**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 Infrastructure-As-A-Service (IaaS)**.

# PART 2
# MOHH IT SECURITY REQUIREMENTS: SYSTEMS INSTALLED ON IAAS

MOH HOLDINGS

## TABLE OF CONTENTS

# PART 2
# MOHH IT SECURITY REQUIREMENTS: SYSTEMS INSTALLED ON IAAS

## 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 have certifications from the mandatory certification list below and indicate whether they are also certified against the preferable list of certifications:

(a) Mandatory Certifications:

(i) SOC 2 Type 2 / SOC 3
(ii) ISO 27001;
(iii) ISO 27017; and
(iv) ISO 27018
(v) Health Information Trust Alliance (HITRUST); and
(vi) 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

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

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

1.1.6 The Participating Service Provider shall comply with the prevailing standards such as:

(a) Payment Card Industry Data Security Standard (PCIDSS) Level 1 / 2 / 3, if payment transaction is involved;
(b) National Institute of Standards and Technology (NIST) 800-53 and 800-144; and
(c) Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS) Level 1 / 2 / 3.

1.1.7 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.

1.1.8 The Participating Service Provider shall highlight in its Proposal, the cloud shared responsibility framework that defines the security obligations for the proposed Infrastructure-As-A-Service (IaaS) platform between cloud service provider (CSP), system integrator and the Company.

1.1.9 The Participating Service Provider shall document and maintain all systems baselines 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.

1.1.10 The Participating Service Provider shall provide details of the security services for the proposed system, and shall clearly demonstrate that the integrity of the Company's data is not compromised by the services provided.

1.1.11 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.

1.1.12 The Participating Service Provider shall indicate 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.

1.1.13 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.

1.1.14 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.

1.1.15 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.

1.1.16 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) 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 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;
(c) Liaising and co-ordinating with partner companies, security organizations and the Company on security matters; and
(d) Performing other activities necessary to assure a secure environment.

**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 intranet facing layer of the proposed system, the Participating Service Provider shall propose to subscribe CSP's certificate manager for the provisioning, management, and deployment of private SSL/TLS certificates for internal connected resources. All certificates shall also conform to X.509 version 3.

2.1.4 If digital certificates are to be deployed in the internet facing layer of 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.

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

2.1.6 The Participating Service Provider shall propose to subscribe CSP's Hardware Security Modules (HSM) service to protect 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.

2.1.7 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;
(b) Be at least TWELVE (12) characters for non-privilege account (except for portable storage devices);
(c) 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.

(d) Be changed once every TWELVE (12) months;
(e) Not be reused for at least FIVE (5) generations;
(f) Not be displayed in clear;
(g) Be stored in a form that is resistant to offline attacks;
(h) Be forced to change on first use;
(i) Not be the same as the account ID or user ID;
(j) Consecutive failed authentication attempts that can be made on a single account be limited to FIVE (5) times or less, which will then lock the account;
(k) A locked account will be authenticated prior to re-granting access; and
(l) 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 self-service portal, which includes features such as password reset, unlocking and activation of account services.

2.2.4 The Participating Service Provider shall centrally manage access permission to all accounts by leveraging on CSP Single-Sign On service, 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 Contract or expiry or termination of the Contract, 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 Contract.

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.

3.1.6 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 Acceptance Usage Policy.

**3.2 Data Protection**

3.2.1 The Participating Service Provider shall leverage on CSP tagging feature and work with the customer to categorize resources by data classification. The recommended standardized data classification is as follows.

| **Information Classification** | | | |
|---|---|---|---|
| Unclassified, Non-Sensitive | Restricted, Non-Sensitive | Restricted, Sensitive (Normal) | Restricted, Sensitive (High) |

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 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.

3.2.4 The Participating Service Provider shall protect the Company's data from other customer's data in a multi-tenancy environment. These measures shall include, but not be limited to, logical segregation, tenant isolation, role-based access control, controlled change management, data encryption and tokenization.

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

3.2.6 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.

3.2.7 The Participating Service Provider shall ensure that all proposed CSP's services are hosted

in Singapore.

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

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

3.2.10 The Participating Service Provider shall ensure that data stored on databases, file systems and storage systems is protected against unauthorized access. Encryption shall be used, where applicable.

3.2.11 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. The Participating Service Provider shall implement the security measures upon approval by the Company and provide evidence of such security measures implementation.

3.2.12 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. The Participating Service Provider shall also ensure that data is securely erased after the testing is completed.

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

3.2.14 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 following sanitisation methods 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).

3.3.2 The Participating Service Provider shall provide a certificate of data sanitization in relation to **Clause 3.3.1** above, upon completion of data sanitization.

### 3.4 Data Loss Prevention

3.4.1 The Participating Service Provider shall propose to subscribe the following security services from CSP marketplace if the systems are classified as mission-critical systems with Restricted, Sensitive (High) data:

(a) Database Activity Monitoring (DAM).

