Information Classification: Restricted, Sensitive (Normal)

MOHH IT Security Requirements

Important Notes

1. This document contains a generic set of security requirements. The Participating Service Provider shall assess the security requirements and respond "Not Applicable" where necessary.

2. No security requirements shall be removed from this document, unless otherwise approved by the Security team and/or Management.

3. If it is an Internet-facing IT system implementation or a "Major" project that involves the installation of "New IT 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 consultant if there is any Non-Compliance (NC) or Partial Compliance (PC) or Non-Applicability (NA) for any IT security requirement.

4. A security management consultant may add additional security requirements for each system or project where necessary.

5. **This document is applicable if the proposed system is to be implemented in-house**.

PART 3
MOHH IT SECURITY REQUIREMENTS: SYSTEMS INSTALLED ON-PREMISES (HEALTHCARE DATA CENTER)

MOH HOLDINGS

TABLE OF CONTENTS

1 SECURITY MANAGEMENT AND GOVERNANCE FRAMEWORK

1.1 Security Management

1.1.1 The Participating Service Provider shall comply with the Company's IT security policies, standards and any instructions on security matters that may be issued by the Company from time to time.

1.1.2 The Participating Service Provider shall align with the Company's security framework, which includes the following:

(a) Security architecture and design;
(b) Security management and operation processes; and
(c) Security incident handling, investigation and response processes.

1.1.3 The Participating Service Provider shall provide security operation manuals (indicating conformance to any industry security standard) in relation to **Clause 1.1.2** above.

1.1.4 The security operation manual shall also be communicated and applicable to all the Participating Service Provider's sub-contractors.

1.1.5 The Participating Service Provider shall document and maintain all systems configurations, processes and procedures that are relevant to the supply and operations of the proposed system. The Participating Service Provider shall establish a proper data and document control management system or process to ensure the confidentiality, integrity and availability of all its data and documentation, in accordance with the approved security policies.

1.1.6 The Participating Service Provider shall provide details of the security measures proposed for the system and services, and shall clearly demonstrate that the integrity of the Company's network and computing environment is not compromised by the service provided.

1.1.7 The Participating Service Provider shall protect and ensure the confidentiality, integrity or availability of the Company's systems, networks and data in all stages of the project lifecycle. The Participating Service Provider shall not disclose any of the Company's information to any other party without prior written consent from the Company.

1.1.8 The Participating Service Provider shall provide the additional costs for the supply and implementation of security measures if they are not included in the core system. This portion of the products and services shall be taken as optional and will be taken into consideration during the evaluation of the Participating Service Provider's Proposal.

1.1.9 The Participating Service Provider should adopt the Security-by-Design framework (e.g. Cyber Security Agency of Singapore's security by design framework or equivalent) in its system development lifecycle process.

1.1.10 The Participating Service Provider shall ensure that when proposing new software, products, applications, and/or systems to be used for storing, processing or accessing sensitive information such as patient data and for supporting essential services, the proposed new software, products, applications, and/or systems shall be security certified in accordance with international, national or industry-recognized standards such as ISO/IEC 15408, FIPS 140-2, IEC 62443, etc., where possible.

1.2 Security Risk Management

1.2.1 The Participating Service Provider shall assist the Company's risk assessment team to conduct security risks assessment to identify internal and external threats that may undermine the proposed system's confidentiality, integrity, or availability before system commissioning.

1.2.2 The Participating Service Provider shall implement control measures that mitigating security risks proposed by the Company's risk assessment team (if any) before system commissioning.

1.2.3 The Participating Service Provider shall also assist the Company's risk assessment team to conduct security risk assessments annually and whenever there are major changes to the proposed system to identify internal and external threats that may undermine the proposed system's confidentiality, integrity, or availability, result in the unauthorized disclosure or destruction of information, or result in a breach of security policies.

Major change refers to a change that: (a) impacts the security function of the application system (such as authentication, access controls, logging, etc.); or (b) has medium or high business impact to the application system (such as those affecting key business functions).

1.2.4 The Participating Service Provider shall facilitate security risk assessments by providing the Company's risk assessment team with the following design documents:

(a) Asset list (e.g. network, servers, applications, tools, etc) within the proposed system;
(b) System architecture diagram;
(c) Network architecture diagram;
(d) Application architecture diagram; and
(e) Data flow diagram.

1.3 Security Personnel

1.3.1 The Participating Service Provider shall appoint a security lead to be overall responsible for ensuring the security and integrity of the proposed system, including all its supporting infrastructure systems. The responsibilities of the security lead shall include:

(a) Preparing information systems security policies and action plans;
(b) Evaluating and recommending information security products for use within the environment;
(c) Managing and conducting investigations on any alleged computer or network security compromises, incidents, or problems;
(d) Keeping up-to-date on the latest security threats and solutions;
(e) Recommending new controls to resolve security incidents or to counter new security threats identified;
(f) Liaising and co-ordinating with partner companies, security organizations and the Company on security matters; and
(g) Performing other activities necessary to assure a secure environment.

1.3.2 The security lead shall be contactable via mobile phone. The contact information of the security lead shall be made available to the Company. The security lead shall be experienced and proficient in carrying out the works required by the Company. The key personnel shall preferably have internationally recognized security certifications such as Certified Information Systems Security Professional (CISSP), CISM, SAN GIAC

certifications, etc.

1.3.3 The security lead shall be informed of all security breaches, and shall be responsible for the following:

(a) Ensuring that security breaches are brought to the attention of those concerned, including advising on measures to ensure that security incidents are immediately reported to the Company;
(b) Maintaining records of all security breaches; and
(c) Ensuring that action is taken to investigate, minimize damage and prevent recurrence.

1.4 Outsourced Development

1.4.1 Where there is any outsourcing of system development, a secure-by-design approach to system development shall be adopted, and the following additional controls shall be implemented:

(a) The development environment shall be protected with an anti-malware solution;
(b) Vulnerability and patch management process shall be in place;
(c) The development environment shall not use production URLs;
(d) The development environment shall be decommissioned upon expiry or termination of the relevant agreement; and
(e) The Company shall have the right to perform audits on development processes and controls (including the right to appoint a third party to conduct such audits).

2 SECURITY STANDARDS

2.1 Cryptographic Standards and Network Security Standards

2.1.1 The following cryptographic standards shall be employed if cryptographic controls are used to protect the confidentiality, integrity and authenticity of information collected, processed and stored on the proposed system:

(a) Asymmetric Encryption

(i) RSA public key encryption with key sizes of at least 2048 bits; or
(ii) Elliptic Curve Cryptography (ECC) with key sizes of at least 384 bits.

(b) Symmetric Encryption

(i) Advanced Encryption Standard (AES) with key sizes of 256 bits; or
(ii) Secure and Fast Encryption Routine (SAFER) SK-128.

(c) Message Digest / Hash Algorithm

(i) Secure Hash Standards (SHA-2) with key size of at least 384 bits; or
(ii) Secure Hash Standards (SHA-3) with key size of at least 384 bits.

2.1.2 The following cryptographic protocols shall be employed in conjunction with the relevant standards stated in **Clause 2.1.1** above:

(a) Transport Layer Security (TLS) Protocol: TLS version 1.2 and above;
(b) File Transfer Protocol: SFTP / FTPS;

(c) Secure Shell (SSH) version 2;
(d) Wi-Fi Protected Access (WPA) Standard: WPA2 and above.

2.1.3 If digital certificates are to be deployed in the proposed system, the Participating Service Provider shall ensure that the certificates are procured from trusted certificate authorities with reliable certificate lifecycle management processes, such as certificate revocation lists (RFC 3280) and/or Online Certificate Status Protocol (OCSP) (RFC 2560) service provisions, and shall manage the lifecycle of the digital certificates, including renewal and revocation with the certificate authority. All certificates shall also conform to X.509 version 3.

2.1.4 The Participating Service Provider shall track the expiry dates of all digital certificates and renew them before expiry.

2.1.5 The Participating Service Provider shall implement procedures to make sure that all cryptographic keys used in the proposed system are managed appropriately throughout their lifecycle, starting from creating or generating a key, distributing, installing, renewing, using, backing up, recovering, revoking and/or expiry of the key, to key destruction, including:

(a) Changing from the default values at the time of equipment installation and thereafter, on a periodic basis, depending on the nature of the IT systems and the risks involved;
(b) All cryptographic keys shall be securely generated and protected against unauthorized modification, copy, loss and destruction. Secret and private keys shall also be protected against unauthorized use and disclosure. Equipment used to generate, store and archive keys shall be physically protected;
(c) Storing cryptographic keys used within the proposed system separately from the data they are protecting, with access to the keys restricted to relevant authorized users;
(d) Ensuring that there are processes in place to recover the keys in the event that they are lost or corrupted; and
(e) Ensuring that when an IT system is decommissioned and data is no longer required, keys used shall be securely destroyed.

