Annexes:

Annex A - Chinese Medicine Pharmacy (CMPh) Floor Plan (For Indicative Only)

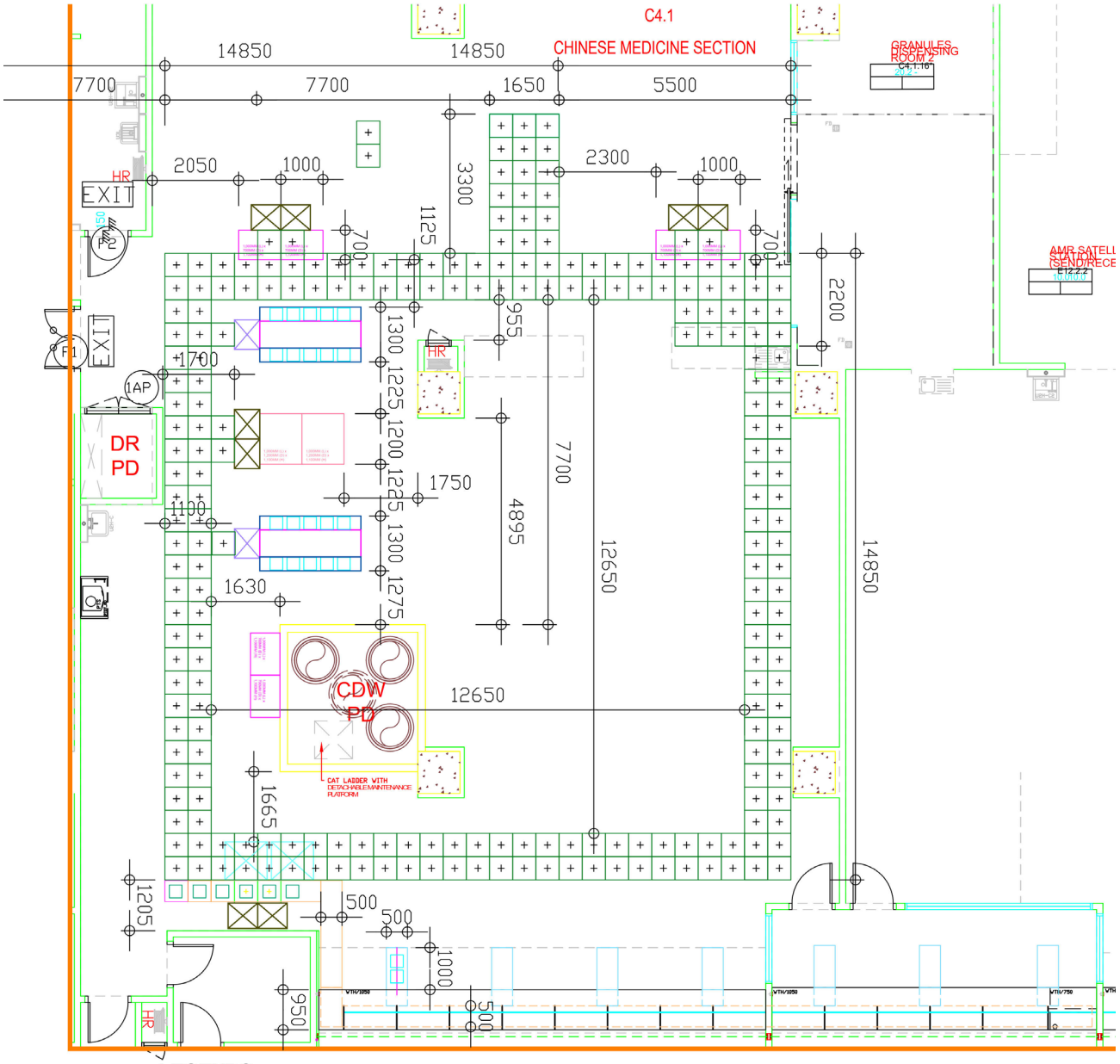
Annex B - Operation Details of Chinese Medicine Pharmacy (CMPh) Sections (For Reference Only)

Annex C - CMHHK IT Infrastructure Services Specifications for Furniture and Equipment

Annex D - CMHHK IT Security Guidelines for Furniture and Equipment

Annex A

Chinese Medicine Pharmacy (CMPh) Floor Plan (For Indicative Only)



LEGENDS:

- Mini Automated Guided Vehicles (AGVs) Pathway at Overhead Platform (OHP)
- 3 Dimensional Sorter (3DS) and totes storage racks
- Mini Lifters (LFT) (At dispatching stations & Offloading points)
- Mini Lifters (LFT) (At 3DS)
- Totes Stacker and De-stacker (TSDS)
- Totes sized 300mm (L) x 300mm (W) x 200mm (H)
- Floor Level Conveyor (FLC)
- Extended Floor Level Conveyor (FLC)
- Totes manual entry station
- Totes Elevator
- AGVs charging station
- Dual-sided totes storage bench (with PTL) 1,000mm (L) x 1,200mm (D) x 1,100mm(H)
- Single-sided totes storage bench (with PTL) 1,000mm (L) x 700mm (D) x 1,100mm(H)

Annex B

Operation Details of Chinese Medicine Pharmacy (CMPh) Sections (For Reference Only)

ZONE I

1 Chinese Medicines Granules Dispensing Room

1.1 This section serves to provide dispensing of Chinese medicines granules (CMGr) into CMPACK ready-to-take packaging through automation. It integrates with HIS (PMS) for correct product selection and correct weighing of each product via barcode verification, and labeling of final product.

