**Furniture and Equipment Security Guidelines for CMH**

## 1. Purpose

This document elaborates policy requirements and sets implementation standards on the security requirements specified in the Baseline IT Security Policy, and provides implementation guidance for effective implementation of corresponding security measures.

Contractors shall follow the guidance in this document to implement security controls to satisfy the relevant security requirements. The security requirements in this document are designed to be technology neutral. Contractors may need to customise the security measures appropriate to their circumstances without prejudice to the security level. An alternative security solution that is able to achieve the same or better security protection, shall be proposed where any System/equipment security requirements are unable to be fulfilled due to product design limitations.

## 2. Scope

This document addresses security considerations in the following 17 security principles and adopts on all CMH's equipment and non-IT systems, including data security, application security, network security, server security, client/desktop security, security incident reporting and vendor maintenance and etc.

This document sets the minimum security requirements. Contractors need to apply enhanced security measures, appropriate to their circumstances and commensurate with the determined risks.

## 3. Target Audience

The document is targeted for the Contractors who require to implement security measures for the F&E systems. It is the responsibility for parties to follow in order to implement the security requirements effectively. In addition, the document is intended for use by vendors, Contractors and consultants who provide IT services to the CMH.

# 4. Security Principles

## 4.1 Safety

4.1.1 Contractors shall ensure the System/equipment remains secure and malicious code free in accordance with the terms and conditions of the relevant contract.

4.1.2 Contractors shall ensure the System/equipment does not create any non-compliance with regulatory or legal frameworks.

## 4.2 Confidentiality and Privacy

4.2.1 Contractors shall ensure the System/equipment does not capture, store or process sensitive data and/or any data related to any individual, including personal health information, in a manner that allows the data to be made available or disclosed in an unauthorised manner.

4.2.2 Contractors shall ensure the System/equipment provides appropriate authentication controls on privacy control when allowing any user, protocol or other form of connection.

## 4.3 Integrity

4.3.1 Contractors shall ensure the System/equipment preserves the accuracy and completeness (i.e. integrity) of data and the methods used to process and manage this data.

## 4.4 Availability

4.4.1 Contractors shall ensure the System/equipment preserves the accuracy and completeness (i.e. integrity) of data and the methods used to process and manage this data.

4.4.2 Contractors shall ensure the System/equipment will be accessible and usable when needed. Contractors shall ensure the System/equipment achieves an overall level of availability with reference to the requirement in the Technical Specifications.

4.4.3 Contractors shall ensure the System/equipment provides adequate System/equipment resilience facilities, including and not limited to redundant hardware components, enabling any faulty components to be switched over to redundant components if applicable.

4.4.4 Contractors shall ensure the System/equipment is supported by uninterruptable power supply (UPS) for maintaining the committed level of System/equipment availability if applicable.

**4.5 Compatibility**

4.5.1 Contractors shall ensure the System/equipment is able to effectively function together with other System/equipment.

4.5.2 Contractors shall ensure the System/equipment does not adversely interfere with the effective operation of any other System/equipment.

4.5.3 Contractors shall ensure the System/equipment continues to function correctly following any System hardening requirements according to Government security standards and guidelines.

**4.6 Longevity**

4.6.1 Contractors shall ensure updates for patching of vulnerabilities are maintained throughout the System/equipment's lifetime.

**4.7 Data Sovereignty**

4.7.1 Contractors shall ensure the data processed or stored by the System/equipment resides in Hong Kong.

4.7.2 Contractors shall ensure the System/equipment does not process or store data outside of Hong Kong.

4.7.3 Contractors shall ensure the System/equipment is governed by the laws of Hong Kong.

**4.8 System Hardening**

4.8.1 Contractors shall ensure the System/equipment, where using the Microsoft Windows operating system, hardens all its components and functionality in accordance with the Government security standards and guidelines.

4.8.2 Contractors shall ensure the System/equipment where using the non-Windows solutions are secured according to the Government security standards and guidelines.

4.8.3 Contractors shall ensure the System/equipment avoids the presence of hard-coded authentication credentials.

**4.9 Data Security**

4.9.1 Contractors shall ensure restricted data downloaded from the System / equipment to end-user devices is protected by a reasonable level of encryption.

Note: Restricted data refers to data including but not limited to identifiable patient information.

4.9.2 Contractors shall ensure restricted data stored within the System/equipment is encrypted.

4.9.3 Contractors shall ensure restricted data stored in backup storage is encrypted.

4.9.4 Contractors shall ensure all important data (knowledge, System/equipment configuration parameters) stored in the System/equipment is safeguarded and preserved through an effective backup mechanism.

4.9.5 Contractors shall ensure restricted data shall NOT be exported for any usage unless prior authorisation has been obtained from the Government.

