

# Melanie software

## Privacy and Security Manual



# Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>3</b>
<b>2</b>	<b>Privacy and security environment .....</b>	<b>5</b>
<b>3</b>	<b>Authentication, authorization and audit logging .....</b>	<b>6</b>
3.1	Access controls .....	7
3.2	Audit logging and accountability controls .....	8
<b>4</b>	<b>Patient privacy consent management .....</b>	<b>9</b>
<b>5</b>	<b>Information protection .....</b>	<b>10</b>
5.1	Network security .....	11
5.2	Data storage and encryption .....	13
5.3	External connections .....	14
<b>6</b>	<b>System protection .....</b>	<b>15</b>
<b>7</b>	<b>Remote access .....</b>	<b>17</b>
<b>8</b>	<b>Personal information collected by the product .....</b>	<b>18</b>
<b>9</b>	<b>Disaster recovery considerations .....</b>	<b>19</b>
<b>10</b>	<b>Additional privacy and security considerations .....</b>	<b>22</b>
<b>11</b>	<b>Product security supplemental documents .....</b>	<b>23</b>

# 1 Introduction

## About this manual

This manual describes the privacy and security considerations of the use of Melanie software.

## Purpose of this manual

This manual describes the expected intended use of Melanie, the privacy and security capabilities included, and how these capabilities are configured.

## Scope of this manual

This manual is valid for Melanie software version 9.3 and above, from hereon referred to as Melanie, or the product.

## Introduction to privacy and security

This manual assumes that the reader understands the concepts of privacy and security. Security protects both system and information from risks to confidentiality, integrity, and availability. Security and privacy work together to help reduce risk to an acceptable level. In healthcare, the privacy, security, and safety must be balanced, relating to the intended use of the product.

The customer is encouraged to use risk management procedures to assess and prioritize privacy, security, and safety risks. Using the risk management, the customer can determine how to best leverage the capabilities provided within the product.

## Product description

Melanie is not a medical device and shall not be used in any clinical procedures or for diagnostic purposes.

Melanie is an image analysis software and does not contain any associated hardware.

## Safety notices

This user documentation contains safety notices concerning the safe use of the product. See the definition below.



### NOTICE

**NOTICE** indicates instructions that must be followed to avoid damage to the product or other equipment.



**IMPORTANT**  
**IMPORTANT** indicates instructions that are essential for the software or application to function.

**Contact information**

For specific privacy and security inquiries, use the contact form found at [cytiva.com/contact](https://cytiva.com/contact).

**Abbreviations**

The following terms and abbreviations are used in this manual:

Term/Abbreviation	Definition
PHI	Protected Health Information
PI	Privacy Information

## 2 Privacy and security environment

### **Privacy and security in the environment**

Melanie has been designed for an intended use with the following expectations of privacy and security protection, that are to be included in the environment where Melanie will be used:

- Melanie is used on a computer with Windows 10 (64-bit), or Windows 11 (64-bit).
- Melanie is designed for use in a standalone desktop environment.
- Melanie should not be used in a mobile system.

To perform analysis using different applications in Melanie, the user must have basic knowledge about image analysis.

# 3 Authentication, authorization and audit logging

## About this chapter

Melanie includes a broad assortment of capabilities to enable privacy and security. This chapter describes the ability and use of these privacy and security capabilities.

## In this chapter

Section		See page
3.1	Access controls	7
3.2	Audit logging and accountability controls	8

## 3.1 Access controls

### Introduction

The access control on Melanie is used to help control access to customer information on the system. Access control includes user account creation, assigning the privileges, and other features.

### Identity provisioning

The provisioning of user accounts requires the steps of account creation, maintenance, and removal of the account when it is no longer needed. A user account is created to be used by a specific individual. This user account is associated with access rights, and is recorded in system security log files.

Melanie does not support user management. This section is not applicable.

### User authentication

The user authentication step verifies that the user attempting to access the system is indeed the user associated with the specific account.

Melanie does not support authentication or data protection. It relies on customer security measures. The user must protect their data, if considered sensitive.

### Assigning access rights

Assigning access rights is the administrative process for connecting permissions with user accounts.

Melanie does not support access control. This section is not applicable.

## 3.2 Audit logging and accountability controls

### Introduction

Privacy and security information logging and control provide accountability through security surveillance, auditable records, and reporting.

Melanie supports audit log functionality. This feature tracks all user actions carried out during the life cycle of a project. Each action is logged in an audit file that is part of the project, and is time stamped and accompanied by the user ID. The parameters that are critical to reproduce the action are stored as well. The history of actions can be displayed in an audit report and exported in PDF format.



## 4 Patient privacy consent management

### **Patient privacy**

Melanie does not handle (create, transfer, or store) patient data, therefore the patient privacy consent is not applicable to Melanie.

# 5 Information protection

## About this chapter

This chapter describes privacy and security operations, and contains guidelines for the preparation of a secure environment for Melanie.

