

Title:	Medical Device and Operating Technology Security Compliance Requirements
Applies To:	IHiS and Public Healthcare Institutions

Medical Device and Operating Technology Security Compliance Requirements

This document is the property of Integrated Health Information Systems Pte Ltd (IHiS) and is intended for internal use only and may be amended from time to time without prior notification. It contains proprietary information that is confidential to IHiS and it should not be reproduced, partially or wholly, in whatever form, without the express written permission of IHiS. Disclosure of this document in full or in part, may result in material damage to IHiS. Written permission must be obtained prior to the disclosure of this document to a third party. Any enquiry should be directed to IHiS, Security Services.





Contents

1	IMPORTANT NOTES	3
2	SECURITY COMPLIANCE REQUIREMENTS	4
3	ASSET INVENTORY	10

1 Important Notes

1. This document contains a set of security compliance requirements for Medical Device and Operating Technology (MD&OT). The Participating Vendor shall assess project requirements and respond “Y” or “N” where necessary. Where “N” is indicated, reason must be provided in the remarks column.
2. No security compliance requirements shall be removed from this document, unless otherwise approved by the IHIS Cyber Defence Group, Strategy and Policy Team.
3. In the installation of “New MD&OT system/installation”, the Company’s project manager shall engage the Company’s security services consultant to review the IT security requirements. For all other projects and CRs, the project manager shall consult the security services if there is any Non-Compliance (NC) or Partial Compliance (PC) or Non-Applicability (NA) for any MD&OT security requirement.
4. A security management consultant may add additional security requirements for each MD&OT system or project where necessary.
5. The Participating Vendor shall adhere with the latest IT security standards and guidelines as prescribed from time to time by the Company unless declared otherwise.
6. The Participating Vendor shall ensure that the provision of necessary security features to guard against the confidentiality, integrity and availability of the system, its data, resources and relevant interfaces to other systems and devices. Security assessment and implementation of controls shall be submitted when managing a MD&OT.
7. The Participating Vendor shall complete and obtain sign-off of the Operation Acceptance Test Form for the configured MD&OT prior to go-live.
8. The Participating Vendor shall adopt the Company’s IT Security Incident Response Plan if the MD&OT has been tampered with or infected.
9. The Participating Vendor shall adopt the Company’s Incident Management Process in the event of a service failure.
10. No hardcode of Active Directory Domain Controller is allowed in an application coding or set-up.
11. The Participating Vendor will have to adhere to the Company’s approved software list, where applicable.
12. This document should be used in conjunction with the Security Requirements for ICT equipment document where appropriate.
13. The Participating Vendor will have to fill section 2 - Security Compliance Requirements and submit the attached Asset Inventory Spreadsheet in section 3.
14. The Participating Vendor will have to provide the completed Manufacturer Disclosure Statement for Medical Device Security (MDS2) of the MD&OT.
(<https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx>)

2 Security Compliance Requirements

S/N o.	Category	Requirements	Comply (Y/N)	Remarks (Please provide reasons why unable to Comply)
1	Asset Inventory	The Participating Vendor to provide the following asset related information upon commissioning or when there are changes after commissioning of the MD&OT. *Please refer to attached Asset Inventory Spreadsheet in section 3. (a) Name/Description of each MD&OT (Type, Brand, Model); (b) Serial number of each MD&OT; (c) Purpose of each MD&OT; (d) Physical location of each MD&OT; (e) IP address of each MD&OT; (f) MAC address of each MD&OT; (g) Connectivity the MD&OT can support (e.g., USB, Bluetooth, Wi-Fi etc.); (h) Operating System/ Application Version and Patch level; (i) Vendor name of each MD&OT; (j) User department that owns each of the MD&OT ; (k) Criticality of the MD&OT system, as according to the criticality defined by the Entities (e.g., critical, non-critical relative to patient risk); (l) Indication if the MD&OT includes Patient Data (Yes/ No); (m) Other ICT systems that each MD&OT is connected to; and (n) Indication if the data flow of the MD&OT allows One (1) way or Two (2) way.		

2	Internet Surfing Separation	MD&OT shall adhere to Internet Surfing Separation (ISS) policy of the Company. If the MD&OT requires connection to the internet or external network, it shall not connect to the internal ICT corporate network. Security implementation design must be provided where applicable.		
		Mobile network dongle shall not be used via MD&OT's USB port or any other forms of wireless connection (e.g. bluetooth/wireless network adapters).		
3	Controlled Use of USB ports & Removable Storage Media	Please provide details on any available controls or measures that the MD&OT can perform/implement to reduce risk of malware through USB/physical ports. e.g. antivirus/anti-malware software, application controls, kiosk mode, application sandbox, USB/Ports disabling/controls.		
		The Participating vendor/manufacturer must adhere to the Company's approval processes and controls when access to device is required.		
		All storage media must be scanned for malware by the Company prior to use with MD&OT. This includes all vendor devices. The Participating Vendor must comply with the Company's removable storage media scanning process/requirements for malware prior to use on the MD&OT.		
		The Participating Vendor must restrict the use of USB ports in MD&OT via OS/Software controls or via a physical lock device (e.g. Lindy port blockers, etc..) Please detail any other USB controls that can be performed by the device.		
		The key to the USB port physical lock device will not be released, except when operational expediency of critical functions is of concern. The Company, may at their discretion, release the key of the USB port lock device to the assigned department or personnel (e.g. Bio-Medical Engineering or Department Head or delegate etc.) with proper		

