Appstore and in device’s settings
* Use strong password/pin code to unlock the device
* Do not click on any URLs or download anything from the internet or received via airdrop
* Limit your file-sharing over internet or locally via airdrop
* Install a good malware detection and mitigation application on the device
* Be careful about opening email attachments or images. Configure the mail server to restrict auto download or auto rendering of images received in emails outside organization.
* Always download applications from Apple’s Appstore. Moreover, install only required application on the device.
* Do not provide any unnecessary permissions (to access system component, data) to any other installed application.

# Support of Anti-Malware (MDLP-2)

The application does not contain any anti-malware functionality within itself. Also, it does not restrict users to install any types of anti-malware programs supported by their operating system. Hence, users are best recommended to purchase and install some of the popular anti-malware programs on their own.

# NODE AUTHENTICATION (NAUT-1, 2, 3)

As application do not have any ability to communicate between multiple devices, this section is not applicable.

# CONNECTIVITY CAPABILITIES (CONN)

All network and removable media connections must be considered in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device.

# Hardware Connectivity Capabilities (CONN-1)

The application itself do not need to connect to any physical media to be connected to the device and does not apply any restrictions in place for the same. However, it is advised for the users to not connect any physical media to the iOS device via OTG connection capability.

The application does require to communicate over the network to transfer the data. It utilizes the wireless connection capability of the device. Users are advised to connect to secure wireless connections only. The wireless connection must be configured on WPA2 protocol along with strong connection password. Do not connect to any public or unsafe wireless connections.

Apart from the wireless network connectivity, application do not require to connect to any other wireless protocol such as Bluetooth, airdrop, NFC etc.

# Communication Provisions (CONN-2, 3, 4, 5, 6, 7)

The application has ability to connect to network via wireless connectivity feature. The connection is made in order to communicate with Stryker’s storage server to store case data, audit/debug logs on the Stryker’s server. The application has ability to make API calls back and forth to transfer the data mentioned above. These API calls are used to upload case data to the Stryker’s azure storage servers. The data is transmitted and stored in Azure cloud with the security and encryption as provided by the Azure cloud.

# PERSON AUTHENTICATION (PAUT)

Kneebalancer application has the person authentication ability to authenticate user for specific features to work. This authentication is done via single sign on authentication mechanism. The user account which is logged into the Stryker’s device where the Kneebalancer app is installed can login into the application via single sign on feature. The authentication happens over the network. The application communicates with Microsoft’s servers in order to authenticate the user via single sign on authentication mechanism.

# Password/ID Assignments (PAUT-1)

The Stryker admin must approve the installation of Kneebalancer application on the Stryker device. The user can log in into the application via MSAL single sign on authentication mechanism. The application does not have ability to create/manage user account or password.

# User Account Management (PAUT-2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14)

The Kneebalancer application can be installed on the Stryker’s own iOS device from Stryker’s app store after approval from the Stryker’s admin. The user can login into the application with single sign on authentication mechanism via MSAL authentication.

The application communicates with MSAL servers to authenticate user into the application via single sign on. There is only single user who can access the application on a device. Thus, this section is not applicable. Users are requested to follow basic security hygiene to secure the iOS device:

* The device should get locked after left idle after reasonable period.
* Physical security should also be considered to manage access to the device.

# PHYSICAL LOCKS (PLOK-1, 2, 3)

Note-This section is not applicable.

# ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)

The app uses the iOS platform which publishes the apps with greater security from the manufacturer using provisioning files and certificates.

# SOFTWARE BILL OF MATERIALS (SBoM-1, 3)

# SBoM Structure and Updates (SBoM-2, 4)

It is addressed in the Software Development Plan prepared by Stryker.

# SYSTEM AND APPLICATION HARDENING (SAHD)

Systems hardening is a set of technologies, approaches, and best practices designed to reduce vulnerability in applications, systems, and other areas. Systems hardening aims to lower security risk by removing potential attack routes and reducing the attack surface of the system.