1.2 Outgoing CMPACK ready for dispatch shall match the barcoded with CMPTS and transferred from LFT (Outside Chinese Medicine Granules Dispensing Room) through the AGVs and FLC to Pharmacy issuing counter.

The completed CMPACK shall be transferred directly to the designated issuing stations at Pharmacy issuing counter. The partially completed CMPACK shall be transferred to the designated totes at 3DS via LFT for re-dispatching

The information of the entering barcoded totes shall be recorded to the Chinese Medicine Package Transfer System (CMPTS); and shall be diverted to the designated assembly stations for product assembling / Pharmacy issuing counter for product issue. CMH Operator will receive the barcoded totes at the designated offloading point.

2 Chinese Medicine Pharmacy

2.1 This section serves to provide dispensing of loose Chinese medicines (CM) decoction pieces, also known as Yin Ping (YP) [飲片], by two methods of dispensing through either automation or manual handling.

Automation refers to automatic stock replenishment of YP [飲片] to the automation machine by robotic arms; and automatic dispensing of YP [飲片] (including product selection, image capture, weighing and verification of each YP) into individually sealed, labelled and barcoded daily-dose or multiple-doses pack.

Manual handling refers to manual stock replenishment of YP [飲片] to CM cabinets [百子櫃]; and manual dispensing of YP [飲片] (including product identification, picking, weighing, bagging, labelling and verification) into daily-dose or multiple-doses pack.

2.2 Outgoing CMPACK ready for dispatch shall match the barcode with Chinese Medicine Package Transfer System (CMPTS) and transferred through the AGVs, LFT, 3DS and FLC to Pharmacy issuing counter.

The completed CMPACK shall be transferred directly to the designated issuing stations at Pharmacy issuing counter. The partially completed CMPACK shall be transferred to the designated totes at 3DS via LFT for re-dispatching. The information of the entering barcoded CMPACK and totes shall be recorded to the CMPTS. CMH Operator shall receive the barcoded totes at the designated offloading point

2.3 Upon receipt or dispatch of the barcoded totes, the CMH Operator shall verify information with HIS (PMS) to ensure the right products are dispensed, labelled and assembled without missing any.

3 Chinese Medicines Assembly Station

3.1 Dispensed Chinese medicines (CMs) from manual dispensing, decoction, compounding CM products with proper labelling shall be transferred in barcoded CMPACK by AGVs at OHP, LFT and 3DS to the designated assembly table for product assembling.

3.2 This section shall receive incoming CMPACK or dispatch outgoing CMPACK via AGVs at OHP and LFT. Outgoing product for dispatch shall match the barcoded with CMPTS before transfer. The information of the incoming / outgoing barcoded totes shall be recorded to the CMPTS; and shall be diverted to the Pharmacy issuing counter for product issue. CMH Operator shall receive the barcoded totes at the designated offloading point.

3.3 Upon receipt or dispatch of the barcoded totes, the CMH Operator shall verify information with HIS (PMS) to ensure the right products are dispensed, labelled and assembled without missing any.

ZONE II

4 Chinese Medicine Pharmacy Issuing Counter

4.1 The FLC situated underneath the issuing stations shall collect the ready for dispatch CMPACK in individual tote from the connecting to the extended FLC transferred from various section above.

4.2 The ready for dispatch CMPACK shall be transferred automatically to the assigned issuing window under a queuing / sequencing system for CMPACK issuance and patient counseling

Annex C

CMHHK IT Infrastructure Services Specifications for Furniture and Equipment

This document describes the CMHHK IT infrastructure services and their technical specifications for vendors who plan to implement Furniture and Equipment solutions in the CMHHK.

1) The following CMHHK IT infrastructure services will be provided by the Government

1. Network Services

(a) Type of network connections in different area:

Type of network connection	**Description** [ii]
Server or network equipment in data centers [i]	Speed: 10 Gb/s Connector: Multi-mode LC fiber
Data outlets [i]	Speed: 1 Gb/s Connector: RJ45
Network across primary and secondary data centers	Speed: 10 Gb/s
Wireless LAN	Wi-Fi 6

Notes:

i. Network patch cord will **NOT** be provided.
ii. Gb/s : gigabit per second; LC : Lucent Connector

2. Data Centre Services

(a) Data Centre Services include Primary Data Centre in CMHHK Building and Secondary Data Centre in hosting site.
(b) EIA standard 19-inch 42U equipment rack (with depth = 1,200mm).
(c) Mobile cart with monitor and keyboard (with touchpad or trackball) will be available for share use.
(d) Environment

Indoor temperature	23°C ± 3°C
Indoor relative humidity	50% ± 10%

(e) Power supply
   i. Two power distribution units (PDU) with output power connection type IEC 320 C13 and IEC 320 C19 will be available in equipment rack and supported by different Uninterruptible Power Supply ("UPS")
   ii. Power cord will **NOT** be provided.