2.1.6 The proposed system shall log all cryptographic module failures.

2.2 Password Management

2.2.1 The Participating Service Provider shall not share passwords of its accounts.

2.2.2 Passwords shall minimally comply with the following:

(a) Be at least FIFTEEN (15) characters long for privilege accounts, and at least TWELVE (12) characters for non-privilege account (except for portable storage devices), and contain characters from at least TWO (2) of the following FOUR (4) categories:

(i) Upper case (A through Z);
(ii) Lower case (a through z);
(iii) Digits (0-9); and
(iv) Special Characters (!, $, #, %, etc.).

The use of passphrases (concatenation of words or text or special character) shall be recommended.

(b) Be changed once every TWELVE (12) months;
(c) Not be reused for at least FIVE (5) generations;
(d) Not be displayed in clear;
(e) Not transmitted or stored in plaintext;
(f) Be stored in a form that is resistant to offline attacks;
(g) Be forced to change on first use;
(h) Not be the same as the account ID or user ID;
(i) Consecutive failed authentication attempts that can be made on a single account be limited to FIVE (5) times or less; and
(j) Be able to protect the system against dictionary or brute-force attacks. For internet-accessible application systems, the Participating Service Provider shall reject users from having commonly used, expected or compromised passwords. The reason for rejection shall be provided in order to assist users.

3 DATA SECURITY

3.1 Information Handling by the Participating Service Provider

3.1.1 The Participating Service Provider shall be accountable for protecting all data under its due care to ensure that it is not used for other purposes, unless the use has been authorized by the Company and permission is obtained.

3.1.2 All personnel engaged by the Participating Service Provider to perform any tasks shall each sign a confidentiality agreement to protect the Company against unauthorized disclosures of restricted information accessed by the personnel in the course of the relevant agreement.

3.1.3 Termination or expiry of the relevant agreement for whatever cause shall not put an end to the security obligations and obligations of confidentiality imposed on the Service Provider, its employees, agents and sub-contractors under the IT security requirement related clauses. The Service Provider shall ensure that no person shall remove any restricted information upon resignation from his/her appointment or retain such information when he no longer requires them for the purposes of performing his/her duties pursuant to the Service Provider's obligations as all such information must remain in the possession of the Company.

3.1.4 The Participating Service Provider shall have a system of control measures to protect restricted information against accidental or unlawful loss, as well as unauthorized access, disclosure, copying, use, or modification. The system shall include administrative, technical, physical and personnel control measures. The Participating Service Provider shall protect the data regardless of the format in which it is held.

3.1.5 The Participating Service Provider shall ensure that during data migration, no data is copied to any media, including hard drives, flash drives, or other electronic device, unless expressly approved by the Company. The approved usage and disposal process shall be complied with, for any media that was approved for data migration.

3.2 Data Protection

3.2.1 Restricted data within the proposed system shall be restricted to only authorized users as defined in the access control matrix (refer to **Clause 6.2.1** below).

3.2.2 The Participating Service Provider shall ensure that proper controls are in place for restricted data owned by the Company. The Participating Service Provider shall also ensure

that the aforementioned data is segregated from data which is not owned by the Company, but which is handled by the Participating Service Provider or its sub-contractor.

3.2.3 The Participating Service Provider shall ensure that the data centre for processing and storing the Company's data is only located in Singapore.

3.2.4 The Participating Service Provider shall ensure that restricted data sent over the network is in encrypted format as defined in **Clause 2.1.2** above (such as using TLS or SSH).

3.2.5 The Participating Service Provider shall ensure that restricted data is backed up to backup media in an encrypted format to protect its confidentiality.

3.2.6 The Participating Service Provider shall ensure that restricted data stored on databases, file systems, print servers (print spools) and storage systems is protected against unauthorized access. Encryption shall be used, where applicable.

3.2.7 The Participating Service Provider shall propose Transparent Data Encryption (TDE) solution on databases or field-level encryption. As an alternative to encryption, the Participating Service Provider shall also consider the use of technologies such as format-preserving encryption and tokenization to "de-identify" Personally Identifiable Information (PII) to protect them when stored in database. These are re-identified "on the fly" only when required to be presented at the frontend, or for backend processing. The Participating Service Provider shall implement the security measures upon approval by the Company and provide evidence of such implementation.

3.2.8 The Participating Service Provider shall ensure that all removable storage media are scanned for malware prior to usage.

3.2.9 The proposed system shall have the capability to allow the Company to define different patient/personnel groups (such as VVIP, VIP, CIP, potential medical legal cases, etc.), to tag specific patient/personnel under one or more of the groups defined, and to restrict access to each patient/personnel group to selected user groups, including in reports, memos and referrals.

3.2.10 The proposed system shall have the capability to allow the Company to define sensitive patient/personal data type (such as confidential tests in health screening packages, HIV, STD, TOP, mental illness, etc., or sensitive personal data such as salary, performance rating, etc.), and to restrict access to each data type to selected user groups, including in reports, memos and referrals.

3.2.11 The proposed system shall implement the following additional controls to protect selected patient/personnel groups:

(a) The proposed system shall re-validate the identity of the users before they are allowed to access such patient/personnel records;
(b) The proposed system shall require the users to enter the reason for access;
(c) The proposed system shall send email alerts to relevant parties on access to such patient/personnel records, including failed access attempts;
(d) The proposed system shall perform audits and log all accesses including failed access attempts; and
(e) The proposed system shall prevent such patient/personnel records from being sent to data warehouse or included in ad-hoc reporting.

3.2.12 The proposed system shall implement the following additional controls to restrict access to

sensitive data types:

(a) The proposed system shall re-validate the identity of the users before they are allowed to access such data;
(b) The proposed system shall require the users to enter the reason for access; and
(c) The proposed system shall perform audits and log all accesses including failed access attempts.

3.2.13 The Participating Service Provider shall ensure that restricted reports (e.g. VIP records) are identified and procedures are drawn up for distribution and disposal for these reports.

3.2.14 The Participating Service Provider shall ensure that restricted data (such as Sensitive Health Information (SHI) and/or PII), is masked or removed, where applicable, when printed on hardcopy reports or sent electronically as email or using other communications systems.

3.2.15 The Participating Service Provider shall describe how the proposed system will ensure that patient/personal data and any PII data are protected from security risk for any services that the proposed system provides through the internet.

3.2.16 The Participating Service Provider shall ensure that production data containing SHI or PII is not used for development or testing purposes, unless such SHI or PII has been removed, anonymized or masked, in order to ensure that there are no reasonable means for the data to be re-identified.

3.2.17 The Participating Service Provider shall ensure that production data is securely erased from a test environment immediately after the testing is completed.

3.2.18 The Participating Service Provider shall ensure that the copying and use of production data are approved by the Company and logged to provide an audit trail.

3.3 Media Sanitization

3.3.1 The following standards sanitisation methods shall be used to minimise the possibility of recovering any data from storage media:

(a) Overwrite (O)

Overwrite all addressable area of the storage media using media-dependent sanitisation techniques, (such as ATA SECURE ERASE UNIT command, SCSI SANITIZE command, Block Erase for solid-state media), or according to the following Media Sanitization Standards:

(i) NIST special publication 800-88 guidelines for media sanitization (Degaussers);
(ii) Peter Gutmann Secure Deletion;
(iii) NIST Special Publication 800-88 Guidelines for Media Sanitization (Optical Media Destruction Devices);
(iv) Bruce Schneier algorithm;
(v) US Department of Defence (DoD 5220.22-M).

(b) Cryptographic Erase (C)

Sanitize the encryption key used to encrypt the target data. Cryptographic erase option may only be used if the following is practised:

(i) The strength of the encryption key complies with the cryptography standards stated in **Clauses 2.1.1** and **2.1.2** above:
(ii) Media encryption is enabled prior to storing any restricted data on the media;
(iii) The encryption key is sanitised using appropriate media-specific sanitisation techniques specified in **Clause 3.3.1(a)** above; and
(iv) The sanitisation shall not be initiated remotely for mobile devices (i.e. over a network), but directly in person on the device.

(c) Degauss (D)

Degauss using degaussers recommended in the Media Sanitization Products below that match or exceed the magnetic coercivity of the storage media:

(i) BCWipe 4.1.2;
(ii) BCWipe Total Wipeout 3.0.4;
(iii) Darik's Boot and Nuke (DBAN) 2.3;
(iv) Eraser 6.1;
(v) SEM Mag EraSURE ME-P3E 2;
(vi) iShredder 4.0.

(d) Shred (S)

For all types of storage media, shred using purpose-built storage media shredder. Optical media shall be physically destroyed into particles that have nominal edge dimensions of 5 mm and surface area not larger than 25 sq. mm.

(e) Incinerate (I)

Incinerate at a commercial incinerator.

