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 hosted on public cloud Software-As-A-Service (SaaS)**.

PART 1
MOHH IT SECURITY REQUIREMENTS: SYSTEMS INSTALLED ON SAAS

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 have certifications from the mandatory certification list below:

(a) Mandatory Certifications:

(i) SOC 2 Type 2 / SOC 3
(ii) ISO 27001;
(iii) ISO 27017; and
(iv) ISO 27018
(v) ITIL

(b) In the absence of SOC 2 Type 2 report, the Participating Service Provider shall provide any of the following certication as an acceptable alternative third party audit requirement:

(i) Health Information Trust Alliance (HITRUST);
(ii) Cloud Security Alliance (CSA)'s Security, Trust, Assurance and Risk Registry (STAR) – Level 2;
(iii) Outsourced Service Provider's Audit Report (OSPAR) or other audits based on the principles of ISCA SSAE 3402;
(iv) All of the following THREE (3) ISO certifications: 27001, 27017, 27018

1.1.3 The Participating Service Provider shall submit evidence of certifications from the list(s) in **Clause 1.1.2** above together with its Proposal.

1.1.4 The Participating Service Provider shall submit the SSAE 18 Service Organisation Control (SOC) 3 report together with its Proposal.

1.1.5 The Participating Service Provider shall share with the Company about the various security measures/controls in protecting the Company's data residing in the proposed system.

1.1.6 The Participating Service Provider shall provide the cloud shared responsibility framework that defines the security obligations for the proposed SAAS platform between cloud service provider, system integrator and the Company in its Proposal.

1.1.7 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.

1.1.8 The Participating Service Provider shall protect and ensure the confidentiality, integrity or availability of the Company's 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.

1.1.9 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.

1.1.10 The Participating Service Provider shall comply with the prevailing laws and regulations such as:

(a) Personal Data Protection Act (PDPA);
(b) Computer Misuse and CyberSecurity Act (Singapore);
(c) Cybersecurity Act (Singapore);
(d) Evidence Act (Singapore);
(e) Electronic Transactions Act (ETA) (Singapore);
(f) Private Hospitals and Medical Clinics Act (PHMCA), if health information is involved;
(g) Healthcare Services Bill (HCS Bill), if health information is involved; and
(h) Other MOH guidelines on the handling of retention of medical records, if health information is involved.

Please refer to References and Attorney-General's Chambers (AGC) Singapore Statutes Online site for further details.

1.1.11 The Participating Service Provider shall notify the Company in advance of any updates in the policies or the systems and services that will or may affect the Company's data.

1.1.12 The Participating Service Provider shall keep abreast of relevant Singapore legal, regulatory, contractual and industry standard, and ensure that its operations remain compliant with applicable laws and regulations. The Participating Service Provider shall ensure that the proposed system and its security measures are up-to-date with evolving industry standards and as new technologies emerge.

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) System architecture diagram;
(b) Network architecture diagram;
(c) Application architecture diagram; and
(d) Data flow diagram.

1.3 Security Personnel

1.3.1 The Participating Service Provider shall be responsible for the following:

(a) Ensuring that data breaches related to the Company are immediately reported to the Company;
(b) Maintaining records of all data breaches; and
(c) Ensuring that action is taken to investigate, minimize damage and prevent recurrence.

2 SECURITY STANDARDS

2.1 Cryptography 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 provide 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;
(e) Ensuring that when an IT system is decommissioned and data is no longer required, keys used shall be securely destroyed; and
(f) Providing a Hardware Security Module (HSM) for the protection of the crypto key lifecycle, by managing, processing and storing cryptographic keys inside a hardened, tamper-resistant device.

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.

2.2.3 The Participating Service Provider shall provide a web portal to provide account activation and password reset functions.

2.2.4 The Participating Service Provider shall provide Single-Sign On, wherever possible.

3 DATA SECURITY

3.1 Information Handling by the Participating Service Provider

3.1.1 The ownership of the data generated upon usage of the proposed system, at any point of time during the term of the relevant agreement or expiry or termination of the relevant agreement, shall rest absolutely with the Company.