		authorisation and tracking documentation which includes the following information: (a) Requestor name; (b) Date and Time; (c) Serial Number and/or name of MD&OT to be accessed; and (d) Purpose and duration of activity The Participating Vendor must comply with this key management process in the Company.		
		The Participating Vendor must adhere to standard operating procedures in place to ensure that the above requirements on USB ports and removable storage media are consistently applied throughout the life span of the MD&OT. Vendor's staff and contractors are expected to comply with these procedures.		
		The Participating Vendor shall deploy anti-malware measures (e.g. antivirus/anti-malware software, and other controls such as process controls, physical access controls, USB port blocking) to ensure MD&OT are protected against malware without compromising the safety and reliability of the MD&OT.		
4	Malware Protection	The Participating Vendor shall define their MD&OT patch management process, which shall be approved by the Company. The MD&OT patch management process shall define the patch deployment timeframes and response times.		
		The Participating Vendor shall ensure that MD&OT access into the Company's ICT system or network (where required) must be approved by the Company before connecting. All network access controls must be detailed and provided. Please provide network topology of deployment of MD&OT. This includes the security diagram and relevant hardening guides to demonstrate compliance to the Company's requirements for network security.		

5	Network Connection	The Participating Vendor shall adhere to the Company's network segmentation requirements for all MD&OT that require connection to the Company's ICT system or network. The Participating Vendor must request for approval from the Company before connecting any device to the Company's ICT system or network.		
		The Participating Vendor shall ensure/adhere to Company's network segmentation requirements that are implemented for MD&OT with the following network access control mechanisms: (a) Only authorised/approved MD&OT are permitted to connected to the network; (b) Restrict all communication/ network traffic/ ports by default and allow only authorised communications between MD&OT and Entity's ICT system/network; (c) All unauthorised connectivity shall be disabled e.g. Wi-Fi, Bluetooth etc.		
		The Participating Vendor shall ensure that for MD&OT connected to the Company's corporate Wireless Local Area Network (LAN), Wi-Fi Protected Access 2 (WPA2) encryption standard is used and the Service Set Identifier (SSID) of the Wireless LAN is hidden.		
		Where required by the Company, the Participating Vendor shall work with the Company's appointed Security Operations Centre (SOC) vendor to have the MD&OT monitored and subscribed to the Healthcare SOC monitoring services. This includes the fine-tuning of the security monitoring services.		
6	Privileged Access Control	The Participating Vendor shall ensure that access to MD&OT is restricted to only authorised Vendor's staff and contractors. Vendor's use of administrator ID shall be controlled.		

	(a) MD&OT privileged accounts shall be restricted on a need-to-use and event-by-event basis, based on the minimum requirement for their functional roles; (b) MD&OT default accounts shall be removed if not required; (c) MD&OT privileged accounts shall have clear ownership; and (d) MD&OT privileged access and activities shall be logged.		
	The Participating Vendor shall ensure that all default passwords are changed immediately after the MD&OT are commissioned.		
	Passwords must be at least 15 characters long for privileged accounts.		
	Passwords must be at least 12 characters long for non-privileged accounts.		
	Passwords must contain characters from at least 2 of the following 4 categories: i. Upper case (A through Z); ii. Lower case (a through z); iii. Digits (0-9); iv. Special Characters (!, \$, #, %, etc.) The use of passphrases (concatenation of words or text or special characters) should be encouraged		
	Passwords must be changed once every 12 months		
	Passwords must not be re-used.		
	Passwords must not be displayed in clear.		
	Passwords must not be transmitted or stored in plaintext.		
	Passwords must be changed on first use.		

		Passwords must not be the same as the Account ID or User ID.		
		For MD&OT devices that cannot support password length of at least 12 characters, they shall: (a) Enforce passwords to be made up of at least 8 characters from at least 2 of the following 4 categories: i. Upper case (A through Z); ii. Lower case (a through z); iii. Digits (0-9); iv. Special Characters (!, \$, #, %, etc.) (b) Password changed every 12 months		
		The Participating Vendor shall ensure that access to the MD&OT for technical support or system changes must be approved, controlled and provisioned via the Company's approved methods and processes.		
		Remote administration access to MD&OT systems shall be disabled unless approved by the Company.		
		The following ICT security controls shall be implemented if remote administration is approved by the Company: (a) Remote administration shall only be granted to authorised personnel; and (b) Personnel who are authorised to perform remote administration shall use 2-Factor Authentication (2FA).		
		The Participating Vendor shall be responsible and liable for secure account administration and remote access.		
7	Data Sanitisation & Secure Disposal	The Participating Vendor shall provide details on the process for factory reset options.		
		The Participating Vendor shall provide details on the process for data sanitisation.		
		The Participating Vendor shall provide details on the secure disposal of equipment.		

3 **Asset Inventory**

Please fill in attached Asset Inventory spreadsheet of devices.



Asset Inventory.xlsx