With the proper system hardening, attackers and malware agents have next to none opportunities to penetrate your IT environment by to gain a foothold within your IT ecosystem. Systems hardening demands a methodical approach to audit, identify, close, and control potential security vulnerabilities. The kind of hardening you implement relies on the risks associated with your current technology, the resources you have, and the importance of fixing problems. The essential ideas that are advised to be considered while putting the system hardening into practice are listed below:

* **Audit your existing systems:** Carry out a comprehensive audit of your existing technology. Use penetration testing, vulnerability scanning, configuration management, and other security auditing tools to find flaws in the system where the application is installed and prioritize fixes.
* **Create a strategy for systems hardening:** You do not need to harden all of your systems at once. Instead, create a strategy and plan based on risks identified within your technology ecosystem, and use a phased approach to remediate the biggest flaws.
* **Patch vulnerabilities immediately:** Ensure that you have an automated and comprehensive vulnerability identification and patching system in place.
* **Network hardening:** Ensure your firewall is properly configured and that all rules are regularly audited; secure remote access points and users; block any unused or unneeded open network ports; disable and remove unnecessary protocols and services; implement access lists; encrypt network traffic.
* **Operating system hardening:** Apply OS updates, service packs, and patches automatically; remove unnecessary drivers, file sharing, libraries, software, services, and functionality; encrypt local storage; tighten registry and other systems permissions; log all activity, errors, and warnings; implement privileged user controls.
* **Eliminate unnecessary accounts and privileges:** Enforce least privilege by removing unnecessary accounts (such as orphaned accounts and unused accounts) and privileges throughout your IT infrastructure.
* **Update system as well as other installed apps:** Configure Appstore to auto update third party and system apps as soon as update is available.
* **Network hardening:** Before connecting to any wireless network, ensure that wireless network is secure and is running on latest protocols. Also, do not connect to any public or open wireless network. It is also recommended to connect to trusted wireless networks only. Ensure your organization’s firewall is properly configured with all rules and is regularly audited.
* **Wireless interfaces hardening:** Along with the wireless network interface, other interfaces such as Bluetooth, RFID, NFC interfaces should be hardened. Configure best possible security mechanism such as connect only to Bluetooth version 3.0 devices, do not connect to external NFC devices automatically etc.

# HEALTH DATA STORAGE CONFIDENTIALITY (STCF-1, 2, 3, 4)

The application does not collect or store any sensitive health data. This section is not applicable.

# TRANSMISSION CONFIDENTIALITY (TXCF)

Data confidentiality is about protecting data against unintentional, unlawful, or unauthorized access, disclosure, or theft. Confidentiality has to do with the privacy of information, including authorizations to view, share, and use it. Information with low confidentiality concerns may be considered "public" or otherwise not threatening if exposed beyond its intended audience. Information with high confidentiality concerns is considered secret and must be kept confidential to prevent identity theft, compromise of accounts and systems, legal or reputational damage, and other severe consequences. As the application stores, the data in encrypted form any data loss or theft is protected from being subjected to the loss of confidentiality.

Kneebalancer application transmits the data over the network via API calls. The data created by user in the application will be transfer via network to the Stryker’s server/storage facilities. The data for storing in device and to transit does not contain any sensitive data such as patient information, credentials or certifications. However, the data is transmitted and stored in Azure cloud with the security and encryption as provided by the Azure cloud.

User are requested to follow some of the guidelines to be followed while managing data confidentiality.

**Manage data access**: Controlling confidentiality is, in large part, about controlling who has access to data. Ensuring that access is only authorized and granted to those who have a "need to know" goes a long way in limiting unnecessary exposure. Users should also authenticate their access with strong passwords and, where practical, two-factor authentication. Periodically review access lists and promptly revoke access when it is no longer necessary.

**Physically secure devices**: Controlling access to data includes controlling access of all kinds, both digital and physical. Protect devices from misuse or theft by storing them in locked areas. Never leave devices or sensitive documents unattended in public locations.

**Securely connect to wireless network:** Connecting to the secure wireless network ensure confidentiality, integrity and availability of the data during transmission.

**Securely dispose of data**: When data is no longer necessary for any-related purposes, it must be disposed of appropriately.

**Manage data acquisition:** When collecting sensitive data, be conscious of how much data is actually needed and carefully consider privacy and confidentiality in the acquisition process. Avoid acquiring sensitive data unless necessary; one of the best ways to reduce confidentiality risk is to reduce the amount of sensitive data being collected in the first place.