3.1.2 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.

3.1.3 The Participating Service Provider and its sub-contractors shall protect the Company against unauthorized disclosures of restricted information accessed by the personnel in the course of the relevant agreement.

3.1.4 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 subcontractors 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.

3.1.5 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.

3.1.6 When requested by the Company, the Participating Service Provider shall provide a detailed description of the control measures.

3.1.7 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.

3.1.8 The Participating Service Provider shall protect the Company's digital assets such as documents with security measures such as encryption, Access Control List (ACL) and usage rights policy.

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 segregate and protect the Company's data from the Participating Service Provider's other customer's data in a multi-tenancy environment. These measures include, but shall not be limited to: tenant isolation, transparency/audit-ability of administrative access, controlled change management, multi-tenancy architecture and data encryption.

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

3.2.5 The Participating Service Provider shall ensure that the Company's data cannot be replicated out of Singapore and system resiliency shall only be within Singapore.

3.2.6 The Participating Service Provider shall provide a solution to prevent and detect data breaches or exfiltration of restricted data owned by the Company.

3.2.7 The Participating Service Provider shall ensure that restricted data sent over the network are in encrypted format as defined in **Clause 2.1.2** above (such as using SSL/TLS, IPsec or SSH).

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

3.2.9 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.

3.2.10 The Participating Service Provider shall propose encryption 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 provide the security measures upon approval by the Company and provide evidence of implementation of such security measures.

3.2.11 The proposed system shall have the capability to allow the Company to define different personnel groups (such as VVIP, VIP, CIP), to tag personnel under one or more of the groups defined, and to restrict access to personnel group to selected user groups, including in reports, memos and referrals.

3.2.12 The proposed system shall have the capability to allow the Company to define sensitive patient/personal data type (such as personal data, for example salary, performance rating, etc.), and to restrict access to each data type to selected user groups, including in reports, memos and referrals.

3.2.13 The Participating Service Provider shall ensure that restricted data (such as personal data) are masked or obfuscated, where applicable, when printed on hardcopy reports or sent electronically as email or using other communications systems.

3.2.14 The Participating Service Provider shall describe how the proposed system will ensure that patient/personal data and any personally identifiable data is protected from security risks for any service that the proposed system provides through the internet.

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

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

3.2.17 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.

3.2.18 The Participating Service Provider shall promptly inform the Company of any requests on accessing the Company's data warranted by law enforcements or in the form of subpoena or a court order.

3.3 Data Handling

3.3.1 The Participating Service Provider shall ensure that data that is placed in archive is protected according to its classification and follows the prevailing laws and regulations stated in **Clause 1.1.10** above.

3.3.2 The following sanitisation method shall be used to minimise the possibility of recovering any data from storage media:

(a) Crypto-Shredding

Sanitize the encryption key used to encrypt the target data. The crypto-shredding option may only be used if the following is practised:

(i) The strength of the encryption key complies with the following cryptography standards:

(1) RSA public key encryption with key sizes of at least 2048 bits. (Asymmetric);
(2) Elliptic curve cryptography standard with key sizes of at least 384 bits. (Asymmetric); and
(3) Advanced Encryption Standard (AES) with key sizes of at least 256 bits. (Symmetric).

3.3.3 The Participating Service Provider shall provide a certificate of data sanitization in relation to **Clause 3.3.2** above, upon completion of data sanitization.

3.4 **Physical Media Transfer**

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

3.5 Data Loss Prevention

3.5.1 The Participating Service Provider shall ensure that the use of encryption and anonymization methods to secure PII is provided, where feasible, to reduce the risk of unauthorized data loss and data being re-identified.

