

| Manufacturer Disclosure Statement for Medical Device Security – MDS ² | | | |
|--|--|----------------------------------|---------------------------|
| DEVICE DESCRIPTION | | | |
| Device Category | Manufacturer | Document ID | Document Release Date |
| Respirator | Draeger | MDS2-2016-01 | "2016-05-19" |
| Device Model | Software Revision | | Software Release Date |
| IACS WS Critical Care (V500) | "2.42" | | "2015-06-16" |
| Manufacturer or Representative Contact Information | Company Name | Manufacturer Contact Information | |
| | Draeger | product-security@draeger.com | |
| | Representative Name/Position | | |
| | Hannes Molsen | | |
| Intended use of device in network-connected environment: Not to be connected to the Hospital IT Network, serial connection to device integrators, usb interface for logbook, screenshots and configuration exchange | | | |
| MANAGEMENT OF PRIVATE DATA | | | |
| Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form. | | | Yes, No, N/A, or See Note |
| | | | # |
| A | Can this device display, transmit, or maintain private data (including electronic Protected Health Information [ePHI])? | See Note | 1 |
| B | Types of private data elements that can be maintained by the device : | | |
| B.1 | Demographic (e.g., name, address, location, unique identification number)? | No | — |
| B.2 | Medical record (e.g., medical record #, account #, test or treatment date, device identification number)? | No | — |
| B.3 | Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)? | No | — |
| B.4 | Open, unstructured text entered by device user/operator ? | No | — |
| B.5 | Biometric data ? | No | — |
| B.6 | Personal financial information? | No | — |
| C | Maintaining private data - Can the device : | | |
| C.1 | Maintain private data temporarily in volatile memory (i.e., until cleared by power-off or reset)? | N/A | — |
| C.2 | Store private data persistently on local media? | N/A | — |
| C.3 | Import/export private data with other systems? | N/A | — |
| C.4 | Maintain private data during power service interruptions? | N/A | — |
| D | Mechanisms used for the transmitting, importing/exporting of private data – Can the device : | | |
| D.1 | Display private data (e.g., video display, etc.)? | N/A | — |
| D.2 | Generate hardcopy reports or images containing private data ? | N/A | — |
| D.3 | Retrieve private data from or record private data to removable media (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick, etc.)? | N/A | — |
| D.4 | Transmit/receive or import/export private data via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)? | N/A | — |
| D.5 | Transmit/receive private data via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)? | N/A | — |
| D.6 | Transmit/receive private data via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)? | N/A | — |
| D.7 | Import private data via scanning? | N/A | — |
| D.8 | Other? | N/A | — |
| Management of Private Data notes: 1: The device maintains only diagnostic and therapeutic data not linked to an identified individual. Demographic data contains patient category (neonate / pediatric / adult), body weight, and height. | | | |

| | | | |
|---|------------------------------------|--|--|
| Device Category Respirator | Manufacturer Draeger | Document ID MDS2-2016-01 | Document Release Date "2016-05-19" |
| Device Model IACS WS Critical Care (V500) | Software Revision "2.42" | Software Release Date "2015-06-16" | |

