Vitrolife security and privacy guide

Recommended cyber security practices

Table of contents

1 Introduction

This guide provides information on how to use the Vitrolife products in the best possible way in terms of cyber security and privacy. It is thus a guideline of best practices for users of the system to minimise risks from cyber security threats and to safeguard personal information when using the Vitrolife products.

In this guide, all references to incubators cover both EmbryoScope D, CulturePro, EmbryoScope+, EmbryoScope Flex and EmbryoScope 8 incubators. References to clients cover EmbryoViewer and Vitrolife Technology Hub.

2 General security instructions

Users are advised to read and understand the following general security instructions before using the Vitrolife products:

- Never connect the Vitrolife products to the internet without implementing proper security measures. Unauthorised internet exposure may lead to cyber threats and compromise sensitive data.
- Firewall protection: The Vitrolife products should be installed on a local network behind a firewall to safeguard them against external threats.
- Responsibility of the clinic’s IT department: It is the responsibility of the clinic's IT department to ensure that sufficient cyber security measures are in place. Clinics are advised to engage with local security experts for assistance in establishing a secure infrastructure.
- Incident response: In the event of a cyber security incident, clinics should promptly reach out to cyber security experts for assistance and resolution.

3 Recommended cyber security practices

When setting up or operating the Vitrolife products, please follow the recommended practices described in this section to minimise any potential security risk and to keep data, including personal information, as safe as possible.

3.1 General cyber security recommendations

Users are advised and expected to take the following measures to reduce cyber security risk to ensure that the products will work as designed in the intended user environment:

- Ensure that personnel are properly trained in cyber security awareness
- Prevent physical access to the equipment by unauthorised users

- Read this guide of recommended practices to reduce cyber security risk.

Users must inform Vitrolife A/S without any undue delay upon becoming aware of a cyber security vulnerability incident or any suspected security events.

3.2 User cyber security awareness

To minimise the risk of any security-related issues that may compromise the system, devices or data, including personal information, please observe the following guidelines:

- Do not allow any unauthorised person to see your screen actions.
- Keep your user account personal, and do not let others see your credentials.
- When leaving an incubator or a client workstation, enable the screen saver function and/or lock the user interface.

Clinics should appoint a security contact inside the organisation that users can consult if they have questions or encounter any suspicious behaviour.

3.3 Use of portable media

It is recommended to limit the use of portable media such as USB sticks, external hard disks, memory cards, etc. If you use portable media to transfer data, you should take the following precautions:

- Check the portable media for malware and viruses before inserting them into any Vitrolife product or computer running Vitrolife software.
- Encrypt the data on the portable media to avoid compromising personal information if the media are lost.
- Only store sensitive data in secure places.
- Delete the portable media’s data content when the data have been transferred.
- Never use portable media of unknown origin.

3.4 Computers connected to the internet

The Vitrolife products can be connected to a network with internet access, and precautions should be taken to avoid exposure to cyber threats from remote locations. To minimise the risk of unauthorised intrusion into the system and its data:

- Set up the internet connection with the latest available software security features, e.g. firewall, network surveillance and intrusion detection systems, etc., as recommended by the clinic’s IT department.

- Ensure that reliable antivirus and antimalware software is installed to safeguard against malicious software.
- Always follow Vitrolife's recommendations for keeping the operating system updated with the latest security patches.
- Enable restricted internet access.
- Avoid any unnecessary access to internet sites that are not strictly work-related.

3.5 User administration and passwords

Please observe the following guidelines to ensure that only authorised use of the system and resources is permitted:

- Only set up the required number of users (user accounts) in the system.
- If a user account is not to be used anymore, remove it completely from the system.
- Do not use shared user accounts. Every account must be individual to a person.
- Limit a user account's access level to what the user needs to carry out his or her work.
- Ensure that the password for a user account is strictly confidential and unique to the user.
- Enforce a policy for regular password change.
- Enable password protection in the built-in BIOS configuration of the computer, especially if the computer is accessible to other users.
- Use strong passwords (at least eight characters including both uppercase and lowercase letters, numbers and at least one special character).
- Use passwords that users can easily remember.
- Never write down passwords.

3.6 Software maintenance and software versions

Keep all software up to date:

- Keep the Windows operating system software up to date according to Vitrolife's recommendations for each PC in the clinic's set-up.
- Ensure that Windows Update is enabled on all PCs running Windows.
- Comply with Vitrolife's recommendations to perform regular software updates as part of service and maintenance.
- Do not install any software on PCs unless cleared with Vitrolife.

3.7 User interfaces

Take the following precautions to protect sensitive information:

- Set up the user interface to lock automatically (e.g. screen saver activation).
- Log out of the software when you are not actively using it.
- Enable automatic Windows logoff/logout after a period of idle time.

3.8 Physical security and device set-up

The following guidelines apply to physical security and device set-up:

- Client computers are connected to the ES server via a LAN network. Connect all incubators using a local network with no internet connectivity.
- Avoid any access to network devices in public places where unauthorised (hostile) persons may find a way into the system via their network connection.
- Ensure that only authorised personnel have physical access to the laboratory area if possible. Any unauthorised personnel should be monitored.
- For all devices with Bluetooth connectivity, only enable this feature if needed for the device's functionality.
- Disable autoload/autorun of any kind on all devices when portable media are inserted or added.
- Do not leave any device in an insecure state when no supervision is available.

4 Contact information

Urgently need help? Call our service hotline for support:

+45 7023 0500

(available 24 hours a day, 7 days a week)

E-mail support: support.embryoscope@vitrolife.com

(response within 2 working days)

Vitrolife A/S
Jens Juuls Vej 20
DK-8260 Viby J
Denmark

Telephone: +45 7221 7900

Website: www.vitrolife.com

VITROLIFE A/S, DENMARK