3.5.2 The Participating Service Provider shall employ a multi-layer data loss protection architecture in case of failure. All data shall be replicated in real-time to standby servers in a secondary data centre, providing at least n+1 redundancy within Singapore. Critical data shall be replicated on-premises to provide n+2 redundancy and to allow for immediate and transparent recovery, with no data loss in case of a hardware failure.

4 SYSTEMS SECURITY

4.1 Authentication and Access Control

4.1.1 The Participating Service Provider shall provide a Single Sign-On (SSO) service to centrally manage multiple accounts and business applications.

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 If the Company's AD ID is proposed to perform authentication, the Participating Service Provider shall ensure that an approved authentication service (e.g. Azure AD, AWS directory service) is used to login to the proposed system.

4.1.4 All access to servers, infrastructure and database systems shall be done through a secure channel (such as SSH) via the Participating Service Provider's Privileged Identity Management (PIM). All access shall be logged to facilitate independent reviews of the access and transactions completed.

4.1.5 The Participating Service Provider shall employ a 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 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 The Participating Service Provider shall provide 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.

4.1.10 The Participating Service Provider shall disable all accounts belonging to users found to pose a significant risk to the proposed system within TWO (2) hours of discovery of the risk of any compromised account.

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 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. The service account password needs to be reset annually; and
(e) Disabling autorun, etc.

4.3 Protection Against Malicious Code

4.3.1 The Participating Service Provider shall ensure that its SaaS platform is protected against advanced malware through heuristics detection/machine learning/artificial intelligence.

5 NETWORK SECURITY

5.1 Network Segmentation

5.1.1 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 provide measures to protect against Denial-of-Service (DoS) attacks.

5.2.2 The Participating Service Provider shall have in-place measures to mitigate DNS tunneling and DNS-spoofing attacks.

5.2.3 The Participating Service Provider shall ensure that encryption is used to protect

confidentiality of data in the inter-connections of networks across the internet, and virtual private networks (VPNs).

5.2.4 The proposed system shall support geo-location restrictions if access to the proposed system from outside of Singapore is not allowed.

5.3 Remote Administration by the Participating Service Provider

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

(a) Remote administration shall only be granted to the Company's authorised personnel;
(b) Personnel who are authorized to perform remote administration shall use 2FA to authenticate to the servers or applications; and
(c) 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.

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 applications, 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 The Participating Service Provider shall ensure that the proposed system is designed and provided 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 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.

6.1.3 The Participating Service Provider shall make sure that all input fields are validated at server-side and their failures are logged.

Note: Input fields validation refers to the input validation checks carried out by the

application system upon the submission of inputs by the users. Logging of input validation failure is a form of anomaly logging, from which the captured logs will be useful for investigation when an unauthorized access take place through the input fields.

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

6.1.5 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.

6.1.6 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.

6.1.7 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 proposed 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 users 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.

6.2.3 The Participating Service Provider shall ensure that the appropriate access rights are accorded to data throughout its life cycle. This must apply to the various stages of the data lifecycle from creation, usage, transfer, sharing, storage to disposal.

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

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

6.2.6 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.

6.2.7 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 proposed system shall be able to support 2FA services for users accessing the application.

6.2.10 The proposed system shall provide automatic time-out for sessions that are inactive for a specific period of time (THIRTY (30) minutes).

6.2.11 The proposed system shall provide 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.

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

6.2.13 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.

6.2.14 The proposed system shall allow the following THREE (3) groups of user administrator functions to be segregated, and shall not allow user administrators to manage their 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 provide 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.

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

6.4.2 The Participating Service Provider shall provide security measures such as Web Application Firewall (WAF) and/or IDS to protect the proposed system against 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 ensure that the WAF optimizes its protection capabilities and minimizes false positives on an on-going basis.

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. The following events shall minimally be recorded:

(a) All successful and unsuccessful login attempts;
(b) All successful and failed access to patient/personnel records;
(c) All successful and failed access to personally identifiable data;
(d) All successful and failed access to sensitive/restricted data;
(e) Changes to all records;
(f) Changes to all system configurations; and
(g) All privileged users, administration, and account management activities.

