Cybersecurity Information

1 Purpose

To communicate to users the relevant device security information that may enable their own ongoing security posture, thereby helping ensure a device remains safe and effective throughout its lifecycle.

2 Device Cybersecurity Information

This section describes the cybersecurity controls implemented in the PV-003 ProVee Video Processing Unit (VPU) and how to maintain system integrity and function.

2.1 Cybersecurity System Overview

Refer to the figure below for an overview of the cybersecurity controls implemented in the ProVee VPU.

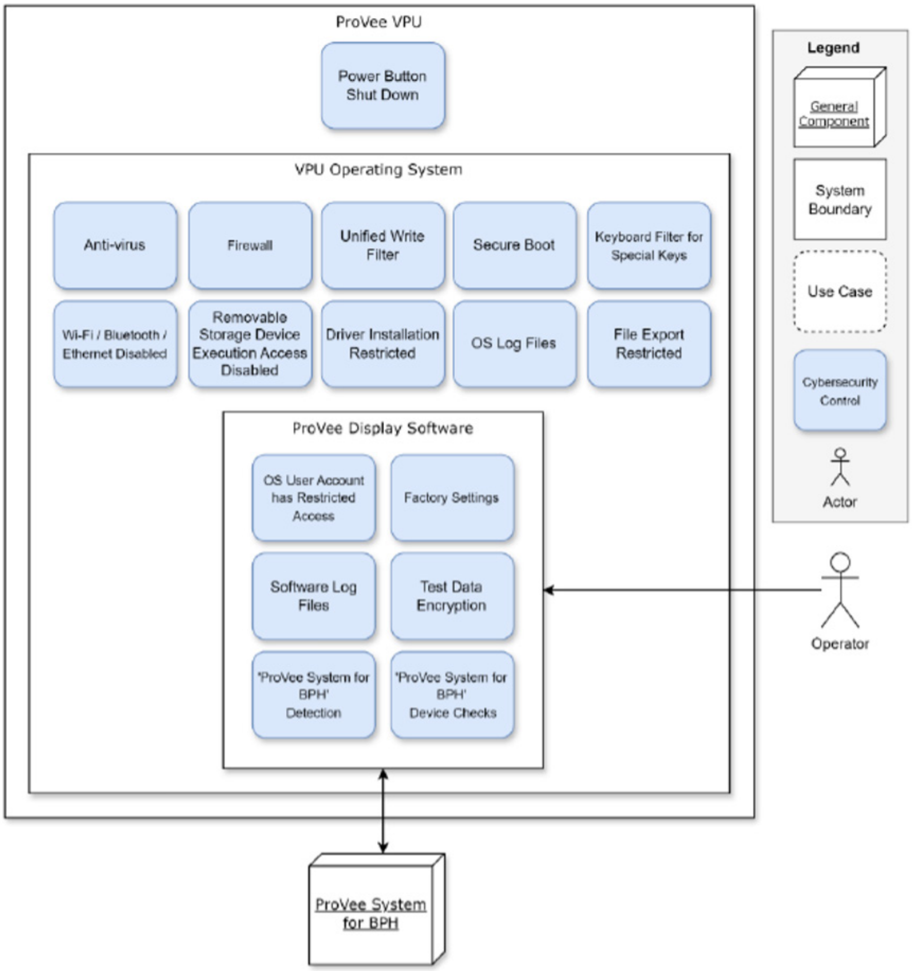

Figure 1. *Overview of Operator Cybersecurity Controls*

Cybersecurity Information *(continued)*

2.1.1 Controls

The ProVee VPU has the following cybersecurity controls implemented to provide protection of critical functionality:

- ProVee VPU:
  - Power Button on the enclosure provides a means to shut down the ProVee VPU in event of the system is locked up or compromised.
- ProVee VPU Operating System (OS):
  - Windows Anti-Virus is enabled to prevent malicious files.
  - Windows Firewall is enabled to block incoming and outgoing ports.
  - Windows Unified Write Filter (UWF) is enabled to ensure the ProVee VPU is reset back to its factory state when the system is turned on. This includes default configuration of network interfaces and other external interfaces.
  - Windows Secure Boot is enabled to ensure only trusted software is allowed to execute during the boot process.
  - Windows Keyboard filter is enabled to prevent use of special keyboard keys.
  - Wi-Fi, Ethernet, and Bluetooth interfaces are disabled to prevent network connectivity.
  - Execution access for removable storage devices is disabled, to prevent execution of files from an external device that could be inserted via the USB ports.
  - Installation of additional Windows drivers are prohibited.
  - Windows events are logged and retained to provide forensic evidence.
  - Operators cannot export any of files from the OS.
- ProVee VPU Display Software:
  - ProVee VPU Display Software application has restricted access to the ProVee VPU OS.
  - Factory settings ensure a configuration based on a safe selection of defaults settings are maintained throughout restarts.
  - ProVee VPU Display Software events are logged and retained to provide forensic evidence.
  - ProVee System for BPH device information is checked when connected to the ProVee VPU.
  - Automatic detection of ProVee System for BPH to recover when device is unplugged or interrupted.

2.1.2 Maintenance

The operator is not required to perform maintenance of the cybersecurity controls to preserve the device’s security. The ProVee VPU cybersecurity controls are maintained by ProVerum.