3.3.2 The following shall be adhered to when re-deploying, repairing or disposing storage media that are used to contain restricted information:

Media Type / Use Case	Magnetic media	Solid-state media	Optical media
Re-deployment of fully functional media	O or C	O or C	X
Repair of media; Read and write access is possible	C, then O	C, then O	X
Repair of media; Read and write access is NOT possible	D, then S or I	X	X
End-of-life disposal; Read and write access is possible	O or C, then D, S or I	O or C, then S or I	S or I
End-of-life disposal; Read and write access is NOT possible	D, then S or I	S or I	S or I

O: Overwrite, C: Cryptographic Erase, D: Degauss, S: Shred, I: Incinerate, X: Not Allowed.

For mobile devices with built-in storage media, repair is allowed only if it is due to faulty parts such as faulty volume button, unresponsive buttons, damaged battery or broken

screen, where the ability to perform overwrite or cryptographic erase is not impacted. If this ability is impacted, the media shall be treated as an end-of-life disposal.

3.3.3 The Participating Service Provider shall adhere to the following procedures either at the Company's premises or at an approved site as part of the secure erasure of storage media:

(a) Only authorised personnel shall perform sanitisation and/or destruction;
(b) For destruction, only equipment maintained in good working condition shall be used (e.g. regular certification for degaussers, cleaning / oiling maintenance for cutters);
(c) Media shall continue to be:

(i) Physically secured at all times based on its security classification; and
(ii) Under the custody of authorized staff until data has been sanitized beyond recovery.

(d) Destruction shall be witnessed by at least ONE (1) staff from the Company not performing the destruction;
(e) Detailed documentation of the media, sanitisation and/or destruction process and declaration by staff and witness shall be maintained with the following documented:

(i) Description of the media (type, model and serial number);
(ii) Method of sanitisation used;
(iii) Reason for sanitization of the media (i.e. re-deployment, repair, disposal);
(iv) Authorization letter from the Company's approving authority;
(v) The name(s) and signature(s) of the personnel executing the procedures and the witnesses verifying the results of the process; and
(vi) The intended recipient of the storage media.

3.3.4 The Participating Service Provider shall refer to the Media Sanitization Standards and Media Sanitization Products for the supported technology standards and products for degaussing and sanitisation, as specified in **Clause 3.3.1** above. The Participating Service Provider shall obtain the Company's approval for the use of any Media Sanitization Product.

3.4 Physical Media Transfer

3.4.1 The Participating Service Provider shall develop procedures to protect backup media containing restricted information from unauthorised access, misuse or corruption during transportation to off-site facilities.

3.4.2 In the event that the proposed system is hosted in a third-party data centre, the Participating Service Provider shall ensure that records are kept to identify the content of the backup media, the protection applied to the backup media, and to record the times the backup media is transferred to the transit custodians and received at the destination.

3.5 Data Loss Prevention

3.5.1 The Participating Service Provider shall ensure that the following measures are implemented where systems are classified as Mission-Critical systems with Restricted (Sensitive High) data:

(a) Database Activity Monitoring (DAM) system, as specified in **Clause 7.3** below, to monitor database that is classified as Mission-Critical systems with Restricted (Sensitive High).

4 SYSTEMS SECURITY

4.1 Authentication and Access Control

4.1.1 All requests to provide access to systems by the Participating Service Provider shall be formally approved by the system owner(s).

4.1.2 All users shall have a unique identifier (user ID) for their own use so that activities can be traced to the responsible individual for all types of users, including but not limited to:

(a) Application support personnel;
(b) Operators;
(c) Network administrators;
(d) System administrators;
(e) Security administrators; and
(f) Database administrators.

4.1.3 All access to the servers, infrastructure and database systems shall be done through a secure channel (such as SSH) via the Company's Privileged Access Management (PAM) server. If the proposed system is deployed in a data centre not managed by the Company, then the Participating Service Provider shall provide and implement the Company's standard PAM tool, and all access shall be logged to facilitate independent reviews of the access and transactions completed.

4.1.4 The Participating Service Provider shall use SingPass or CorpPass as the main authentication mechanism for all digital services serving the public or companies, respectively.

4.1.5 The Participating Service Provider shall leverage on the Company's TWO-(2)-Factor Authentication (2FA) platform to authenticate all access by the Participating Service Provider and the Company's IT support staff to the servers and infrastructure systems used in support of the proposed system. Users with system or application administrative roles shall be authenticated with 2FA.

4.1.6 All passwords used within the proposed system shall conform to the password standards stated in **Clause 2.2** above.

4.1.7 The Participating Service Provider shall ensure that all access is granted on a "need-to-have" basis and is strictly controlled to reduce the exposure of unauthorized activities. Such access shall be reviewed on a quarterly basis and removed promptly when not required.

4.1.8 Application services shall not run under super-user privileges.

4.1.9 Access permissions to database objects (tables, views, stored procedures, etc.) shall be defined, and granted in accordance with the least privilege and "need-to-use" principle. Database connections shall be using database accounts assigned with minimum database privilege required.

4.1.10 Access to production copy of program source code and source libraries shall be strictly controlled to prevent the introduction of unauthorized functionality and to avoid unintentional changes.

4.1.11 The Participating Service Provider shall ensure that the production systems only hold

approved executable code and not development code or compilers.

4.1.12 The Participating Service Provider shall leverage on the Company's password vaulting and session recording solution to track, manage and approve requests for privileged user access (including system administrators, database administrator, privileged accounts) to production environment and to record the activities performed during such sessions.

4.1.13 Support accounts created for emergency use, such as for remote problem solving or fault resolution, shall only be enabled when required and disabled upon completion of the activity. A record of such access shall be maintained.

4.1.14 All servers, infrastructure and database systems shall be configured with timeout and automatic logout feature for non-active sessions.

4.1.15 The Participating Service Provider shall implement security measures to prohibit direct access by system administrators, database administrators or other privileged users to restricted information/data/records/databases, to prevent any unauthorized access, modification or deletion of restricted information. Access attempts by such users shall be securely logged and traceable.

4.2 Secure Configuration

4.2.1 The Participating Service Provider shall secure all components within the proposed system (from applications down to operating system level) in accordance with the Company's hardening standards, industry-accepted hardening standards from the Center for Internet Security (CIS), and/or Service Provider-specific security best practices. The actions required prior to the commissioning of the proposed system shall minimally include the following:

(a) Disabling or removing accounts that are not required (including test, sample, guest and default accounts);
(b) Disabling or removing unused ports, services and components;
(c) Changing all default passwords;
(d) Configuring service accounts as non-interactive; and
(e) Disabling autorun, etc.

4.2.2 For operating systems managed by the Company, the Participating Service Provider shall work with the Company to ensure that the proposed system is compatible with the Company's security hardening guidelines which are based on the CIS security benchmark.

4.2.3 The Participating Service Provider shall develop and maintain detailed security configurations of all system components used within the proposed system that are managed by the Participating Service Provider.

4.2.4 The Participating Service Provider shall ensure that the latest security patches for the servers, infrastructure, applications and databases systems are applied prior to system commissioning.

4.3 Protection Against Malicious Code

4.3.1 The Participating Service Provider shall leverage on the Company's anti-malware solution. This may require the installation of the anti-malware agent on the proposed system. The Participating Service Provider shall work with the Company to make sure that the anti-malware agent is compatible with the proposed system, and to allow automatic updates of

the agents and virus signatures. If the proposed operating system is not supported by the Company, the Participating Service Provider shall provide and implement an anti-malware solution supported on the proposed operating system.

4.3.2 The Participating Service Provider shall ensure that anti-malware scans are carried out regularly, in the event that anti-malware solution proposed by the Participating Service Provider is approved by the Company.

4.3.3 The Participating Service Provider shall provide and implement a content-scan solution to all file-based functionalities, including but not limited to, web-based file upload function and FTP-based file upload function.

4.3.4 As part of release management process, the Participating Service Provider shall scan release packages with the content-scan solution prior to deployment in the production environment.

4.3.5 The Participating Service Provider shall leverage on the Company's End-point Detection and Response (EDR) solution to protect the proposed system against advanced threats, including file-less and memory attacks. This may require the installation of the software agent on the proposed system, including servers and workstations. The Participating Service Provider shall work with the Company to make sure that the software agent is compatible with the proposed system, and to allow automatic updates of the agents and signature updates.

5 NETWORK SECURITY

5.1 Network Segmentation

5.1.1 The Participating Service Provider shall work with the Company to ensure that network segmentation is done to segregate traffic between internal, external and DMZ network segments related to the proposed system. Management traffic shall also be segregated from user traffic. Further network segmentation can occur within a network zone, if required.

5.1.2 Inbound connections from external networks shall be restricted to servers hosted in a DMZ segment. Direct inbound connections from external to internal networks shall not be allowed.

5.1.3 The Participating Service Provider shall ensure that development, testing, and production environments are logically separated.

5.2 Network Security Controls

5.2.1 The Participating Service Provider shall leverage on the Company's network firewall to inspect network traffic traversing across different network zones, so as to protect the network against malicious and unauthorized traffic to/from other networks or sub-networks (internal and external).

5.2.2 The Participating Service Provider shall leverage on the Company's Network-based Intrusion Detection (IDS) or Prevention Systems (IPS) to protect the proposed system against malware and network attacks.