## Defense in depth

Security operations are best implemented as part of an overall "defense in depth" information assurance strategy. This strategy is used throughout an information technology system that addresses personnel, physical security, and technology. The layered approach of defense in depth limits the risk that the failure of a single security safeguard allows the system to be compromised.

Melanie does not claim any layered approach of defense in depth for its applications. Nevertheless, the failure in security for a single application does not compromise other applications in the software.

## In this chapter

Section		See page
5.1	Network security	11
5.2	Data storage and encryption	13
5.3	External connections	14

## 5.1 Network security

### Wired network security

Cytiva strongly recommends that Melanie is operated in a network environment that is separated from the general purpose computing network of the owner's organization. There are many effective techniques for isolating Melanie on a secure sub-network, including implementing firewall protection, demilitarized zones (DMZs), virtual local area networks (VLANs), and network enclaves.

To assist in secure network design, the following sections describe the required network services for Melanie.

Melanie does not support or claim any wired network security features. It is the responsibility of the customer to take care of the security if wired network is still used.

### Network setup

The following is valid for Melanie regarding the network setup:

- Melanie uses the network setup provided by the operating system environment, and does not provide any network features. The user does not need to configure any special operating system and network features.
- Melanie does not use any ports directly.
- Melanie does not support any remote service or features.

The user needs to make sure that Melanie is only exposed to a secure network environment. The License Server application uses TCP port 8090. This server is used by Melanie for its floating license. This port must not be closed when using a floating license to run Melanie.



#### **IMPORTANT**

The TCP port 8090 is used for a floating license. Make sure the port is open when running Melanie.

### Wireless network security

Radio signals are used in a wireless network communication, therefore wireless devices require special security consideration. Effective techniques and tools exist for improving the security of wireless communication. This section describes the characteristics for wireless connections for Melanie.

Melanie does not provide any wireless communication features. The features of Melanie can be accessed via wireless communication ports enabled by the operating system. Cytiva recommends to secure all wireless communication ports according to the guidelines of the operating system when using Melanie.

## Removable media security

The files used in Melanie for experiments and analysis can be imported and exported to USB storage media or to any other removable device. However, this feature is an operating system feature that is not unique for Melanie software. The user is responsible for making sure that removable devices connected to the system are free from viruses and other malware. The removable devices must be scanned with recommended antivirus software when transferring files from a computer.

## 5.2 Data storage and encryption

### Data encryption

Melanie does not support explicit data encryption measures in all its data storage.

The customer must secure all the data storage with appropriate measures.

### Data integrity capabilities

Melanie can warn users about edits to a project done manually or by third-party software. If any such modifications are detected, a pop-up window informs the user of the changes. This ensures that users are aware of any alterations made outside the controlled environment of Melanie.

### De-identification capabilities

Melanie is not a medical device and does not handle (create, transfer, or store) patient data. Therefore Melanie does not contain de-identification (anonymization and pseudonymization) capabilities.

### Data at rest security

Melanie does not provide any special security features for data at rest. It is expected that the files and results from Melanie are secured by the user of Melanie in a similar manner to how other system data are secured. Melanie does not store sensitive data, like PHI/PI. However, if there is any important information as part of the analysis which the user performs, Melanie expects the user to protect that information.

## 5.3 External connections

### **Security controls provided by the cloud provider**

Melanie is not hosted on a third-party cloud environment. Cloud security controls are not applicable.

# 6 System protection

## Introduction

This chapter describes the guidelines for how to configure and maintain the product in a way that continuously protects privacy and security.

## Protection from malicious attacks

The computing environment is increasingly hostile, and threats continue to grow from denial of service attacks and malicious software, including computer viruses, worms, Trojan horses, and other malware. Vigilant defense on many levels is required to keep the systems free from intrusion by malicious software. In most cases, effective protection requires cooperation between Cytiva and our customers.

Melanie has no integrated antivirus and malware protection. There is no support from third party antivirus or anti-malware software. It is the responsibility of the user to make sure that the following applies:

- Any removable devices that are connected to the system are free from viruses and other malware.
- In case the system is used in network mode, the network infrastructure is protected with a firewall and other security measures.

For more information on malicious software protection, refer to the following two white papers by the Joint NEMA/COCIR/JIRA Security and Privacy Committee:

- [Defending medical information systems against malicious software](#), December 2003
- [Patching off-the-shelf software used in medical information systems](#), October 2004

## Server and workstation security

Melanie contains additional features to improve local operational security.

Melanie has a license server application to enable the license communication between the server and clients for license management. The application is a third-party application and has its own security enabled.

## Software updates after system delivery

Cytiva recommends that the latest updates to the operating system are always applied.



**NOTICE**

An operating system update might interrupt the operation. To prevent unexpected equipment operation, the update process should be initiated manually and only performed when the equipment is not in use.



## 7 Remote access

### **Remote connection**

Remote connection to the product is not applicable.

## 8 Personal information collected by the product

### **Personal information**

Melanie is not a medical device and does not handle (create, transfer, or store) patient data. Melanie does not collect personal information.