## 4 SYSTEMS SECURITY

### 4.1 Authentication and Access Control

4.1.1 The Participating Service Provider may propose to leverage on CSP's Identity and Access Management (IAM) service. The IAM service shall support the following frameworks:

(a) Web Services-Trust (WS-Trust);
(b) Security Assertion Markup Language (SAML);
(c) System for Cross-domain Identity Management (SCIM);
(d) Open Authorization (OAuth) 2.0; and
(e) OpenID Connect.

4.1.2 The CSP's IAM service shall allow the Company to define different personnel groups (such as VVIP, VIP, CIP, etc.), to tag specific personnel under one or more of the groups defined, and to restrict access to each personnel group to selected user groups, including in reports, memos and referrals.

4.1.3 The CSP's IAM service allow the Company to define sensitive personal data type (such as salary, performance rating, etc.), and to restrict access to each data type to selected user groups, including in reports, memos and referrals.

4.1.4 All requests to generate account shall go through an approving process proposed by the Participating Service Provider and shall be subject to the Company's approval.

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

4.1.6 The Participating Service Provider shall propose to subscribe Privileged Access Management (PAM) service from CSP marketplace and all administrative access to the virtual servers, database, application shall be done through PAM.

4.1.7 All PAM access shall be logged to facilitate independent reviews of the access and transactions completed.

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

4.1.9 The Participating Service Provider shall propose to subscribe CSP Multi-Factor Authentication (MFA) service to authenticate all administrative access to the virtual servers, database, application and management console within the proposed system.

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

4.1.11 The Participating Service Provider shall implement a notification message or banner to display the following:

(a) Last successful and unsuccessful login; and
(b) Key points on usage indicating consent and subject to monitoring, recording and audit.

4.1.12 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.

4.1.13 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.

4.1.14 The Participating Service Provider shall subscribe PAM password vaulting and session recording service from CSPmarketplace to track, manage and approve requests for privileged administrative access (including system administrators, database administrator, privileged accounts) to production environment and to record the activities performed during such sessions.

4.1.15 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.

4.1.16 All operating system, database and application systems shall be configured with timeout and automatic logout feature for non-active sessions.

**4.2 Secure Configuration**

4.2.1 The Participating Service Provider shall adhere to the Company’s security baselines for virtual machine, networking appliance and database. The security baselines will be shared during the design phase.

4.2.2 In the event that the security baseline for any new hardware or software introduced is not available, the Participating Service Provider shall propose a new security baseline that adheres to industry best practices such as Center for Information Security (CIS) for the Company’s approval.

4.2.3 The Participating Service Provider shall propose to subscribe CSP’s configuration compliance service to identify patching information and configuration inconsistencies against the Company’s security baseline.

4.2.4 The Participating Service Provider shall ensure that the latest security patches for the virtual servers, database and application are applied prior to system commissioning.

4.2.5 The Participating Service Provider shall propose to subscribe security service from CSP to provide a dashboard that gives the Company a comprehensive view of high-priority security and compliance status across accounts, from CSP service and CSP partner tools.

### 4.3 Protection Against Malicious Code

4.3.1 The Participating Service Provider shall subscribe advanced threat protection service from CSP marketplace to protect virtual machines and containers against advanced malware through heuristics detection/machine learning/artificial intelligence.

4.3.2 The Participating Service Provider shall subscribe monitoring and observability services from CSP to provide data and actionable insights to monitor both endpoint protection and advanced threat protection service, as well as to optimize resource utilization and unified view of operational health.

4.3.3 The Participating Service Provider shall subscribe security services from CSP to provide a dashboard that gives the Company a comprehensive view of high-priority security and compliance status across accounts, from CSP service and CSP partner tools.

## 5 NETWORK SECURITY

### 5.1 Network Segmentation and Microsegmentation

5.1.1 The Participating Service Provider shall adopt both network segmentation (north-south network traffic control) and micro-segmentation (east-west network traffic control) concepts in designing network related to the proposed system.

5.1.2 The Participating Service Provider shall adopt the use of separate CSP environment-specific accounts for production vs non-production environments to ensure that development, testing and production environments are logically separated.

5.1.3 The Participating Service Provider shall leverage on CSP tagging feature to enable customer to categorize resources by the different environments.

### 5.2 Network Security Controls

5.2.1 The Participating Service Provider shall propose to subscribe NextGen firewall service from CSP marketplace to protect internet bound traffic (both egress and ingress traffic) and network.

5.2.2 The Participating Service Provider shall leverage on CSP service to implement end-to-end encryption in the proposed system.

5.2.3 The Participating Service Provider shall implement encryption on point to point connections to protect privacy and integrity of the data.

5.2.4 The Participating Service Provider shall design and implement domain name system which consists of both Internet-facing DNS servers and intranet DNS servers, and both DNS servers shall be logically segregated.

5.2.5 The Participating Service Provider shall implement DNS Security Extensions (DNSSEC) for Internet-facing DNS servers.

5.2.6 The Participating Service Provider shall propose to subscribe Content Delivery service from CSP to protect internet-accessible systems and/or internet-accessible network infrastructure to improve reliability and against Denial-of-Service (DoS) attacks. These services include, but not be limited to:

(a) Web Application Firewall (WAF); or
(b) Content Distribution Network (CDN) services.