5.2.3 The Participating Service Provider shall ensure that encryption is used to protect the transmission of classified data over the internet, intranet, virtual private networks (VPNs) and wireless networks.

5.2.4 If the Participating Service Provider proposes wireless networks solutions, the Participating Service Provider shall implement 802.1x authentication as the access control mechanism to provide user authentication, so that only authorized users are allowed to access the Company's enterprise networks. If the Company-approved devices are not able to support 802.1x authentication in a wireless network, the Participating Service Provider shall put in place another authentication method such as MAC address authentication.

5.2.5 If the Participating Service Provider proposes wireless networks solutions, the Participating Service Provider shall ensure that all wireless traffics are encrypted to protect the confidentiality and integrity of the data.

5.2.6 If the Participating Service Provider proposes wireless networks solutions that are set up to provide internet access to the general public, it shall be implemented as a physically-separated network with no connection to the Company's enterprise networks.

5.2.7 The Participating Service Provider shall work with the Company to fine-tune the IPS to optimize its protection capabilities and minimize false positives on an on-going basis.

5.2.8 The Participating Service Provider shall implement the following measures to protect internet-accessible systems and/or internet-accessible network infrastructure against Denial-of-Service (DoS) attacks:

(a) Web Application Firewall (WAF); or
(b) Clean-pipe scrubbing services; or
(c) Content Distribution Network (CDN) services.

5.2.9 The Participating Service Provider shall enable geo-location restriction (to the range of IP addresses assigned to Singapore) to the proposed system, if access to the proposed system from outside of Singapore is required.

5.2.10 The Participating Service Provider shall work with the Company's technical team to characterize and baseline the network traffic patterns of the proposed system. This is to facilitate the monitoring and detection of unusual network traffic patterns within the proposed system. If the proposed system is not hosted in a data centre managed by the Company, the Participating Service Provider shall provide and implement the Company's standard network traffic analyzer tool to monitor and detect any unusual network traffic patterns which may be indications of malicious activities, including:

(a) Host deviating from baselined traffic patterns;
(b) Worm propagation;
(c) Data exfiltration;
(d) Network scanning activities; and
(e) DoS attacks.

5.3 Security Configuration

5.3.1 The Participating Service Provider shall secure all network and security devices (including firewalls, routers, switches, etc.) within the proposed system in accordance with the Company's hardening standards, and/or Service Provider-specific security best practices. These shall minimally include the following before the proposed system is commissioned:

(a) Disabling or removing of unused accounts (including test, sample, guest and default accounts);

(b) Disabling or removing of unused ports, services and components;
(c) Changing of all default passwords;
(d) Configuring service accounts as non-interactive, and
(e) Disabling of autorun, etc.

The Participating Service Provider shall provide detailed checklists of the system hardening and secure configuration for all network and security devices for the Company's review.

5.3.2 For network and security devices managed by the Company, the Participating Service Provider shall work with the Company to ensure that the proposed system is compatible with the Company's security hardening guidelines for these devices.

5.3.3 The Participating Service Provider shall develop and maintain detailed security configurations of all network and security devices used within the proposed system that are managed by the Participating Service Provider.

5.3.4 The Participating Service Provider shall ensure that the latest security patches for the network and security devices are applied prior to system commissioning.

5.3.5 If the Participating Service Provider proposes wireless networks solutions, the Participating Service Provider shall ensure that firmware and software on all wireless infrastructures are kept updated, to ensure that security vulnerabilities are addressed.

5.4 Remote Administration by the Participating Service Provider

5.4.1 Remote administration access to network devices, servers or applications shall be disabled if it is not needed.

5.4.2 The Participating Service Provider shall leverage on the Company's remote access infrastructure if remote administration to server or applications is needed. Servers include all types of server and network devices, and applications include all types of application software, including Content Management Systems (CMS).

5.4.3 If remote administration is required, the Participating Service Provider shall implement the following IT security controls:

(a) Remote administration shall only be granted to authorized personnel;
(b) Remote server or application administration shall be performed from a Company-approved hardened device or through an approved jump host (i.e. a special-purpose computer on a network, such as a management LAN that provides a controlled and secured access to servers). Where possible, access filtering (i.e. the Participating Service Provider can consider implementing MAC address filtering as an additional layer of control) based on IP address shall be implemented to control the remote administration;
(c) All remote administration to servers shall be performed from within a management LAN (i.e. a dedicated network for administration purposes which is separate from the user traffic) meant only for administration;
(d) Personnel who are authorized to perform remote administration shall use 2FA to authenticate to the servers or applications; and
(e) Logging of the date, time, IP addresses of the source and destination systems, user information as well as the type of action performed shall be enabled on the servers that allow remote administrative access.

5.4.4 All requests by the Participating Service Provider for remote administration shall be

approved by the Company on a per request basis and the request shall be for emergency support only as and when required by the Company. No standing requests will be allowed.

6 APPLICATION SECURITY

6.1 Application Development

6.1.1 The Participating Service Provider shall conform to industry best practices on application secure coding such as the Open Web Application Security Project (OWASP) guidelines to prevent errors, loss, unauthorized modification or misuse of information in application, including but not limited to injection attacks, broken authentication and session management, cross site scripting, cross-site request forgery, insecure direct object references, security misconfiguration, etc.

6.1.2 If the system is deemed Mission Critical by the Company or if the system is internet-accessible, the Participating Service Provider shall carry out source code review before the proposed system is deployed and/or when there are major source code changes to the proposed system.

Source code review refers to a systematic examination of the computer program code to find and remove vulnerabilities. This applies to program codes or scripts that the Company has control over. Source code review can be carried out using manual (such as peer code review) or automated means (such as code scanner).

6.1.3 All findings rated as “Medium” and above from the source code review shall be remediated before the proposed system can be deployed for production use.

6.1.4 Secure coding practices shall be incorporated in the design, coding and implementation of turnkey applications including internet-facing ICT systems.

6.1.5 The Participating Service Provider shall ensure that the proposed system is designed and implemented with proper validation controls that address the vulnerabilities listed below. Checks shall be carried out to make sure that the following known vulnerabilities (without limitation) are handled correctly in the application system before it is deployed or when a major change is made:

(a) Non-validated input (i.e. input fields shall conform to the desired formats and values);
(b) Injection (such as SQL, NoSQL, OS and LDAP);
(c) Broken authentication;
(d) Sensitive data exposure (such as SHI and PII);
(e) XML external entities (XXE);
(f) Broken access control;
(g) Security misconfiguration;
(h) Cross-site scripting (XSS);
(i) Insecure deserialization;
(j) Using components with known vulnerabilities; and
(k) Insufficient logging and monitoring.

6.1.6 The Participating Service Provider shall ensure that the proposed system incorporates appropriate validation checks for all input fields with failures logged.

6.1.7 The Participating Service Provider shall make sure that the proposed system does not reveal to the users more information than needed (e.g. debug messages, stack trace,

system error messages) when a failure or error occurs.

6.1.8 The Participating Service Provider shall have a proven track record in secure software development methodology, and responsiveness to address vulnerabilities reported on its platform. The Participating Service Provider shall provide further information to support this.

6.1.9 The Participating Service Provider shall ensure that the output data is validated for correctness and appropriateness. This shall include, but not be limited to, the following:

(a) Checking for completeness via reconciliation controls; and
(b) Checking for correctness via sanity or sample checks.

6.2 Authentication and Access Control

6.2.1 The Participating Service Provider shall propose the Access Control Matrix (ACM) based on business and security requirements for access, covering:

(a) End user roles supported by the IT system;
(b) Authorization profiles that have been defined to support these roles; and
(c) End user provisioning and de-provisioning process.

The ACM shall be approved by the Company.

6.2.2 User access to applications, resources and data shall be assigned based on the following principles:

(a) “Need-to-know”: user is only granted access to the information needed to perform his/her tasks (different tasks/roles mean different need-to-know and hence, different access profile);
(b) “Principle of least privilege” (permissions that are required for the user to complete his/her task); and
(c) “Need-to-use”: user is only granted access to the resources (ICT equipment, applications, procedures, rooms) needed to perform his/her task/job/role.

An access control matrix defines the roles and the profiles supporting these roles for access to applications, network and security equipment, server, operating systems and databases.

6.2.3 The Participating Service Provider shall ensure that access controls are implemented in a fail-secure mode, which will not allow access to the proposed system when the authentication is not successfully completed.

6.2.4 The Participating Service Provider shall ensure that the automation of these account and access controls and procedures are implemented, where feasible.

6.2.5 All users and support personnel's access within the proposed system shall be granted as per the defined access control matrix using role-based access control to restrict users' access privileges.

6.2.6 The privileged access rights associated with components of each system (e.g. operating system, database management, middleware and application system) and the users to whom they need to be allocated, shall be identified and documented by the Participating Service Provider.

6.2.7 All users shall have a unique identifier (user ID) for their personal use so that activities can

be traced to the responsible individual.

