EndoSize

Software version 3.1.x

Software Safety Information and Precautions

Change history

Date	Version	Description
2023-01	SafetyInfoPrecau-EndoSize-EN-1.0	Initial version – Taiwan requirements (and potentially US) for Cybersecurity

Manufacturer

Therenva SAS
74 F rue de Paris
35000 Rennes
France

Phone: +33 9 72 52 29 18
Fax: +33 9 72 52 54 16
E-mail: contact@therenva.com
Web site: www.therenva.com

Support:
Phone: +33 9 72 52 29 18
E-mail: support@therenva.com

CE 0476

℞ ONLY

Contents

PART 1 – Software environment

1. IT Security

To minimize risks linked to IT, the user needs to comply with software and hardware minimum requirements.

The Software has been developed and tested using the hardware components and software application versions described in the user manual.

It is the user's responsibility to assure a safe, validated, and functioning environment. This includes getting a proper level of training, providing protecting systems, controlling medical devices from cyber-security threats, and performing maintenance on hardware.

The physical security for PCs, server hosts and database are not provided by Therenva.

2. Network Security

The network security is under the responsibility of the user's organization.

It is recommended that the network on which the Software is used has effective security procedures in place, including physical and network access control.

3. Compatibility and Interoperability

Some software applications or operating systems which are not under the control of Therenva such as antivirus, VPN, firewall running on the computers where the Software is installed

- may impair the performance and effectiveness of the device or its integrity.
- may block the installation or proper running of the Software.

If you have any suspicions or experiencing troubles, please contact the Support.

4. Malicious code protection

To the knowledge of Therenva, the Software does not contain any time bomb, virus, malware, worm, Trojan horse, spyware or any other code designed or intended to have, or capable of performing or facilitating, any of the following functions: disrupting, disabling, harming, or otherwise impeding in any manner the operation of, or providing unauthorized access to, a computer system or network or other device on which such code is stored or installed.

Therenva implements reasonable measures designed to prevent the introduction of Malicious Code into its Proprietary Software Devices, including firewall protections and regular virus scans of its computer fleet.

It is up to the user to take all appropriate measures to protect his own data and materials from contamination by viruses or other forms of attack.

5. Software Integrity

The integrity of the Software is guaranteed by Therenva through the use of specific tools for software development, configuration management and maintainability over time (e.g. code review, static analysis).

The modification, decompilation, disassembling, reproduction, translation or recreation of the Software, even partially, or attempt or allow third parties to perform such acts is not permitted in any way by Therenva and may be subject to legal action.

In the event that the user wishes to obtain information enabling the interoperability of the Software with other software, the user undertakes to consult Therenva or its distributor in order to find out if such information is not quickly and/or easily accessible, and in this case, to limit the reproduction of the code or the translation of the code to only those parts of the program necessary for the implementation of the aforementioned interoperability.

6. SW updates and patches

The Software and third-party software or systems such as SOUP - Software of Unknown Provenance or Operating Systems) may be updated or otherwise modified, including, but not limited to, for the purpose of error correction and improvement of functions or performances (security included).

All Software updates and patches required for reasons of operational security (e.g. known or suspicious vulnerabilities) must be installed by the user (with the support of Therenva if required) without undue delay. If the Customer refuses such an update/patch, Therenva will not guarantee the operational stability and security.

It is recommended not to enable automatic updates to operating systems on computers on which the Software is installed to keep control over the updates made. Therenva strives to test the software on the latest OS versions but for safety, manual updates are recommended.

Therenva does not provide Software update/upgrades by email. You may need to be suspicious of any email messages that claim to have a software update file attached – these attachments may contain malware.

The updates, upgrades or patches for the Software are proposed on a regular basis.

If you are connected to the internet, an update wizard opens automatically at the software launching. Updates are recommended but you are free to install or postpone the update.

If you cannot be connected to the internet (“offline license”), the person in charge of the maintenance of the software, whose contact data was given to Therenva at the time of the first installation of the software, is informed by the Therenva teams that an update is available. In this case, Therenva will provide the installation file for the update, preferably by secure online transfer or other means (to be agreed upon).

Software update may be installed remotely by Therenva's staff or by trained specialists (with your prior notification and consent) but never over an untrusted network. A secured connection must be imposed.

Prior to any update/upgrade or patch application, it is recommended to check the procedures in place for backing up and restoring data, and to ensure that the data can successfully be restored from earlier backups.

7. Event Detection and Logging

A logging system is created as soon as the program starts.
All events related to user actions and system processes are detailed in a log file.
This temporary file is in the applications data folder of the PC default disk, before being deleted at the software closing.
In the event of an error during program execution, the file is sent to our license server before deletion, for analysis purposes.
The log files are not encrypted. They do not contain any personal data.

8. Denial of service protection

EndoSize does not provide specific protection against denial-of-service attacks. EndoSize has to be used only in a clinical environment protected from remote attacks by the Healthcare Establishment's network.

PART 2 – Privacy and Security Information

1. Authorization

Therenva does not allow any modification of the software code by a third party or even the installation of a version of the software prior to the latest authorized version, in order not to allow potential attackers to exploit vulnerabilities that Therenva would have avoided.

The user undertakes to use its best efforts and to take all necessary measures to prevent access to the Software by any unauthorized person as well as any unauthorized copying, publication, disclosure and/or distribution of the Software, in whole or in part, in any form whatsoever.

2. Authentication

EndoSize is standalone software installed of a staff or individual PC and by implication requiring admin privileges.

EndoSize access is then permitted if the license key, provided by Therenva at purchase and entered by the user at the first launch, is valid.

EndoSize is also protected by a password upon starting.

The software is provided with a user agreement that grants the user a non-transferable license for its sole and exclusive use with the hardware provided or intended by Therenva.

3. Remote access

It is the customer's responsibility to provide an encrypted VPN - or another access mechanism - if access is needed outside of the Healthcare Facility.

4. Encryption

EndoSize does not apply any encryption of data.

The protection of sensitive data is controlled by the Healthcare Facility's systems and data security policy.

5. Patient data confidentiality

It is strongly recommended that access to patient records be protected from anyone not subject to medical confidentiality.

To prevent unauthorized access to patient data:

When leaving the device unattended for any length of time, be sure to properly close all applications and software access.

6. Pseudonymisation/Anonymization

In the context of its service activities, Therenva will favor anonymization over pseudonymization because the company has no need or even legitimacy for re-identification. The principle of using data strictly essential to the processing is applied.

PART 3 – Vulnerability communication plan

Therenva has addressed cybersecurity risks from the earliest phases of product design. The scope of cybersecurity risk management is the device in its environment of use, with its external interactions and the risks that can impact the patient, but also the architecture of the device and the proper functioning of the device, the data (confidentiality, integrity, etc.) and the company. Risks are re-evaluated with each software modification plan and according to feedback and field observations, particularly from post-marketing surveillance activities (bug and incident analysis, treatment of escalated vulnerabilities from other parties, proactive review of vigilance events/security vulnerabilities).

Depending on the criticality of the potential or proven risk, a security update may be essential. In these cases, Therenva's Support teams or representative staff will inform you as soon as possible and help you to make your installation safe.