Cybersecurity Information *(continued)*

2.1.3 External Interfaces

The following external interfaces are required for system operation:

- USB 3.0 Type A and Type C Ports: Used for export of log/application files
- Medical grade connector: ProVee System for BPH and the ProVee VPU interface

The following external interfaces are disabled to eliminate potential attacker vectors:

- Network Interfaces: Ethernet, Wireless and Bluetooth interfaces via ProVee VPU OS
- Programmable button via ProVee VPU BIOS
- Speaker via ProVee VPU OS

The Docking Interface is enabled, which has the ability provide power to the ProVee VPU, as well as the ability to add various peripherals. A ProVee VPU OS security policy applied to all external interfaces is implemented, which only allows the ProVee System for BPH to be interfaced with. All other devices, including USB removable storage devices, require ProVee VPU OS administrative access.

2.2 Infrastructure Requirements

The ProVee VPU has been configured to have no external network connectivity.

In the event of a potential cybersecurity vulnerability or incident on the ProVee VPU, it is recommended to either:

- Restart the ProVee VPU since the Windows UWF will maintain the ProVee VPU's configuration.
- Shut down the ProVee VPU and send the ProVee VPU back to ProVerum.

2.3. Software Updates

ProVerum may provide software update periodically to address cybersecurity vulnerabilities.

Software updates are not available to Operators. They are only performed by authorised ProVerum staff once the ProVee VPU is returned.

2.4. Detection of Anomalies

The ProVee VPU windows configuration changes and peripherals are tracked in Windows events and ProVee VPU Display Software logs.

2.5. Secure Configuration and Recovery

Secure configurations for the ProVee VPU OS and ProVee VPU Display Software are applied by ProVerum when updated and cannot be changed by the Operator. These configurations are backed up by the Windows Write Filter and retained between system restarts.

If the configuration is suspected to be tampered with, the ProVee VPU should be restarted. Once restarted the ProVee VPU OS and ProVee Display Software will be recovered by restoring the backed-up configurations.

Cybersecurity Information *(continued)*

2.5. Secure Configuration and Recovery *(continued)*

The secure configuration include:

- Windows Anti-Virus (MS Defender)
    - Folder Exclusions (included sub-directories and files):
        - D:\
        - C:\Program Files\ProVerum\ProVee Display Software\
- Windows Firewall (MS Defender):
    - Inbound Rules:
        - Block all traffic, on all ports, for all profiles
    - Outbound Rules:
        - Block all traffic, on all ports, for all profiles
- Windows Unified Write Filter
    - Overlay
        - Type = Disk
        - Overlay Size = 15360 MB (15GB)
        - Warning Threshold = 10240 MB (10GB)
        - Critical Threshold = 14336 MB (15GB – 1MB)
        - Read Only Media = OFF
        - Freespace Passthrough = ON
        - Persistent = OFF
        - Reset Mode = N/A
        - Reset Saved Mode = N/A
    - File Exclusions:
        - C:\Windows\System32\winevt\Logs (Windows Event logs)
        - C:\Windows\assembly (.Net optimisation support)
        - C:\Program Files\Windows Defender
        - C:\ProgramData\Microsoft\Windows Defender
        - C:\Windows\Windowsupdate.log
        - C:\Windows\Temp\MpCMDRUN.log
        - C:\Windows\System32\config\SAM
    - Registry Exclusions
        - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Time Zones
        - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation
        - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender
        - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WdBoot
        - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WdFilter
        - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WdNisSvc
        - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WdNisDrv
        - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinDefend

Cybersecurity Information *(continued)*

2.6 Forensic Evidence Capture & Log File Management

ProVee VPU OS and ProVee VPU Display Software events are logged and retained to provide forensic evidence. These log files can only be accessed an authorised ProVerum staff.

2.7. Technical Support

For technical assistance or when a system requires a software update, contact ProVerum.

2.8. Software Bill of Materials (SBOM)

The SBOM is available for download via the *Streamlet Cybersecurity SBOM - ProVee Display Software* link.

2.9. Software End of Support

The table below describes the known and anticipated end of support information for critical software components. Critical software components are based on software components whose utilisation within a given sub-system can lead to a foreseeable or known threat.

Software Sub-system	Component Name	Maintenance Status	End of Support
ProVee Display Software	Microsoft.Extensions.DependencyInjection	Actively maintained	10 Nov 2026
ProVee Display Software	Microsoft.Extensions.DependencyInjection.	1.5 T and 3.0 T	1.5 T and 3.0 T
Abstractions	Actively maintained	10 Nov 2026	1.5 T and 3.0 T
ProVee Display Software	OpenCvSharp4	Actively maintained	Not found
ProVee Display Software	OpenCvSharp4.Extensions	Actively maintained	Not found
ProVee Display Software	OpenCvSharp4.runtime.win	Actively maintained	Not found
ProVee Display Software	OpenCvSharp4.WpfExtensions	Actively maintained	Not found
ProVee Display Software	SharpZipLib	Actively maintained	Not found
VPU OS	Windows 10 IoT Enterprise LTSC 2021	Actively maintained	13 Jan 2032
VPU OS	Windows Defender Antivirus	Actively maintained	13 Jan 2032
Image Signal Processor Sub-System	Image Signal Processor Firmware	The firmware is embedded in its supplied component and is managed by supplier controls.	

Table 1. *Software End of Support*

2.10 Decommissioning

At the end of its life cycle, the ProVee VPU must be disposed of in accordance with local regulations for electrical and electronic waste. ProVerum has determined that the ProVee VPU does not contain any sensitive, confidential, or proprietary data or software; therefore, no data sanitization of the units is required.