6.2.8 The proposed system shall conform to the password standards stated in **Clause 2.2** above.

6.2.9 The Participating Service Provider shall protect authentication credentials and secret keys (cryptographic keys) that are used in scripts and applications such as automation scripts, mobile and web applications, using encryption and store inside secure protected storages. The Participating Service Provider shall use either secure protected storage methods that are recommended as best practices by the programming language/framework providers or runtime/hosting platforms, or use secure protected storage that are available in secret management tools.

When the use of secure protected storage is not possible, program codes used by the Participating Service Provider shall retrieve the authentication credentials and secret keys directly from the computer memory using means such as exporting credentials and secret keys to environment variables.

6.2.10 The proposed system shall integrate with the Company's provided 2FA services for users accessing the application over the Internet or from untrusted network.

6.2.11 The proposed system shall also implement an absolute time-out, regardless of session activity. This timeout defines the maximum amount of time a session can be active, closing and invalidating the session upon the defined absolute duration that is approved by the Company. After invalidating the session, the user is forced to re-authenticate again in the application and establish a new session.

6.2.12 The proposed system shall implement single user logon session to make sure that users cannot log on to multiple sessions at any given time using the same user credentials. Multiple logon sessions are allowed only if there is a business requirement by the Company.

6.2.13 The proposed system shall disallow multiple sessions from being launched concurrently from the same terminal either by the same user or by different users.

6.2.14 The proposed system shall re-validate the users before allowing them access to view sensitive patient/personal data. All access to sensitive patient/personal data shall be audited and logged.

6.2.15 The proposed system shall be designed to protect SHI and PII against unauthorized access via unattended terminals, through the following:

(a) Terminal screen timeouts; and/or
(b) Re-authentication challenges for user passwords, answers to secret questions, or any other similar mechanisms.

6.2.16 The proposed system shall not allow downloading of SHI and PII by end-users onto personal computer workstations, unless such function is deemed necessary and approved by the Company's approving authority.

6.2.17 The proposed system shall require end users to acknowledge the terms of use for access to the application as part of the user provisioning process, upon first login, or as and when there are changes to the terms of use.

6.2.18 The proposed system shall authenticate against the Microsoft Active Directory (AD) infrastructure managed by the Company to allow end-users to access the application using

their Microsoft AD credentials with the appropriate user rights assigned.

6.2.19 The proposed system shall allow the following THREE (3) groups of user administrator functions to be segregated, and shall not allow the user administrator to manage his/her own access:

(a) User administration: To create and delete user accounts;
(b) Authorization administration: To create roles, assigning the applicable functions / authorization to each role; and
(c) User maintenance: To assign the roles to user account (except for own account).

6.3 Web Services Security

6.3.1 The proposed system shall authenticate and authorize all web services requests. The Participating Service Provider shall provide and implement the Company's standard authentication and authorization of web services.

6.3.2 Application-to-application interfaces (such as APIs, web services, etc.) shall use cryptographic controls such as digital signatures to protect the authenticity and integrity of electronic information, where applicable.

6.4 Application Protection

6.4.1 The Participating Service Provider shall implement the proposed system based on a multi-tier architecture and make sure that the presentation logic, business logic and database accesses are separated by either physical or virtual network firewalls. At a minimum, the database access tier shall be separated from the other tiers, if the application software is unable to support the multi-tier architecture.

In a typical THREE-(3)-tier architecture, separation is achieved when a firewall is implemented to monitor all network traffics between the web and application tiers and similarly, a second firewall is implemented to monitor all network traffics between the application and database tiers.

6.4.2 The Participating Service Provider shall leverage on the Company's Web Application Firewall (WAF) to safeguard all internet-accessible systems, to secure the connection to untrusted external networks, such as connections with third parties and application level attacks such as, but not limited to:

(a) Code injection attacks (e.g. SQL injection, cross site scripting, cross-site request forgery);
(b) Field and parameter manipulation;
(c) Cookie and session exploit;
(d) SSL-based attacks;
(e) Brute force password attacks; and
(f) Layer 7 DoS/DDoS attacks.

6.4.3 The Participating Service Provider shall work with the Company to fine-tune the WAF to optimize its protection capabilities and minimize false positives on an on-going basis.

6.5 Use of Privileged Utility Programs

6.5.1 The Participating Service Provider shall ensure that the use of utility programs, that might be capable of overriding system and application controls, shall be controlled to prevent it

from being used for unauthorized purposes.

6.5.2 The Participating Service Provider shall seek the Company's approval for any installation cum usage of privileged utility programs, before it can be implemented.

6.5.3 The Participating Service Provider shall ensure that end-users do not have access to such utility programs.

7 AUDIT LOGGING AND MONITORING

7.1 Audit Trails and Logs

7.1.1 Security-relevant events shall be enabled and recorded in system logs and audit trails for all components within the proposed system (from applications, middleware, databases, down to operating system level, and all network and security devices). The following events shall minimally be recorded:

Log Source	Security-related Events
(a) Operating System	(i) System configuration changes; (ii) Security policy and configuration changes; (iii) System account and access rights creation and changes; (iv) Elevation of privilege; (v) Privileged account activities; (vi) Log on attempts; (vii) Network connection changes or failures; (viii) System start up and shutdown events; (ix) Service start up and shutdown events; and (x) Installation of new software and services.
(b) Database	(i) Database configuration changes; (ii) Database account and access rights creation and changes; (iii) Connection attempts to the database; (iv) Occurrence of errors; (v) Database schema modifications; (vi) Queries of database schemas; (vii) Queries for unexpected large dataset; (viii) Queries with multiple embedded queries; and (ix) Execution of operating system commands.
(c) Application	(i) Application configuration changes; (ii) Application security policy and configuration changes; (iii) Application account and access rights creation and changes; (iv) Successful and failed login attempts; (v) Occurrence of errors; (vi) Activities performed by the users (as determined through the Company's risk management process); and (vii) API calls invoked by users or other services.

7.1.2 The Participating Service Provider shall implement logging mechanisms to record events such as user activities, exceptions, faults and ICT security events for timely detection and

investigation of events that can lead to ICT security violations or incidents. The logs shall minimally record the following, where relevant:

(a) User IDs;
(b) Dates, times and details of key events, e.g. log-on and log-off;
(c) Terminal identity or network address or location;
(d) Records of successful and failed system access attempts;
(e) Records of successful and rejected data access attempts; and
(f) Activities carried out by privileged users, system/service accounts or administrators.

7.1.3 The Participating Service Provider shall ensure that the log format is accepted by the log monitoring system.

7.1.4 The Participating Service Provider shall ensure that all systems do not capture passwords in their logs and audit trails.

7.1.5 The Participating Service Provider shall ensure that the proposed system maintains the audit logs to facilitate playback of activities performed by specific user account on the proposed system over a specified time period.

7.1.6 The Participating Service Provider shall ensure that the proposed system maintains the audit logs to facilitate tracking of activities performed on specific patient/personnel records over a specified time period.

7.1.7 All logs shall be readable in ASCII plaintext or UTF-8. If the logs are not in ASCII plaintext or UTF-8 format, a tool shall be provided to convert the logs to the required format.

7.1.8 The proposed system shall retain all logs based on the following:

(a) Online – at least THREE (3) months; and
(b) Offline – all logs are to be stored offline for at least TWELVE (12) months.

If the proposed system does not leverage on the Company's virtualized environment, then the Participating Service Provider shall provide and implement the log retention housekeeping scripts and storage. For deployment within the Company, offline logs storage shall be handled by the Company. However, the Participating Service Provider shall provide an estimation on the storage required.

7.1.9 The Participating Service Provider shall ensure that the clocks of all systems and network devices within the proposed system are synchronized to a single reference time source.

7.1.10 The Participating Service Provider shall ensure that logs are protected against tampering and unauthorized access, are kept for a minimum of TWELVE (12) months, and are reviewed for timely detection and investigation of events that can lead to ICT security violations or incidents.

7.1.11 The Participating Service Provider shall ensure that the solution disallows removal or deletion of records related to patient/personnel and medication. For example, patient/personnel clinical notes will only be marked as 'deleted' when necessary, but the proposed system shall retain the record for audit trail purposes.

7.2 Audit Log Reporting

7.2.1 The proposed system shall provide the facility to generate exception reports on a periodic basis to facilitate detection of unauthorized activities and access, including the following:

(a) Unauthorized changes to patient/personnel data;
(b) Access to specific patient/personnel groups;
(c) Frequent access (access X patient/personnel records within Y minutes);
(d) Privileged admin access;
(e) Access during non-working hours or odd hours; and
(f) Users exceeding maximum login attempts allowed.

The scenarios and conditions for exception reporting shall be configurable by users as and when required.

7.2.2 The reports shall include adequate details to facilitate investigation, and this shall minimally include:

(a) User-ID;
(b) Date and time of event;
(c) Source IP address / location / terminal identity;
(d) Destination IP address / application / component; and
(e) Details of event, including the exact values before and after changes to provide the whole historical picture of any records or transactions.