4.9.6 Contractors shall ensure where there is a requirement to copy or move data from the System/equipment using portable media (i.e. USB Drive or CD), then this media is scanned for malicious code on a CMH PC before the data is being copied.

**4.10 Application Security**

4.10.1 Contractors shall ensure the System/equipment employs prevalent authentication mechanisms at reasonable safety level.

4.10.2 Contractors shall ensure the System/equipment supports role-based access control.

4.10.3 Contractors shall ensure the System/equipment applies network level encryption.

4.10.4 Contractors shall ensure the System/equipment provides comprehensive version control and configuration management mechanisms.

**4.11 Malicious Code Protection**

4.11.1 Contractors shall ensure the System/equipment is protected with the installation of a reputable Anti-Virus program in all servers, PC and Workstation components.

4.11.2 Contractors shall ensure the System/equipment is protected with regular updates of the latest virus definitions.

4.11.3 Contractors shall be responsible for the on-going support and for keeping the virus definitions and related software up-to-date in all servers, PCs and workstations.

4.11.4 Contractors shall ensure virus definitions are updated within 24 hours from the date of release.

4.11.5 Contractors shall be responsible for the regular scanning of all servers and PCs in the System/equipment every three months to ensure that they are not infected by virus, worms and spyware including the on-going support of scheduling and verifying the results of the virus scan.

**4.12 Vulnerability / Patch Management**

4.12.1 Contractors shall maintain ongoing System/equipment support, including the

installation of the latest security patches for the operating systems and related software in all System servers, PCs and workstations.

4.12.2 Contractors shall ensure security patches are updated within three months from the date of release.

**4.13 Network Connectivity and Restricted Network Access**

4.13.1 Contractors shall ensure any network connection for a System/equipment to the CMH network is endorsed by CMH and implemented and operated according to CMH policies, procedures and guidelines.

4.13.2 Contractors shall ensure that there are no External network connections to the System/equipment unless supported by prior authorisation and knowledge of CMH.

4.13.3 Contractors shall ensure that the System/equipment does not automatically establish any wired or wireless connections without prior authorisation and knowledge of CMH.

**4.14 Maintenance Support**

4.14.1 Contractors shall ensure that when maintenance is performed on the System/equipment or when accessing the System/equipment in any remote manner that the tools and software have been confirmed to be free of malicious code.

4.14.2 Contractors shall ensure that where maintenance on the System/equipment needs to be performed, that CMH is provided with a level of assurance that the vendor has undertaken proactive actions to ensure their connecting media or device (USB stick, portable media, laptops, iPads, etc.) has been scanned for malicious code before and after every time that portable media is used to apply changes/updates to the System/equipment.

4.14.3 Contractors shall bring with them a mobile computer (i.e. laptop) which contains the latest version of anti-virus software, complete with up to date virus signatures to confirm onsite within CMH premises that their media to be connected (i.e. USB) is free of malicious code.

4.14.4 Contractors shall ensure portable media (USB stick, CD/DVD, etc.) is scanned (in addition to clause 4.14.3) on a CMH PC to ensure that the media is not infected by virus, worms and spyware before being used to apply changes/updates to the System/equipment.

4.14.5 Contractors shall ensure the vendor provides CMH a completed attestation of compliance to confirm the media or device to be connected to the System/equipment has been scanned for viruses and found to be free of

malicious code.

4.14.6 Contractors shall perform technical support on-site unless appropriate remote support arrangement is endorsed.

4.14.7 Contractors shall erase the sensitive data in the storage devices of the System/equipment before taking away the equipment for repairing or disposal.

4.14.8 Contractors shall sign and fully comply with a non-disclosure confidentiality agreement during on-site and remote support.

4.14.9 Contractors should use different portable media (i.e. USB sticks), which have been scanned for malicious code, for each item of External network equipment they need to apply an update to.

4.14.10 Contractors shall where not able to use different individual portable media (i.e. USB sticks) for applying changes/updates to multiple items of External network equipment (see clause 4.14.9), repeat Clauses 4.14.3 and 4.14.4 before proceeding to attach/apply the portable media to the second and subsequent items of External network equipment.

**4.15 Decommissioning Support**

4.15.1 Contractors shall ensure that upon decommissioning of the System/equipment, data exports and data definitions (sometimes known as data dictionary) are provided for all clinical data, and other data as appropriate, in a data structure and format as required by CMH.

4.15.2 Contractors shall provide assistance, as required, for the successful migration of any data to a new replacement System/equipment as adopted by CMH.

**4.16 Security Incident Reporting and Compliance**

4.16.1 Contractors shall ensure the System/equipment provides health-checking and audit logging capabilities.

4.16.2 Contractors shall immediately report to the Government and the Operator of the CMH any security incident relating to the System/equipment.

4.16.3 Contractors shall submit security compliance reports upon request by the Government with respect to the requirements stipulated in this document. Appendix A provides a sample of a “Network Security Compliance Report” which should be used.

