

VDGH-WHITEPAPER

# IT-Product Security Whitepaper Template

Content

Preface . . . . . 3

How to use the Whitepaper . . . . . 3

Development and Authorship . . . . . 4

Disclaimer and Feedback . . . . . 4

## Preface

The IT-Security of medical devices, also known as ‘product security’, is an important aspect of their functionality. It is essential for their safe operation and to ensure:

- Confidentiality of patient data
- Integrity of the medical device, i.e. the device functions as intended.
- Availability of the medical device

To ensure product security, a medical device must be designed, implemented and tested properly. Moreover, it must be installed, configured, maintained and operated as intended. Failure to observe any of these aspects can easily compromise the product security of the medical device, with potentially severe consequences for its safety.

The intention of the IT-Product Security Whitepaper Template is to provide those responsible for the installation, maintenance and operation of medical devices with all the necessary information to carry out their work to the required standard:

- Provide information on all relevant product security aspects to customers and service personnel.
- Ensure the availability of all data and guidance required for the secure installation, configuration, maintenance and operation of the system.

In addition, the IT-Product Security Whitepaper Template is intended to provide all the information that may be required during the procurement and selection process for a medical device, thereby eliminating the need for customer-specific questionnaires.

## How to use the IT-Product Security Whitepaper Template

Users may fill in the white paper as a template with all relevant information about their product. First, general information about the system is to be provided, including hardware, software and operating system with details of the version, patch status and network configuration. The next section is to describe the basic principles and key security measures for the product. These include protection mechanisms against malware and vulnerabilities, network security, incident and vulnerability handling, and regulations for remote access. The topics of authentication and authorisation should also be examined in detail. This includes user account management, role-based access control, special mechanisms such as the ‘break the glass’ concept, and organisational data separation.

The completed document should also contain clear specifications on data protection for transmitted, stored and exported data. Also, data protection-compliant handling of information throughout the entire product life cycle should be outlined. Important aspects such as physical security, monitoring of security-related incidents through event and audit logging, disaster recovery, compliance with guidelines and certifications, and best practices for secure system configuration are part of the white paper and should be taken into account. The white paper can also be supplemented by a network or system diagram in

which the product is integrated and a standardised MDS<sup>2</sup> form with further security information. The whitepaper should also include a legal notice on liability issues.

Filled out this results in a comprehensive, practice-oriented presentation of most important security-critical areas of an IT-Product and can be used across the healthcare industry.

## Development and Authorship

The IT-Product Security Whitepaper Template was developed by the IT Security Working group of the VDPGH (Verband der Diagnostica-Industrie e.V.) to provide standardised guidance on product security documentation within the diagnostics industry. Consisting of industry experts and security professionals, the working group is dedicated to establishing best practices and supporting member companies in implementing comprehensive security measures for their products.

## Disclaimer and Feedback

This white paper is provided for reference purposes only and serves as a general template. The creator/manufacturer of the IT product is solely responsible for implementing, maintaining and ensuring the accuracy of all security measures described herein. It is worth noting that the white paper is not exhaustive, and that not all sections of the template need to be completed if they are not applicable to the product.

The VDPGH welcomes suggestions and feedback on how to improve the template – please contact us with your recommendations or questions to help us enhance this resource for the diagnostics community.

## Imprint

### Publisher

VDGH · Verband der Diagnostica-Industrie e. V.  
(Association of the Diagnostics Industry)  
Dr. Martin Walger, responsible

Neustädtische Kirchstraße 8  
10117 Berlin

Phone +49 30 2005 99 -40

vdgh@vdgh.de  
www.vdgh.de

### Referat Digitales

Benedikt Beyer  
Telefon +49 30 2005 99 -52  
beyer@vdgh.de

### Design

FGS Kommunikation, Berlin

Berlin, November 2025



[www.vdgh.de/en/productsecurity/](http://www.vdgh.de/en/productsecurity/)