7.2.3 The Participating Service Provider shall automate the generation of reports to maintain the integrity of the reports and to make sure that the generated reports are not tampered with.

7.2.4 The Participating Service Provider shall ensure that the proposed system provides the facility to allow extraction of audit logs sortable by user accounts, patient records, or specific key activities.

7.2.5 The proposed system shall have the facility to allow forwarding of user usage logs (such as login events, patient/personnel records accessed, etc.) to a security log analytics platform.

7.2.6 The Participating Service Provider shall provide to the Company, the list of audit reports including out-of-the-box from the product, and shall describe how the audit capabilities in the proposed system can help the Company to identify any potential misuse of the proposed system or suspicious activities.

7.3 Database Activity Monitoring (DAM)

7.3.1 If the proposed system is deemed as Critical Information Infrastructure (CII) and/or Mission-Critical with Restricted (Sensitive High) data by the Company, the Participating Service Provider shall work with the Company to leverage on the existing DAM solution to monitor and detect any unusual or unauthorized activities on the databases of the proposed system. High risk database activities shall be blocked where appropriate (for example, restricting database access only by approved applications).

7.4 Central Log Management

7.4.1 The Participating Service Provider shall leverage on the Company's central log management infrastructure for log retention and to facilitate investigations, where required.

7.4.2 The collection of logs may require the installation of a log-collecting software agent on the

proposed system. The Participating Service Provider shall work with the Company to integrate the software agent into the proposed system.

7.4.3 The Participating Service Provider shall transmit security-related events and logs generated from the proposed system (including those described in **Clause 7.1.1** above) in near real-time to the central log management infrastructure.

7.4.4 The Participating Service Provider shall adhere to the following stipulated retrieval timeframes for logs that are requested for incident investigation:

Logs Availability	Timeframe
Logs (up to THREE (3) months old)	Within ONE (1) day
Logs (more than THREE (3) months old)	Within FIVE (5) days

7.5 Security Monitoring

7.5.1 The Participating Service Provider shall work with the Company's appointed Security Operations Centre (SOC) Service Provider to have the proposed system monitored in near real-time 24x7x365, which is to subscribe to the Healthcare SOC monitoring services. This is to facilitate the prompt detection of anomalous activities, unless it is deemed by the Company to not be required for the proposed system.

7.5.2 The Participating Service Provider shall work with the Company's appointed SOC Service Provider on the installation of a log-collecting software agent in the proposed system or forward the required logs to the Company's appointed SOC Service Provider via syslog.

7.5.3 The Participating Service Provider shall transmit security-related events and logs generated from the proposed system in near real-time to the Company's appointed SOC Service Provider for monitoring purposes and overall situation awareness of the infrastructure. The type of logs to be transmitted shall minimally include the following:

(a) User log-on and log-off events (from applications, databases, operating systems);
(b) Unsuccessful log-on attempts (from applications, databases, operating systems);
(c) Security events generated by operating systems;
(d) Security events generated by security devices (such as firewalls, IPSes, WAF, anti-malware, etc.); and
(e) Any other logs that are deemed necessary.

7.5.4 The Participating Service Provider shall leverage on the internet website defacement-monitoring services provided by the Company's appointed SOC Service Provider to perform timely detection of defacement and recovery from the defacement. The types of defacement to be detected shall include, but not be limited to, the following:

(a) Website graffiti;
(b) Injection of custom website pages; and
(c) Injection of codes to the websites.

7.5.5 The Participating Service Provider shall investigate and address all security alerts and alarms raised by the Company's appointed SOC Service Provider on the proposed system, as well as all suspicious activities escalated to the Participating Service Provider. Such alerts and suspicious activities may include, but not be limited to, the following:

(a) Malware attacks;
(b) DoS/DDoS attacks;

(c) Web application attacks;
(d) Unauthorized access; and
(e) Password guessing attacks.

7.5.6 The Participating Service Provider shall work with the Company's appointed SOC Service Provider to support the fine-tuning of the 24x7 security monitoring services to improve its accuracy and minimize false positives on an on-going basis. This includes the creation, modification and customization of rule sets required for the fine-tuning.

8 SECURITY ASSESSMENT

8.1 Security Penetration Testing

8.1.1 If the proposed system is deemed Mission Critical by the Company or if the proposed system is internet-accessible, the Participating Service Provider shall engage an independent party that has no prior involvement in the development of the proposed system to perform security penetration testing. The test is to exploit any weaknesses to gain unauthorized access to the proposed system, prior to system commissioning. The scope for penetration testing shall include checks for weaknesses in servers and network infrastructure, custom code, components, products, and system configuration, as well as web application vulnerabilities including, but not limited to data injection attacks, cross site scripting, cross-site request forgery, broken authentication and session management, buffer overflow, broken access control, input parameter manipulation, logic flaw, insecure configuration, improper error handling, etc. The Participating Service Provider shall make sure that security patches, applicable to the proposed system, are kept up-to-date, prior to the commencement of the test.

8.1.2 The independent penetration tester engaged must be equipped with industry-recognized accreditations and certifications listed below, and must be approved by the Company:

(a) Penetration tester must have CREST accreditation to demonstrate assurance of its policies and procedures in penetration testing service, reporting and data handling, and due diligence in hiring of ethical penetration testers.
(b) Assessor(s) performing the penetration tests must possess at least ONE (1) of following:

(i) CREST penetration testing certification;
(ii) CREST Registered Penetration Tester;
(iii) CREST Certified Web Application Tester; or
(iv) CREST Certified Infrastructure Tester.

(c) The appointed penetration test service provider shall adopt the Company's Standard for Penetration Testing. This document will be shared with the Participating Service Provider during the system design phase.

8.1.3 The independent penetration tester shall provide the penetration test plan, including methodology and approach in carrying out the penetration testing, and this shall be agreed with the Company.

8.1.4 The independent penetration tester engaged by the Participating Service Provider shall perform re-testing to verify that the weaknesses and defects have been rectified, before system commissioning. Regression testing of the affected functionalities, where applicable, shall also be performed after the weaknesses and defects have been rectified.

8.1.5 The Participating Service Provider shall remediate all findings rated as Medium and above before the proposed system is deployed for production use. For the remaining findings, the Participating Service Provider must provide mitigating measures on handling the vulnerabilities, risk impact assessment and the expected timeline to make the necessary correction(s) to resolve the defects. All remediations as recommended by the independent penetration tester shall be carried out at no additional cost to the Company.

8.1.6 The Participating Service Provider shall submit a report to the Company on the results of the penetration testing performed, the recommendations and actions taken, including:

(a) A summary of the test plan;
(b) An executive summary presenting the results in a business risk context;
(c) Highlighting particular concerns, any patterns, and a high-level statement of the required form of the corrective action;
(d) A quantitative summary on the number of vulnerabilities uncovered at the various criticality and risk levels;
(e) A findings table comprising technical content describing:

(i) Vulnerabilities found;
(ii) Risk rating (e.g. High, Medium or Low) for each vulnerability identified;
(iii) Mitigations put in place; and
(iv) Remediation steps;

(f) A test narrative describing process that the tester used to achieve particular results, so that the results can be reproduced;
(g) The set of test evidence as an appendix. The evidence shall include results of automated testing tools, screen shots of successful exploits, etc.;
(h) Providing recommendations to the vulnerabilities identified and assisting in understanding the vulnerabilities and recommendations; and
(i) Performing follow-up testing to verify the mitigation controls implemented.

8.1.7 The Company reserves the right to engage the service of an independent penetration tester to conduct similar security testing on the proposed system on periodic basis. The Participating Service Provider shall provide necessary support, including addressing any vulnerabilities found, at no additional cost to the Company.

8.2 Vulnerability Scanning

8.2.1 The Participating Service Provider shall ensure that all ICT infrastructure (including servers, databases, virtual machines (VM), network equipment and appliances) used in the support of the systems is securely configured and hardened, including:

(a) Disabling or removing of unused accounts (including test, sample, guest and default accounts;
(b) Disabling or removing of unused ports, services and components;
(c) Changing of all default passwords; and
(d) Configuring service accounts as non-interactive.

8.2.2 The Participating Service Provider shall ensure that software, hardware and Service Provider tools that have not reached end-of-support (EOS, which refers to a situation in which a product Service Provider no longer provides support to the product, including no further security updates or bug fixes for its product) are deployed.

8.2.3 The Participating Service Provider shall work closely with the Company to perform

vulnerability scanning of all systems. The application software, operating system and network infrastructure shall be scanned according to the frequency shown below:

Component	Frequency
ICT Systems "Go Live"	Prior to "Go Live"
Application Software	Annually
Operating System	Quarterly
Network	Quarterly

8.2.4 The Participating Service Provider shall also work closely with the Company to perform vulnerability scanning of the affected systems prior to subsequent commissioning of new servers.