**Manage data utilization:** Confidentiality risk can be further reduced by using sensitive data only as approved and as necessary. Misusing sensitive data violates the privacy and confidentiality of that data and of the individuals or groups the data represents.

**Manage devices**: By protecting devices, you can also protect the data they contain. Follow basic cybersecurity hygiene by using anti-virus software, routinely patching software, using device passcodes to unlock the device, installing apps only via Appstore.

# TRANSMISSION INTEGRITY (TXIG-1, 2)

*The ability of the device to ensure the integrity of transmitted data.*

**<<This section is tentative. Can be updated once SSL pinning status is confirmed>>**

# REMOTE SERVICE (RMOT-1, 2, 3)

**Note-This section is not applicable.**

# SECURITY PROGRAM INTEGRATION

This section provides configuration guidance to enable the customer to achieve compliance when integrating the product.

# Vulnerability Management

Section 3.3, Related Manufacturer Programs, defines Stryker’s process for vulnerability identification, assessment, and communication. See Section 8, CYBER SECURITY PRODUCT UPGRADES, for information regarding software patches.

# Incident Response

***Existing Security Features:***Only Stryker’s service engineer is authorized to visit & perform maintenance of the Kneebalancer solution components (device, tablet) on need basis, maybe at the time of incident reported. When Stryker obtains vulnerability information through surveillance or other sources, an assessment of the vulnerability’s exploitability and impact is conducted. Based on the assessment report, Stryker determines if further actions similar to providing security updates and/or providing information to the customer in targeted time. Vulnerability information may also be requested from Stryker at any time. Malware detection is crucial as attackers can exploit the system in multiple ways and hence it can serve as an early warning regarding cyberattacks. Only Stryker Technical Team is authorized to repair or resolve issues whenever a severe malware is detected.

Vulnerability Management Process/Practice(s) usually followed includes:

* Usage of Vulnerability/Malware scanning tools
* Onboarding the application/infrastructure to the scanning tool
* Identification and prioritization of the vulnerability as per vulnerability rating such as Critical, High, Medium, and Low
* Planning the vulnerability remediation/mitigation steps
* Integration of the solution and revalidation of the reported vulnerability

For following observations Incident Reporting & Recovery can be initiated:

* Any suspected/confirmed malware found on the system
* Any unexpected system behavior observed
* Any suspected misuse of the device (can confirm through logs)
* Incorporated methods detect that any data inappropriately accessed or copied from the device
* From the report of forensic inspection of the device
* Chances for recovery of data from a damaged or non-functional system

Guidelines to the customer (HDO):

Customer (HDO) is recommended to be up to date with the software being used or latest hardware

* Customer (HDO) needs to test or validate the effectiveness of the system functionality from security perspective at regular intervals
* Functional testing should be performed to identify the weaknesses/vulnerabilities that can be exploited

Risk Management:

* Customer (HDO) needs to conduct security risk identification process which monitors the ongoing security posture of this device/infrastructure and reports any security incidents that might arise.
* Risk assessment should be conducted within the organization to identify the gaps and plan improvements

Training and Awareness:

* Staff members utilizing the devices should be provided with proper training including their functionality
* Customer (HDO) needs to evaluate the security training requirements for this product and also identify any standard user security awareness training needed to users from business perspective.
* Workforce members utilizing medical devices should be appropriately trained.
* Medical device owners or designees should train appropriate workforce members on the use of the medical device that address any issues/concerns related to its use.

***Recommendation for customer (HDO):*** Customer’s role is limited to incident reporting & not responsible for the remediation*.* Please reach out to Stryker Customer Care for incident response. Whenever severe malware is detected, it is resolved by the Stryker service engineer. The customer has to block few IOCs and IOAs in their network devices. The customer is highly recommended to use the network firewall. Kneebalancer solution should be behind a stateful firewall. The firewall helps in preventing network access to devices. If properly configured and used, it can lead to protected and reliable accessibility. It can help in prevention of unauthorized access and network connections that can lead to external threats, IP spoofing & routing attacks and malicious packets.

# Security Testing

The product is installed on an iOS operating system, and Stryker has evaluated that standard security testing methodologies commonly employed for the Operating System type are appropriate. No special procedures for security testing are required beyond those typically applied to the Operating System.