3. Common Infrastructure Services

   (a) Domain Name System ("DNS")
   (b) Lightweight Directory Access Protocol ("LDAP") for account authentication
   (c) Network Time Protocol ("NTP") service
   (d) Global Server Load Balancing ("GSLB") service

Annex D

CMHHK IT Security Guidelines for Furniture and Equipment

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.

The Contractor 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. The Contractor 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 CMHHK'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. The Contractor 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 CMHHK.

4. Security Principles

4.1 Safety

4.1.1 The Contractor 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 The Contractor shall ensure the System/equipment does not create any non-compliance with regulatory or legal frameworks.

4.2 Confidentiality and Privacy

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

4.4.3 The Contractor 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 The Contractor 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 The Contractor shall ensure the System/equipment is able to effectively function together with other System/equipment.

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

4.5.3 The Contractor 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 The Contractor shall ensure updates for patching of vulnerabilities are maintained throughout the System/equipment's lifetime.

4.7 Data Sovereignty

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

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

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

4.8 System Hardening

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

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

4.9 Data Security

4.9.1 The Contractor 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 The Contractor shall ensure restricted data stored within the System/equipment is encrypted.

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

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

4.9.6 The Contractor 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 CMHHK PC before the data is being copied.

4.10 Application Security

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

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

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

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

4.11 Malicious Code Protection

4.11.1 The Contractor 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 The Contractor shall ensure the System/equipment is protected with regular updates of the latest virus definitions.

4.11.3 The Contractor 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 The Contractor shall ensure virus definitions are updated within 24 hours from the date of release.

4.11.5 The Contractor 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 The Contractor 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 The Contractor 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 The Contractor shall ensure any network connection for a System/equipment to the CMHHK network is endorsed by CMHHK and implemented and operated according to CMHHK policies, procedures and guidelines.

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

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

4.14 Maintenance Support

4.14.1 The Contractor 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 The Contractor shall ensure that where maintenance on the System/equipment needs to be performed, that CMHHK 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 The Contractor 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 CMHHK premises that their media to be connected (i.e. USB) is free of malicious code.

4.14.4 The Contractor shall ensure portable media (USB stick, CD/DVD, etc.) is scanned (in addition to clause 4.14.3) on a CMHHK 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 The Contractor shall ensure the vendor provides CMHHK 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 The Contractor shall perform technical support on-site unless appropriate remote support arrangement is endorsed.

4.14.7 The Contractor 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 The Contractor shall sign and fully comply with a non-disclosure confidentiality agreement during on-site and remote support.

4.14.9 The Contractor 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 The Contractor 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 The Contractor 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 CMHHK.

4.15.2 The Contractor shall provide assistance, as required, for the successful

migration of any data to a new replacement System/equipment as adopted by CMHHK.

4.16 Security Incident Reporting and Compliance

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

4.16.2 The Contractor shall immediately report to the Government and the CMHHK Operator any security incident relating to the System/equipment.

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

4.17.2 The Contractor shall ensure any electronic message exchange with the IT systems that supplied by the CMHHK 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 CMHHK.

4.17.3 The Contractor shall ensure the System/equipment maintains the existing exchange of patient data with the IT systems that supplied by the CMHHK 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 The Contractor shall ensure the System/equipment automatically updates

patient's demographic data upon reception of Admit, Discharge and Transfer (ADT) messages.

4.17.5 The Contractor shall ensure the System/equipment adopts the preferred date format that align with CMHHK 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 CMHHK;

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

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

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

4.17.7 The Contractor 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 CMHHK. (e.g. system alert to users).

Department: **Name of System:**

Location: **IP Subnet:**

Reviewer: **Date:**

Items for Verification with the 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 CMHHK 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	The Contractor should implement the server security according to Government security policy and guidelines		
C2	The Contractor should install into the servers an anti-virus program running with the latest virus definitions		

C3	The Contractor should install the latest security patches in the servers		
C4	The Contractor should perform a regular scanning in the servers		
D. Client / Desktop Security (Review in regular basis)			
D1	The Contractor should implement the security controls at the PCs of the System, such as anti-virus		
E. Security Incident Reporting (On-going exercise)			
E1	The Contractor should immediately report security incidents to CMHHK management		
F. Contractor Maintenance (Review in regular basis)			
F1	The Contractor should erase the data in storage devices before taking away the equipment for repair		
F2	The Contractor should perform technical support on-site unless appropriate remote support arrangement is endorsed		
F3	The 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?		

[END OF APPENDICES]