7.1.2 The Participating Service Provider shall provide logging mechanisms to record events such as user activities, exceptions and security events for timely detection and investigation of events that can lead to security violations or incidents. The logs shall minimally record the following, where relevant:

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

7.1.3 The Participating Service Provider shall ensure that the proposed system does not capture passwords in its logs and audit trails.

7.1.4 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.

7.1.5 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.

7.1.6 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.

7.1.7 The Participating Service Provider shall ensure that the clocks of the proposed system are synchronized to a single reference time source.

7.1.8 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 data breach.

7.1.9 The proposed system shall provide cryptographic mechanisms to protect the integrity of the audit log or record.

7.1.10 The Participating Service Provider shall provide an alternate audit capability in the event of a failure in primary audit capability that provides security-related audit information.

7.2 Audit Log Reporting

7.2.1 The Participating Service Provider shall work with the Company and provide a secure approach of importing application logs into the Company's Security Information and Event Management (SIEM) system to enable a real-time analysis of security alerts.

7.2.2 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.

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

7.2.4 The Participating Service Provider shall provide the Company with 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

7.3.1 The Participating Service Provider shall propose a monitoring service to monitor the following database security-related events if the proposed system stores and/or processes Restricted (Sensitive High) data.

(a) Administration of database tables and records;
(b) Abnormal queries and/or commands such as unexpected queries for schema related information, creation or deletion of tables;
(c) Queries and extraction of large volume of data records;
(d) Queries and/or extraction of Protected Patient Records (PPRs) i.e. VVIP medical records; and
(e) Query errors.

7.4 Security Monitoring

7.4.1 The Participating Service Provider shall work with the Company's appointed Security Operations Centre (SOC) Service Provider to have the proposed system monitored in real-time 24x7. This is to facilitate the prompt detection of anomalous activities, unless the Company deems that it is not required for the proposed system.

7.4.2 The Participating Service Provider shall ensure that the logs can be forwarded to the security monitoring service via syslog or API.

7.4.3 The Participating Service Provider shall provide their website defacement-monitoring services 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.

7.4.4 The Participating Service Provider shall perform the security monitoring for proposed system in real-time 24x7. They shall investigate and address all security alerts and alarms raised by the security monitoring service 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.

7.4.5 The Participating Service Provider shall fine-tune 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 fine-tuning.

7.4.6 The Participating Service Provider shall test the capability of the incidence response to determine its effectiveness, at least once a year and the process and results shall be documented.

7.5 Application Performance Monitoring

7.5.1 The Participating Service Provider shall provide a Cloud Application Performance Management (CAPM) to provide monitoring resources to continuously observe a system in action, tracking availability, functionality and responsiveness.

8 SECURITY ASSESSMENTS

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 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 shallinclude 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 provide a Vulnerability Scanning report, upon request.

8.3 Security Review and Audit

8.3.1 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 its sub-contractors, whenever the need arises or in the event of a data breach. The Participating Service Provider and its sub-contractors shall give full support to the Company and the auditors engaged throughout the audit. Alternatively, the Participating Service Provider shall produce an independent audit assurance report as a compensating control (i.e. **SOC 2 Type 2).**

8.3.2 In the absence of the SOC 2 Type 2 report, the Participating Service Provider shall provide any of the certications as per **Clause 1.1.2 (b)** as an acceptable alternative third party audit requirement.

8.3.3 The Participating Service Provider shall provide the audit recommendations no later than ONE (1) month 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.

8.3.4 The Participating Service Provider shall also assist the Company's risk assessment team to conduct security review of the proposed system's application, including the system 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 provide 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.

9.2 Security Incident Management

9.2.1 The Participating Service Provider shall provide 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;

(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 provide 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 informed, before any data breach information (related to the Company) 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 Business Continuity Management

9.3.1 The Participating Service Provider shall work with the Company to establish a Business Continuity Plan to ensure continuous operation of the proposed system with minimum disruption, in the case of major service disruption.