**4.17 Clinical Data Exchange**

4.17.1 Contractors shall ensure seamless electronic data exchange with systems that supplied by the Government complies with Health Level Seven (HL7) standard.

4.17.2 Contractors shall ensure any electronic message exchange with the IT systems

that supplied by the CMH includes reference keys such as:

(a) HKID

(b) Name

(c) Date of birth

(d) Sex

Note: Electronic message exchange is important to ensure high integrity associated with patient identification and automatic mapping to patient records within the CMH.

4.17.3 Contractors shall ensure the System/equipment maintains the existing exchange of patient data with the IT systems that supplied by the CMH and provides exchange for other data including but not limited to:

(a) Admit, discharge & transfer, and patient demographics

(b) Allergy, Adverse Drug Reaction and Alert information

(c) Clinical order, observations and results

(d) Multimedia and imagery data

4.17.4 Contractors shall ensure the System/equipment automatically updates patient's demographic data upon reception of ADT message.

4.17.5 Contractors shall ensure the System/equipment adopts the preferred date format that align with CMH standard, including but not limited to:

(a) For the display of date in frontend screen;

(b) For the display of date-time in frontend screen;

(c) For the transfer of date information to IT systems that supplied by the CMH;

(d) For the transfer of date-time information to IT systems that supplied by the CMH.

Note: This enables user friendliness and system interoperability to be achieved.

4.17.6 Contractors shall ensure the System/equipment sends update or delete messages, if necessary, to perform corresponding actions with the IT systems that supplied by the CMH, with proper authorization mechanism from supervisor and audit trail.

4.17.7 Contractors shall ensure the System/equipment provides appropriate feedback to users to indicate the successfulness of message exchange with the IT systems that supplied by the CMH. (e.g. system alert to users).

**Sample Network Security Compliance Report** **Appendix A**

**Department:** **Name of System:**

**Location:** **IP Subnet:**

**Reviewer:** **Date:**

| Items for Verification with Contractor | | Comply (Y/N) | Remark |
|---|---|---|---|
| **A. Data Security (Review in regular basis)** | | | |
| A1 | Restricted data downloaded from the System/equipment to end-user devices should be encrypted | | |
| A2 | Restricted data transferring between the System/equipment and other CMH IT systems should be encrypted | | |
| A3 | Restricted data stored within the System/equipment should be encrypted | | |
| A4 | Restricted data stored in backup storage should be encrypted | | |
| A5 | Restricted data must not be exported for any usage unless prior authorisation has been obtained from the Government. | | |
| A6 | Is the restricted data in the System/equipment and backup being protected from unauthorized access / leakage, including physical security controls? Please specify the controls in “Remark” | | |
| **B. Application Security (Review in regular basis)** | | | |
| B1 | The application should support role-based access control | | |
| B2 | The application should employ prevalent authentication mechanism at reasonable safety level | | |
| B3 | The application should apply network level encryption | | |
| B4 | The application should provide health-checking information | | |
| B5 | The application should keep audit logs | | |
| **C. Server Security (Review in regular basis)** | | | |
| C1 | Contractor should implement the server security according to Government security policy and guidelines | | |
| C2 | Contractor should install into the servers an anti-virus program running with the latest virus definitions | | |

| | | | |
|---|---|---|---|
| C3 | Contractor should install the latest security patches in the servers | | |
| C4 | Contractor should perform a regular scanning in the servers | | |
| **D. Client / Desktop Security (Review in regular basis)** | | | |
| D1 | Contractor should implement the security controls at the PCs of the System, such as anti-virus | | |
| **E. Security Incident Reporting (On-going exercise)** | | | |
| E1 | Contractor should immediately report security incidents to CMH management | | |
| **F. Contractor Maintenance (Review in regular basis)** | | | |
| F1 | Contractor should erase the data in storage devices before taking away the equipment for repair | | |
| F2 | Contractor should perform technical support on-site unless appropriate remote support arrangement is endorsed | | |
| F3 | Contractor support staff should sign the non-disclosure confidentiality agreement | | |
| F4 | When equipment is required to be taken away for offsite repair, are there ways to remove / erase / protect the restricted data in the equipment from leakage? Please specify the controls in “Remark” | | |
| **G. Privacy Control (Review in regular basis)** | | | |
| G1 | Are there any user authentication controls present in the System/equipment? | | |
| G2 | Is unique user ID being assigned to every user? | | |
| G3 | Does the System/equipment allow setting of complex password such as upper / lower case, alpha, numeric and special characters? | | |
| G4 | Does the System/equipment provide audit trails of user accesses? Please specify the controls in “Remark”. | | |
| G5 | Is there any means to synchronize System/equipment time with a trustworthy time server for accurate system record? | | |