8.2.5 The Participating Service Provider shall ensure all security vulnerabilities related to the application (from the vulnerability scanning) are remediated before system commissioning, and the remediation are tested before deploying to production environment. All security vulnerabilities rated as "Critical" shall be remediated within TWO (2) weeks.

Severity Level	Period to Close
High (Critical/XSS)	TWO (2) weeks
Medium (Severe)	ONE (1) month
Low (Moderate)	TWO (2) months

8.2.6 The Participating Service Provider shall submit a report to the Company on the results of the vulnerability scanning related to the application, the proposed remediation, and the remediation implemented.

8.2.7 The Participating Service Provider shall establish a vulnerability and security patch management process to ensure thorough tracking of security vulnerabilities for the proposed system.

8.3 System Security Acceptance Test (SSAT)

8.3.1 The Participating Service Provider shall ensure that SSAT is carried out on all systems, including mobile applications, to make sure that the security measures are functioning as intended.

SSAT is a type of acceptance test specifically for checking IT security controls, and to validate that the technical security controls implemented in a system are working properly according to requirements and design. Examples of technical security controls typically covered in SSAT include authentication, anti-malware, logging, etc. There could be more technical security controls in the system that are used but not listed here, and assistance from the deployment contractor / Service Provider shall be sought to identify those technical security controls, as well as to recommend test cases for validating them. SSAT may also include checking correctness of security configurations of all servers, devices, operating systems and applications, etc. in the system, if this is not covered by other tests.

8.3.2 The Participating Service Provider shall include SSAT in the proposed system test plan. The test plan shall be reviewed and approved by the Company's project team.

8.3.3 The Participating Service Provider shall develop relevant SSAT test case in the proposed system. The test case shall be reviewed and approved by the Company's security team.

8.3.4 The Participating Service Provider shall resolve all SSAT issues before the proposed

system goes through vulnerability assessment or penetration testing.

8.4 Security Review and Audit

8.4.1 The Company reserves the right to audit on the outsourced services as well as its supporting systems and processes that are managed by the Participating Service Provider and sub-contractors, whenever the need arises. The Participating Service Provider and its sub-contractors shall give full support to the Company and the auditors engaged throughout the audit.

8.4.2 The Participating Service Provider shall work with the Company, and any other parties identified by the Company, to implement the audit recommendations not later than SIX (6) months after the Company's approval of the audit report. The Participating Service Provider shall conduct a follow-up audit on any reported non-compliance within TWO (2) months upon completion of the implementation of the recommendations.

8.4.3 The Participating Service Provider shall also assist the Company's risk assessment team to conduct security review of the proposed system's application and network architecture, including the network design, as well as system and network interconnections, on an annual basis to identify potential security weaknesses. The issues identified from the security review must be tracked and addressed in a timely manner by the Participating Service Provider.

9 SECURITY OPERATIONS

9.1 Security Patch Management

9.1.1 The Participating Service Provider shall implement and operate the necessary infrastructure and processes to make sure all components in the proposed system (including all hardware [e.g. servers, workstations, laptops, network devices, security devices] and software [e.g. database, middleware, web applications]) are updated with the latest security patches. The scope shall cover all environments in the proposed system, including development, test, DR and production.

9.1.2 The Participating Service Provider shall implement security patches according to the timeframe shown below:

Type of Asset	Type of System	Type of Patch	Deployment upon Availability of Patch
All	All	Emergency*	As soon as possible, subject to urgent allocation of resources
Asset Type A Includes higher risk assets that have broad attack surface or high cyber risk impact	1. Internet-accessible ICT systems (includeing internet-facing infrastructure, servers, software) in the Internet Zone	Critical** / High	ONE (1) month
		Medium / Low	TWO (2) months
	2. CII Systems	Critical** / High	TWO (2) months
		Medium / Low	THREE (3) months

Type of Asset	Type of System	Type of Patch	Deployment upon Availability of Patch
	3. Internal infrastructure systems on the intranet (e.g. core switch, core firewall, hypervisor)	All**	TWELVE (12) months
Asset Type B Intranet ICT application systems	1. ICT systems using Windows platforms (including End User Computing (EUC))	All**	THREE (3) months. For Windows EUC, co-existence testing is required before deployment
	2. ICT systems using non-Windows platforms	All**	SIX (6) months
	3. ICT systems that support medical systems that require medical regulator certification	All	THREE (3) months
For Commercial off-the-shelf (COTS) in Asset Type A and Asset Type B, COTS Service Providers and/or Product Principal shall provide the certification that the security patch will not impact the efficacy of the ICT systems within three (3) months from the date of patch availability. For ICT systems that support medical systems that require medical regular certification, patch shall be applied three (3) months from date of certification by Product Principal.			
* Emergency patch will be directed by Cyber Security Agency (CSA), Ministry of Health (MOH). In addition, as directed by Cyber Defence Group (CDG) following Code Red assessment.			
**The timeline for patching may be shortened based on urgency of the patch. This will be at the direction of CSA, MOH or CDG. If the patch is assessed with high cyber risk impact (e.g., vulnerabilities that are known to be targeted by adversaries), it will be escalated as an Emergency patch.			

The systems include software, servers, network and security equipment. If a Business Critical or Standard system is internet-accessible, the stipulated timeframe for internet-accessible system shall apply.

9.1.3 During the period of Heightened Security Threat made known by the Company, security patches shall be deployed as below:

Type of Patch	Implementation Timeline (Inclusive of Testing)	Reporting Timeframe
Emergency	Within TWELVE (12) hours	Immediate
Critical	Within ONE (1) day	

9.1.4 The Participating Service Provider shall ensure that quarterly patch status reports are submitted to the Company for management oversight and reporting.

9.1.5 For servers managed by the Company, the Participating Service Provider shall work with the Company to ensure timely updates of the security patches on the operating systems of the servers. The Participating Service Provider shall be responsible to patch any components above the operating systems on these servers.

9.1.6 The Participating Service Provider shall assess the applicability of a security patch to the

environment of the proposed system. This shall include:

(a) Proactively monitoring for new security patch releases;
(b) Review of advisories from the Company as and when it is made available; and
(c) Review of the new security patch to determine and classify the applicability to the environment of the proposed system.

9.1.7 The Participating Service Provider shall test the security patches prior to deploying to the production environment.

9.1.8 The Participating Service Provider shall maintain an up-to-date inventory of the hardware and software deployed in the proposed system to facilitate the rollout of applicable security patches to affected systems. This inventory shall be made available to the Company.

9.2 Security Incident Management

9.2.1 The Participating Service Provider shall develop, implement and maintain the security incident handling and response plan to facilitate decision making when a security incident affecting the proposed system occurs. The security incident handling and response plan shall align with the Cybersecurity Incident Response Framework for Healthcare (CIRF) which defines a systematic incident response approach and the incident escalation structure, incident categories, reporting timeline, reporting mechanism and format, through which incidents are to be notified and resolved. A copy of the CIRF will be made available to the successful Participating Service Provider upon award.

9.2.2 The security incident handling and response plan shall minimally contain the following:

(a) Detection phase

(i) Incident triage and analysis process; and
(ii) Incident notification process;

(b) Containment, Eradication and Recovery

(i) Containment strategies;
(ii) Evidence gathering and handling process; and
(iii) Eradication and recovery process;

(c) Post-Incident Review phase

(i) Root-cause analysis;
(ii) Impact analysis; and
(iii) Corrective measures to prevent recurrence; and

(d) Communication process and protocol with relevant external stakeholders supporting the incident management process (e.g. media, third party service providers, law enforcement agencies, etc.).

9.2.3 In the event of any computer security incidents, the Participating Service Provider's responsibilities shall include:

(a) Investigating, resolving and recovering from security incidents;
(b) Ensuring the preservation and admissibility of evidence by protecting and documenting all access to incident information; and

(c) Exercising the prescribed incident response guidelines and procedures of the security incident handling and response plan and CIRF.

9.2.4 The Participating Service Provider shall ensure that all its personnel are briefed on the incident reporting procedures. Furthermore, the Participating Service Provider shall provide its staff and sub-contractors with procedures for reporting security incidents.

9.2.5 All security incidents, including malware infections, defacements, server intrusions, any unauthorized access and modifications, shall be reported directly to operation support teams. The operation support teams shall take the necessary actions to ensure that all security incidents are properly handled and managed. The Participating Service Provider shall also implement preventive measures to thwart the recurrence of security incidents. The Participating Service Provider and its operation support teams shall also work closely and give full cooperation to the Company in resolving the security incidents when the need arises.

9.2.6 The Participating Service Provider shall inform the Company and personnel appointed by the Company of all security incidents affecting the confidentiality, integrity and availability of the Company's data within ONE (1) hour following initial detection of the incident.

9.2.7 The Participating Service Provider shall keep the Company and personnel appointed by the Company (Detect Respond Recover (DRR) Team and Group/Chief Information Security Officer (G/CISO)) informed, before any ICT security incident information is released through the public communication channels (the public channels include newspaper media (such as Straits Times), radio broadcasts, social media platforms (such as Facebook, Twitter)).