9.4 Account, Access Rights and Activities Review

9.4.1 The Participating Service Provider shall conduct monthly reviews of privileged accounts, including systems administration accounts, database administrator and user administration accounts. The review of all user accounts and the associated access rights including accounts used for support purposes shall be conducted on a quarterly basis in the proposed system to ensure that unused or obsolete accounts and accesses are removed in a timely manner.

9.4.2 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.

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

9.4.4 The Participating Service Provider shall document and maintain all account usage restrictions, configuration and connection requirements, and implementation processes and procedures for each type of remote access that is allowed, upon the Company's approval.

10 CLOUD MONITORING PORTAL

10.1 The Participating Service Provider shall make available the following to the Company, via a cloud portal:

(a) Annual Service and Organization Control (SOC) 2 Type 2 report; and
(b) Detailed reports of each data breach that is related to the proposed system.

11 SERVICE LEVEL AGREEMENT

11.1 The Participating Service Provider shall minimally cover the following requirements in relation to compliance, best practices and general operational activities, based on the clauses below:

(a) Availability (refer to **Clauses 2.1.5, 2.7.12 and 2.9.4 of Part 4 Service Requirements**);
(b) Performance (refer to **Clauses 2.4(ee)**, **2.6.17**, **2.6.18**, **2.8** and **2.9.4 of Part 4 Service Requirements**);
(c) Security/privacy of data (refer to **Clause 3.2** above);
(d) Logging and reporting (refer to **Clause 7** above);
(e) Disaster recovery expectations (refer to **Clause 2.1.4 of Part 4 Service Requirements**);
(f) Location of the data (refer to **Clauses 3.2.4**, **3.2.5 and 5.2.4** above);
(g) Identification and problem resolution (refer to **Clause 2.5 of Part 4 Service Requirements**);
(h) Exit strategy (refer to **Clause 13.1** below).

12 SUSPENSION OF SERVICES

12.1 If a suspension of service ensues, the responsibilities of the Participating Service Provider are as follows:

(a) The Participating Service Provider shall not delete any data during the suspension period (an advanced notice of a minimum of SIXTY (60) days shall be given to address the reasons for suspension);
(b) If it is determined that the Participating Service Provider had erroneously attributed blame to the Company, payment for services during the suspension period will not be made.

13 EXIT PROCESS

13.1 It is the responsibility of the Participating Service Provider to ensure continuity of service (i.e. data security) at all times during the term of the relevant agreement, including the exit management period and in no way shall any facility/service be affected or degraded. The responsibilities shall include, at least, the following:

(a) The format of the data to be extracted by the Participating Service Provider for the Company shall leverage on standard data formats (i.e. OVF, VHD, etc.), whenever possible, to ease migration to another provider. The format will be finalized by the Company.

(b) The ownership of the data generated upon usage of the proposed system, at any point of time during the term of the relevant agreement or expiry or termination of the relevant agreement, shall rest absolutely with the Company.

(c) Ensure that all the documentation required by the Company, including configuration documents are kept up-to-date and all such documentation is handed over to the Company during regular intervals, as well as during the exit management process.

(d) The Participating Service Provider shall not delete any data at the end of the relevant agreement (for a maximum of FORTY-FIVE (45) days beyond the expiry of the relevant agreement) without the express approval of the Company. There shall not be any additional cost for the storage of data and the Company has the right to access the data during the FORTY-FIVE (45) days period.

(e) Once the exit process is completed, all of the Company's data, content and other assets, including the Company's logs and audit trails, shall be removed from the cloud environment, upon the Company's approval. The Participating Service Provider shall certify that the VM, content and data destruction has been fully actualized, as per stipulations and shall ensure that the data cannot be forensically recovered.

(f) There shall not be any additional cost associated with the exit/transition-out process.