For more information on customer privacy rights and how Cytiva processes personal data, see [Cytiva Privacy Policy](#).

# 9 Disaster recovery considerations

## Disaster recovery plan (DRP)

Cytiva recommends that customers create a disaster recovery plan for their organization, and test the functionality of the plan. This plan should include the elements outlined in the following sections.

## Asset management

The customer should undertake the following tasks:

1. Identify critical assets.

These may be facilities, systems, equipment which – if destroyed, degraded, or otherwise rendered unavailable – would influence the reliability or operability of your product.

Examples: PLC, HMI, bioreactor, etc.

If Melanie is considered to be a critical asset of the organization, the following items have been identified by Cytiva as critical components.

Responsibilities	Assets
Which critical assets are necessary for the operation of the product?	Any control PC
Which components is Cytiva responsible for?	None
Which components is the customer responsible for?	The customer is responsible for the entire installation
Which components is a third-party company responsible for?	None

2. Identify critical infrastructure.

This may be existing and proposed systems and assets, whether physical or virtual. The incapacity or destruction of these systems or assets would have a negative impact on security, economic security, public health or safety, or any combination of these matters.

Examples: cloud service provider, internet connection, third-party services, etc.

If Melanie is considered to be part of the critical infrastructure of the organization, the following items have been identified by Cytiva as critical components.

Responsibilities	Infrastructure
Which critical infrastructure is necessary for the operation of the product?	<ul style="list-style-type: none"> <li>Any control PC</li> <li>Network, if concurrent license needs to be configured</li> </ul>
Which components is Cytiva responsible for?	None
Which components is the customer responsible for?	<ul style="list-style-type: none"> <li>Local area network</li> <li>Internet connection</li> </ul>
Which components is a third-party company responsible for?	None

## Identifying recovery objectives

It is essential to establish the Recovery Time Objective and Recovery Point Objective. The customer is responsible for establishing both objectives for their products.

- The Recovery Time Objective is a pre-established deadline for a business to recover their systems after an outage. The customer should specify when the system needs to be recovered.

Examples: day, week, month, year.

- The Recovery Point Objective relates to a business' loss tolerance. This is measured by the amount of data that is deemed acceptable to be lost, before causing major damage to the customer business. The customer should specify to which time point in the past the system needs to be recovered.

Examples: day, week, month, year.

The following table identifies the responsibilities for recovery.

Responsibilities	Objectives
What parts of the product is Cytiva able to restore back to working order in case of failure?	Cytiva is not responsible for managing any part of the installation
How far back is Cytiva able to recover a failed component (restore to last working configuration)?	Not applicable
What data is Cytiva responsible for restoring (if any) in case of failure?	None
What data is the customer responsible for restoring (if any) in case of failure?	The customer needs to keep the activation IDs safe. These can be used to recover license information for PC renewal/re-hosting. In case of any failure.

## Perform regular testing

The customer should perform regular testing, auditing, and assessment of their DRP to make sure that the plan is effective. It is important to evaluate the DRP routinely and confirm that the processes and procedures are still applicable. The DRP should be updated and improved when applicable.

Cytiva recommends to evaluate the DRP annually.

## Additional information

For any disaster recovery support related to Melanie contact your Cytiva service representative.

For more information for industry best practices about disaster recovery visit the following websites:

- [\*CISA Disaster Recovery Consultation, Documentation, and Testing\*](#)
- [\*SANS Disaster Recovery Plan Strategies and Processes\*](#)

# 10 Additional privacy and security considerations

## **Additional risks**

Melanie has been designed with privacy and security functionality integrated into the core design. However, there exist privacy and security residual risks that must be mitigated when Melanie is integrated into the work environment. This section describes some risks that should be imported into the risk assessment of the deployment of Melanie for proper mitigation.

All modules in Melanie expect the user to maintain all security measures needed to prevent any kind of vulnerabilities.

# 11 Product security supplemental documents

## **Manufacturer Disclosure Statement for Medical Device Security (MDS2)**

The MDS2 is available for Melanie upon request. Contact the sales representative, or use the contact form found at [cytiva.com/contact](https://cytiva.com/contact).

## **Software Bill of Materials (SBOM)**

SBOM is available for Melanie upon request. Contact the sales representative for a copy of SBOM.

**Give feedback on this document**

Visit [cytiva.com/techdocfeedback](https://cytiva.com/techdocfeedback) or  
scan the QR code.



## cytiva.com

Cytiva and the Drop logo are trademarks of Life Sciences IP Holdings Corporation or an affiliate doing business as Cytiva.

Melanie is a trademark of SIB Swiss Institute of Bioinformatics. Windows is a trademark of the Microsoft group of companies.

Any other third-party trademarks are the property of their respective owners.

© 2023—2025 Cytiva

Any use of software may be subject to one or more end user license agreements, a copy of, or notice of which, are available on request.

For local office contact information, visit [cytiva.com/contact](https://cytiva.com/contact)

29738798 AB V:7 02/2025