9.2.8 Forensics

(a) The Participating Service Provider shall perform root cause analysis on compromised and/or suspected systems. The Company, however, reserves the right to undertake parallel investigations or take over any ongoing investigations that it deems as critical.
(b) The Participating Service Provider shall have personnel who are trained in basic forensic investigation to undertake the root cause analysis. The Participating Service Provider shall state the forensic certificates that these personnel possess, if any. These personnel are required to have at least THREE (3) years of experience in performing forensic and investigation.
(c) The Participating Service Provider shall ensure that tools used in the root cause analysis are able to preserve evidence for admission in court.

9.2.9 Reporting

(a) The Participating Service Provider shall provide status updates on the incident until closure based on the schedule indicated in the CIRF.
(b) A detailed investigation report for each security incident shall be generated and be made available to the Company based on the schedule indicated in the CIRF.

9.3 Information and Communication Technology (ICT) Disaster Recovery Management

9.3.1 The Participating Service Provider shall ensure that the Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) are defined if the proposed system is deemed as Mission Critical by the Company.

9.3.2 The Participating Service Provider shall develop Disaster Recovery Plans (DRPs) for the proposed system if the proposed system is deemed as Mission Critical by the Company. DRP shall achieve the target RTOs and RPOs, and shall be endorsed by the Company.

9.3.3 All DRPs developed shall clearly describe the following:

(a) Identification and descriptions of key failure scenarios and their respective RTO and RPO;
(b) Estimation of the service disruption "downtime" and the loss in data;
(c) RTO and its starting point for which services are to be restored and data recovered;
(d) The DR strategy;
(e) The composition, roles and responsibilities, and contact numbers of the DR team;
(f) Escalation and communications procedures with updated contact information;
(g) Detailed procedures to be used during a disaster; and
(h) Restoration procedures to restore system operations back to normal.

9.3.4 The Participating Service Provider shall ensure that all DRPs are documented and reviewed, at least once a year.

9.3.5 The Participating Service Provider shall ensure that tests of DRPs are carried out annually, if the proposed system is deemed as Mission Critical system.

9.3.6 The Participating Service Provider shall ensure that the DRPs are updated to address gaps identified during the DRP exercises.

9.3.7 The Participating Service Provider shall ensure that the results of DRP tests are documented and kept to facilitate audit reviews.

9.4 Systems Change Management

9.4.1 The Participating Service Provider shall align to the Company's change management process to ensure that changes to the production system, including hardware, software and firmware, are evaluated, properly tested and implemented, to minimize the risk of data corruption, unauthorized activities and unplanned outages.

9.4.2 The Participating Service Provider shall ensure that all changes to production systems are documented, reviewed and authorized, to ensure a proper record of all production system changes.

9.4.3 The Participating Service Provider shall only be able to access the development and testing environment.

9.4.4 Conflicting duties and areas of responsibility shall be segregated to prevent a conflict of interest, collusion or fraud as no single person can access, modify or use assets without authorisation or detection. Examples of segregation of duties include:

(a) Software developers shall not be assigned software migration and promotion permissions;
(b) The release manager shall not have access to modify source codes;
(c) The server system administrators and the database administrator role shall not be assigned to the same person;
(d) Application administrator or privileged accounts (with ICT functions) shall not be assigned with operational access rights;
(e) Personnel that reviews the audit logs or activities shall be independent (i.e. not

involved in the same activities being reviewed); and

(f) Administrators and users shall not have access to modify audit trails of their activities in application/database/servers.

When segregation of duties is not feasible or practical, risk mitigation measures such as monitoring of activities, audit trails and management supervision, shall be implemented.

9.5 Use of Authorized Software

9.5.1 The Participating Service Provider shall manage the acquisition, installation (including vulnerability patching and version upgrades) and use of authorised software that are legally acquired and complies with licensing agreements, and implement processes to remove unauthorised software.

9.5.2 The Participating Service Provider shall ensure that authorized software on the Company-issued end-user computing devices is not removed or tampered with, and personal software is not installed.

9.6 Backup

9.6.1 A data backup and recovery plan shall be implemented for systems based on each system's Recovery Time Objective and Recovery Point Objective that will, at the very least, include the following areas.

(a) Frequency of backup (daily, weekly, monthly, yearly);
(b) Type of backup (full, incremental, differential);
(c) Archival (including data retention requirement) and storage facility;
(d) Testing and restoration requirements; and
(e) Disposal requirements, as shown in Media Sanitization (refer to **Clause 3.3** above).

9.7 Technology Refresh Management

9.7.1 The Participating Service Provider shall develop a technology refresh plan for the replacement of hardware and software in a timely manner, before they reach EOS. Security shall be an important consideration when determining if and when the hardware and software are to be upgraded, and how such upgrades are prioritized.

Software refers both to systems software and application software. Systems software includes the programs that are dedicated to managing the computer itself, such as the operating system. Application software includes programs that are used to complete tasks, such as creating documents, spreadsheets, and publications, doing online research, sending email, etc.

9.7.2 The plan shall cover the following:

(a) Maintenance of a Company-level software inventory;
(b) Planning process for upgrades;
(c) Identification of upgrades significant to security;
(d) Risk assessment and prioritization; and
(e) Upgrade timelines.

9.8 Account, Access Rights and Activities Review

9.8.1 The Participating Service Provider shall ensure that regular reviews of accounts (including privileged accounts) and the associated access rights in the systems are conducted as per the table below, including those given to external parties, to confirm that they are valid and to make sure that all unused or obsolete accounts and accesses are removed in a timely manner. Old, unused or obsolete accounts and/accesses shall be deleted from the systems within FIVE (5) working days from completion of the review. However, if the accounts need to be retained (such as for tracing accountability or for maintaining postings in collaborative platforms, and so on), then at a minimum, the access rights of these accounts shall be deleted from the affected systems.

Type	Review Frequency
All accounts in Mission Critical systems	Half-yearly
All accounts in Business Critical and Standard systems	Annually
List of inactive/suspended accounts	Quarterly

Accounts (except for accounts used in Digital Services by members of the public) shall be suspended when they have not been used for the past NINETY (90) days.

9.8.2 The review procedures implemented shall cover the following scenarios:

(a) Staff resignation/ retirement;
(b) Termination;
(c) Role change;
(d) Extended leave; and
(e) External party user resignation/redeployment.

9.8.3 The access rights of all employees and external party users shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

9.8.4 The Participating Service Provider shall conduct monthly review of privileged user and administrator activities (e.g. system administrator, database administrator, application administrator, etc.) within the proposed system to detect misuse and to ensure that all activities are proper and accounted for.

9.8.5 The Participating Service Provider shall automate the generation of the reports used for the reviews as described in this **Clause 9** to maintain the integrity of the reports and to make sure that the generated reports are not tampered with.

9.8.6 The Participating Service Provider shall make sure that ownership of all accounts in the proposed system, including default and services accounts, are clearly defined.

9.8.7 The Participating Service Provider shall work with the Company to conduct an annual review of the firewall rules pertaining to the proposed system to remove redundant rules, resolve conflicting rules and to tighten broadly defined rules. The review shall minimally include the following:

(a) Detailed examination of all changes since the last review, particularly on the person who made the changes and under what circumstances; and
(b) The reviewer role shall be held by someone with no administrative or privileged access to the firewall and have good firewall and networking knowledge, or review shall be conducted by a peer-administrator who is different from the person who made the changes.

9.9 Security Reporting

9.9.1 The Participating Service Provider shall submit a monthly security report to the Company. The security report shall include a summary of all security-related activities that have taken place during the reporting period, including:

(a) Security incident reported;
(b) Findings on security assessment conducted;
(c) Outcome of security reviews conducted;
(d) Recommendations on new controls to resolve security incidents or to improve security;
(e) Implementation status of security controls in the proposed system;
(f) SLA for security incident management; and
(g) SLA for patch deployment.

9.10 Inventory of ICT Assets

9.10.1 The Participating Service Provider shall maintain and update the IT asset (IT asset includes hardware, software (including operating system), storage equipment, network equipment and network attached equipment such as printers) inventory related to the proposed system, at least annually, or when there are changes to the IT assets. The inventory shall capture all IT assets owned, leases, and developed by the Company and the Participating Service Provider tools that are connected to the Company's networks.

9.10.2 The ICT asset inventory shall minimally include the following information:

(a) Name/description of each asset;
(b) Main functions of each asset;
(c) Owner and/or operator of each asset;
(d) Physical location of each asset;
(e) System dependencies on internal and/or external ICT systems/networks; and
(f) Network perimeter and all external ICT systems which each asset interfaces.

9.11 Disciplinary Process

9.11.1 The Participating Service Provider shall ensure that a disciplinary process has been established to take action against employees who have committed an IT security violation.

9.12 Termination and Change of Employment

9.12.1 IT security obligations that remain valid after termination or change of employment shall be defined and communicated to the Company.