# Scanning

The Kneebalancer application requires to communicate over the internet for authentication and data transfer. Hence, it is required for customer to have network level vulnerability scanning mechanism implemented. Also, Stryker has already done extensive security testing of the application at the time of release. However, beyond this security measures in place it is advised for the users to take a step ahead and follow some of the below guidelines to ensure better security postures:

* Do not connect to any public or open wireless network. Only connect the device to trusted wireless network. Also, do not connect to any wireless network which has enabled old or outdated protocols such as WPA or WPS.
* Do not connect to any insecure wireless interfaces such as Bluetooth, NFC etc.
* Device should be scanned on regular basis with anti-malware application for detection and mitigation of any threats and spywares

Do not install any application from place other than Apple’s Appstore. Also, do not install unnecessary applications in the device.

# Risk Management

* Customer (HDO) needs to conduct security risk identification process which monitors the ongoing security posture of this device/infrastructure and reports any security incidents that might arise.
* Risk assessment should be conducted within the organization to identify the gaps and plan improvements

# Training and Awareness

Stryker has evaluated the security training requirements for this product and determined that standard user security and awareness training commonly provided to users of general-purpose business environments is sufficient for standard users. This general security awareness may include the below points:

* Do not connect to any public or open wireless network. Only join a reliable wireless network with the device. Additionally, avoid using any wireless networks that have WPA or WPS enabled if possible.
* Along with wireless network interfaces, do not connect and communicate with other insecure or public wireless interfaces such as Bluetooth, NFC, airdrop communication
* Use strong pin or passcode to unlock the device. This reduces the risk of unattended device access.
* While device is connected to the internet, do not click on any unknown link’s or do not download any files that may be a potential security threat to the system as well as to the application.
* System should be updated on a regular basis and general anti-malware scanning should be performed.
* Do not connect any external drive such as USB drive via OTG cable or plug to the device. Do not connect the charging interface to insecure connection port.

# SECURE DECOMMISSIONING

***Recommendation for customer (HDO):*** Please reach out to Stryker Customer Care for secured decommissioning of Stryker owned Kneebalancer components such as (iOS device, tablets)*.* Components owned by HDO should follow the HDO IT policies for secure decommissioning.

# Appendix

# List of 3rd party components:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Title | Manufacturer | Version | Release Date | License Type | Maintenance procedure |
| MITK | MITK | 2018.04.02 | 13/03/2019 | BSD | Dynamically linked, Embedded in product |
| Qt | Qt | 5.11 | 22/05/2018 | Qt Commercial License, GPL 2.0, 3.0, LGPL 3.0 | Dynamically linked, Embedded in product |
| VTK | VTK.org | 8.1 | 22/12/2017 | BSD | Dynamically linked, Embedded in product |
| ITK | ITK community | 4.13.1 | 13/08/2018 | Apache 2.0 license | Dynamically linked, Embedded in product |
| CTK | Commontk.org | 0.1.0 |  | Apache 2.0 license | Dynamically linked, Embedded in product |
| Log4cpp | Lifeline Networks bv | 1.1.1 | 26/11/2013 | GNU Lesser General Public License. | Dynamically linked, Embedded in product |
| boost | boost | 1.69.0 | 12/12/2018 | Boost software license | Dynamically linked, Embedded in product |
| tiff | Adobe | 4.0.7 |  |  | Dynamically linked, Embedded in product |
| teem |  | 1.11.0.5 |  | GNU Lesser General Public License. | Dynamically linked, Embedded in product |
| minizip | zlib | 1.1 |  | zlib license | Dynamically linked, Embedded in product |
| cppunit |  | 1.14.1 |  | GNU Lesser General Public License. | Dynamically linked, Embedded in product |
| tinyxml2 | zlib | 4.0.1 |  | zlib license | Dynamically linked, Embedded in product |
| opencv | Opencv.org | 4.1.0 | 8/04/2019 | open-source Apache 2 License | Dynamically linked, Embedded in product |
| DCMTK | Dcmtk.org | 3.6.4 | 30/11/2018 | BSD | Dynamically linked, Embedded in product |
| OpennGL | The Khronos Group |  |  | BSD | Dynamically linked, Embedded in product |