| SECURITY CAPABILITIES | | | | |
|--|---|--|---------------------------------|-----------|
| Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form. | | | Yes, No, N/A, or See Note | # Note |
| 1 AUTOMATIC LOGOFF (ALOF) | | | | |
| The device's ability to prevent access and misuse by unauthorized users if device is left idle for a period of time. | | | | |
| 1-1 | Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)? | | Yes | 3 |
| 1-1.1 | Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable? (Indicate time [fixed or configurable range] in notes.) | | No | — |
| 1-1.2 | Can auto-logoff/screen lock be manually invoked (e.g., via a shortcut key or proximity sensor, etc.) by the user ? | | No | — |
| ALOF notes: 3: System Configuration and Service Dialog are timeout protected | | | | |
| 2 AUDIT CONTROLS (AUDT) | | | | |
| The ability to reliably audit activity on the device . | | | | |
| 2-1 | Can the medical device create an audit trail ? | | Yes | 4 |
| 2-2 | Indicate which of the following events are recorded in the audit log: | | | |
| 2-2.1 | Login/logout | | No | — |
| 2-2.2 | Display/presentation of data | | No | — |
| 2-2.3 | Creation/modification/deletion of data | | Yes | 5 |
| 2-2.4 | Import/export of data from removable media | | Yes | 6 |
| 2-2.5 | Receipt/transmission of data from/to external (e.g., network) connection | | Yes | 7 |
| 2-2.5.1 | Remote service activity | | N/A | — |
| 2-2.6 | Other events? (describe in the notes section) | | N/A | — |
| 2-3 | Indicate what information is used to identify individual events recorded in the audit log: | | | |
| 2-3.1 | User ID | | No | — |
| 2-3.2 | Date/time | | Yes | 8 |
| AUDT notes: 4: User Log (see device Instructions for Use) 5: logged events comprise, e.g., calibration events, ventilation parameter changes, patient admission, ... 6: Import and export of configuration data for identical setup of multiple devices via USB 7: Logging of switching to device state: Product Test in which service technician over RJ45 cross cable is able to access service features. Service session establishment is logged. 8: Date/Time is set config menu | | | | |
| 3 AUTHORIZATION (AUTH) | | | | |
| The ability of the device to determine the authorization of users. | | | | |
| 3-1 | Can the device prevent access to unauthorized users through user login requirements or other mechanism? | | No | 9 |
| 3-2 | Can users be assigned different privilege levels within an application based on 'roles' (e.g., guests, regular users , power users , administrators, etc.)? | | No | 9 |
| 3-3 | Can the device owner/operator obtain unrestricted administrative privileges (e.g., access operating system or application via local root or admin account)? | | No | 9 |
| AUTH notes: 9: System Configuration and Service Dialog password protected, see Instructions for Use | | | | |

| | | | |
|---|------------------------------------|--|--|
| Device Category Respirator | Manufacturer Draeger | Document ID MDS2-2016-01 | Document Release Date "2016-05-19" |
| Device Model IACS WS Critical Care (V500) | Software Revision "2.42" | Software Release Date "2015-06-16" | |

| Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form. | | | Yes, No, N/A, or See Note | # Note |
|---|---|--|---------------------------------|-----------|
| 4 CONFIGURATION OF SECURITY FEATURES (CNFS) | | | | |
| The ability to configure/re-configure device security capabilities to meet users' needs. | | | | |
| 4-1 | Can the device owner/operator reconfigure product security capabilities ? | | No | — |
| CNFS notes: | | | | |
| 5 CYBER SECURITY PRODUCT UPGRADES (CSUP) | | | | |
| The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade device's security patches. | | | | |
| 5-1 | Can relevant OS and device security patches be applied to the device as they become available? | | No | 10 |
| | 5-1.1 Can security patches or other software be installed remotely? | | N/A | — |
| CSUP notes: | | | | |
| 6 HEALTH DATA DE-IDENTIFICATION (DIDT) | | | | |
| The ability of the device to directly remove information that allows identification of a person. | | | | |
| 6-1 | Does the device provide an integral capability to de-identify private data ? | | N/A | 11 |
| DIDT notes: | | | | |
| 7 DATA BACKUP AND DISASTER RECOVERY (DTBK) | | | | |
| The ability to recover after damage or destruction of device data, hardware, or software. | | | | |
| 7-1 | Does the device have an integral data backup capability (i.e., backup to remote storage or removable media such as tape, disk)? | | N/A | |
| DTBK notes: | | | | |
| 8 EMERGENCY ACCESS (EMRG) | | | | |
| The ability of device users to access private data in case of an emergency situation that requires immediate access to stored private data . | | | | |
| 8-1 | Does the device incorporate an emergency access ("break-glass") feature? | | N/A | 12 |
| EMRG notes: | | | | |
| 9 HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU) | | | | |
| How the device ensures that data processed by the device has not been altered or destroyed in an unauthorized manner and is from the originator. | | | | |
| 9-1 | Does the device ensure the integrity of stored data with implicit or explicit error detection/correction technology? | | Yes | — |
| IGAU notes: | | | | |

| | | | |
|---|------------------------------------|--|--|
| Device Category Respirator | Manufacturer Draeger | Document ID MDS2-2016-01 | Document Release Date "2016-05-19" |
| Device Model IACS WS Critical Care (V500) | Software Revision "2.42" | Software Release Date "2015-06-16" | |

| Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form. | | Yes, No, N/A, or See Note | Note # |
|--|---|---------------------------------|--------|
| 10 MALWARE DETECTION/PROTECTION (MLDP) | | | |
| The ability of the device to effectively prevent, detect and remove malicious software (malware). | | | |
| 10-1 | Does the device support the use of anti-malware software (or other anti-malware mechanism)? | No | 13 |
| 10-1.1 | Can the user independently re-configure anti-malware settings? | No | — |
| 10-1.2 | Does notification of malware detection occur in the device user interface? | No | — |
| 10-1.3 | Can only manufacturer-authorized persons repair systems when malware has been detected? | No | — |
| 10-2 | Can the device owner install or update anti-virus software ? | No | — |
| 10-3 | Can the device owner/ operator (technically/physically) update virus definitions on manufacturer-installed anti-virus software ? | No | — |
| MLDP notes: | 13: Malware and antivirus strategy is based on the Windows XP-Embedded HORM (Hibernate Once, Resume Many) feature, malware removal is done by a reboot. Access to operating system is locked down, cf. separately available Device Security Whitepaper. | | |
| 11 NODE AUTHENTICATION (NAUT) | | | |
| The ability of the device to authenticate communication partners/nodes. | | | |
| 11-1 | Does the device provide/support any means of node authentication that assures both the sender and the recipient of data are known to each other and are authorized to receive transferred information? | Yes | 14 |
| NAUT notes: | 14: For MEDIBUS / MEDIBUS.X, cf. MEDIBUS Instructions for Use; for Service Access via RJ45 cross cable cf. separately available Device Security Whitepaper. | | |
| 12 PERSON AUTHENTICATION (PAUT) | | | |
| Ability of the device to authenticate users | | | |
| 12-1 | Does the device support user/operator -specific username(s) and password(s) for at least one user ? | No | — |
| 12-1.1 | Does the device support unique user/operator -specific IDs and passwords for multiple users? | No | — |
| 12-2 | Can the device be configured to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, etc.)? | No | — |
| 12-3 | Can the device be configured to lock out a user after a certain number of unsuccessful logon attempts? | N/A | — |
| 12-4 | Can default passwords be changed at/prior to installation? | N/A | — |
| 12-5 | Are any shared user IDs used in this system? | N/A | — |
| 12-6 | Can the device be configured to enforce creation of user account passwords that meet established complexity rules? | N/A | — |
| 12-7 | Can the device be configured so that account passwords expire periodically? | N/A | — |
| PAUT notes: | | | |
| 13 PHYSICAL LOCKS (PLOK) | | | |
| Physical locks can prevent unauthorized users with physical access to the device from compromising the integrity and confidentiality of private data stored on the device or on removable media . | | | |
| 13-1 | Are all device components maintaining private data (other than removable media) physically secure (i.e., cannot remove without tools)? | N/A | — |
| PLOK notes: | | | |

| | | | |
|---|------------------------------------|--|--|
| Device Category Respirator | Manufacturer Draeger | Document ID MDS2-2016-01 | Document Release Date "2016-05-19" |
| Device Model IACS WS Critical Care (V500) | Software Revision "2.42" | Software Release Date "2015-06-16" | |

| Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form. | | | Yes, No, N/A, or See Note | # Note |
|---|--|--|---------------------------------|-----------|
| 14 ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP) | | | | |
| Manufacturer's plans for security support of 3rd party components within device life cycle. | | | | |
| 14-1 | In the notes section, list the provided or required (separately purchased and/or delivered) operating system(s) - including version number(s). | | See Note | 14 |
| 14-2 | Is a list of other third party applications provided by the manufacturer available? Windows XP Embedded SP3, VxWorks 6.9.2.3 | | No | |
| RDMP notes: | | | | |
| 15 SYSTEM AND APPLICATION HARDENING (SAHD) | | | | |
| The device's resistance to cyber attacks and malware . | | | | |
| 15-1 | Does the device employ any hardening measures? Please indicate in the notes the level of conformance to any industry-recognized hardening standards. | | Yes | 15 |
| 15-2 | Does the device employ any mechanism (e.g., release-specific hash key, checksums, etc.) to ensure the installed program/update is the manufacturer-authorized program or software update? | | Yes | 16 |
| 15-3 | Does the device have external communication capability (e.g., network, modem, etc.)? | | Yes | 15 |
| 15-4 | Does the file system allow the implementation of file-level access controls (e.g., New Technology File System (NTFS) for MS Windows platforms)? | | See Note | 15 |
| 15-5 | Are all accounts which are not required for the intended use of the device disabled or deleted, for both users and applications? | | Yes | 15 |
| 15-6 | Are all shared resources (e.g., file shares) which are not required for the intended use of the device , disabled? | | N/A | — |
| 15-7 | Are all communication ports which are not required for the intended use of the device closed/disabled? | | Yes | — |
| 15-8 | Are all services (e.g., telnet, file transfer protocol [FTP], internet information server [IIS], etc.), which are not required for the intended use of the device deleted/disabled? | | Yes | 15 |
| 15-9 | Are all applications (COTS applications as well as OS-included applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device deleted/disabled? | | Yes | — |
| 15-10 | Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)? | | No | — |
| 15-11 | Can software or hardware not authorized by the device manufacturer be installed on the device without the use of tools? 15: cf. separately available Device Security Whitepaper. 16: expected hash of SW update package sent over secured secondary channel (SNMPv3) to the device. | | No | — |
| SAHD notes: | | | | |
| 16 SECURITY GUIDANCE (SGUD) | | | | |
| The availability of security guidance for operator and administrator of the system and manufacturer sales and service. | | | | |
| 16-1 | Are security-related features documented for the device user ? | | No | — |
| 16-2 | Are instructions available for device/media sanitization (i.e., instructions for how to achieve the permanent deletion of personal or other sensitive data)? 17: see chapter "Management of Private Data" | | N/A | 17 |
| SGUD notes: | | | | |

| | | | |
|---|------------------------------------|------------------------------------|--|
| Device Category Respirator | Manufacturer Draeger | Document ID MDS2-2016-01 | Document Release Date "2016-05-19" |
| Device Model IACS WS Critical Care (V500) | Software Revision "2.42" | | Software Release Date "2015-06-16" |

| Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form. | | | Yes, No, N/A, or See Note | # Note |
|---|--|--|---------------------------------|-----------|
| 17 HEALTH DATA STORAGE CONFIDENTIALITY (STCF) | | | | |
| The ability of the device to ensure unauthorized access does not compromise the integrity and confidentiality of private data stored on device or removable media . | | | | |
| 17-1 | Can the device encrypt data at rest? | | N/A | 18 |
| STCF notes: 18: see chapter "Management of Private Data" | | | | |
| 18 TRANSMISSION CONFIDENTIALITY (TXCF) | | | | |
| The ability of the device to ensure the confidentiality of transmitted private data . | | | | |
| 18-1 | Can private data be transmitted only via a point-to-point dedicated cable? | | N/A | 19 |
| 18-2 | Is private data encrypted prior to transmission via a network or removable media ? (If yes, indicate in the notes which encryption standard is implemented.) | | N/A | 19 |
| 18-3 | Is private data transmission restricted to a fixed list of network destinations? | | N/A | 19 |
| TXCF notes: 19: see chapter "Management of Private Data" | | | | |
| 19 TRANSMISSION INTEGRITY (TXIG) | | | | |
| The ability of the device to ensure the integrity of transmitted private data . | | | | |
| 19-1 | Does the device support any mechanism intended to ensure data is not modified during transmission? (If yes, describe in the notes section how this is achieved.) | | N/A | 20 |
| TXIG notes: 20: see chapter "Management of Private Data" | | | | |
| 20 OTHER SECURITY CONSIDERATIONS (OTHR) | | | | |
| Additional security considerations/notes regarding medical device security. | | | | |
| 20-1 | Can the device be serviced remotely? | | No | — |
| 20-2 | Can the device restrict remote access to/from specified devices or users or network locations (e.g., specific IP addresses)? | | No | — |
| 20-2.1 | Can the device be configured to require the local user to accept or initiate remote access? | | N/A | — |
| OTHR notes: | | | | |