5.2.7 The Content Delivery service shall support geo-fencing and IP address whitelist and blacklist features.

5.2.8 The Participating Service Provider shall assign both firewall and Network Access Control List (ACL) to protect all instances in Virtual Network Zone.

5.2.9 The Participating Service Provider shall subscribe monitoring and observability service from CSP to provide data and actionable insights to monitor and detectunusual network traffic patterns, as well as to optimize resource utilization and unified view of operational health within the proposed system.

5.2.10 The Participating Service Provider shall propose to subscribe secure web gateway and secure mail gateway services from CSP to block malicious codes.

**5.3 Security Configuration**

5.3.1 The Participating Service Provider shall harden and secure all virtual 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.

5.3.2 The Participating Service Provider shall propose to subscribe CSP configuration compliance service to identify network device or security device patching information, configuration inconsistencies against the Company’s security baselines, and other potential misconfigurations.

**5.4 Remote Administration by the Participating Service Provider**

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

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

(a) Remote administration shall only be granted to the Company’s authorized personnel;
(b) Personnel who are authorized to perform remote administration shall use MFA to authenticate to the virtual machine 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.

5.4.3 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 proposed system is internet-accessible and consists of custom software development, 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 In the event that the proposed system is Commercial-off-the-Shelf (COTS) product, the Participating Service Provider shall provide security attestation that the COTS product has been designed, manufactured, and delivered with integrated security at every phase of the product life cycle.

6.1.4 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.

6.1.5 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.

6.1.6 The Participating Service Provider shall ensure that the production systems only hold approved executable code and not development code or compilers.

6.1.7 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.

6.1.8 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.

6.1.9 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.

6.1.10 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.

6.1.11 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 User Access Matrix (UAM) 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 UAM 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.

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 All users shall have a unique identifier (user ID) for their personal use so that activities can be traced to the responsible individual.

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

6.2.8 The Participating Service Provider shall ensure that non-interactive service account is assigned with least privileged access that is specific to the tasks of the service account. For new systems, the Participating Service Provider shall not allow the use of system/service accounts in scripts or programs, unless it is approved by the Company.

6.2.9 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, closed and invalidated 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.

6.2.10 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.

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

6.2.12 The proposed system shall be designed to protect 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.

6.2.13 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 If the Company AD ID is proposed to be used for authentication, the Participating Service Provider shall ensure that approved company authentication service (e.g. Azure AD, AWS directory service) is used to login to the proposed system.

6.2.15 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 Participating Service Provider shall subscribe CSP Security Token Service to

authenticate and authorize all web services requests used in application.

6.3.2 Application-to-application interfaces (e.g. 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.

Note: In a typical THREE-(3)-tier architecture, separation is achieved when a Firewall and/or Network ACL is implemented to monitor all network traffics between the web and application tiers and similarly, between the application and database tiers.

6.4.2 The Participating Service Provider shall subscribe Web Application Firewall (WAF) service from CSP to safeguard all internet-accessible systems, to secure the connection to untrusted external networks such as connections with third parties, and 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.

### 6.5 Application Performance Monitoring

6.5.1 The Participating Service Provider shall propose a Cloud Application Performance Management (CAPM) to provide monitoring resources for continuous observation of a system in action, tracking system availability and performance.

## 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;<br>(ii) Security policy and configuration changes;<br>(iii) System account and access rights creation and changes;<br>(iv) Elevation of privilege;<br>(v) Privileged account activities;<br>(vi) Log on attempts;<br>(vii) Network connection changes or failures; |

| Log Source | Security-related Events |
|---|---|
| | (viii) System start up and shutdown events;<br>(ix) Service start up and shutdown events; and<br>(x) Installation of new software and services |
| **(b) Database** | (i) Database configuration changes;<br>(ii) Database account and access rights creation and changes;<br>(iii) Connection attempts to the database;<br>(iv) Occurrence of errors;<br>(v) Database schema modifications;<br>(vi) Queries of database schemas;<br>(vii) Queries for unexpected large dataset;<br>(viii) Queries with multiple embedded queries; and<br>(ix) Execution of operating system commands. |
| **(c) Application** | (i) Application configuration changes;<br>(ii) Application security policy and configuration changes;<br>(iii) Application account and access rights creation and changes;<br>(iv) Successful and failed login attempts;<br>(v) Occurrence of errors;<br>(vi) Activities performed by the users (as determined through the Company's risk management process); and<br>(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 security service 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 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 Company's log monitoring system.

7.1.4 The Participating Service Provider shall ensure that the proposed system does not capture passwords and other sensitive data in its 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 personnel records over a specified time period.

7.1.7 The Participating Service Provider shall ensure that 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 Participating Service Provider shall ensure that 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.

7.1.9 The Participating Service Provider shall ensure that the clocks of the proposed system are synchronized to a single reference time source (Singapore time zone).

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 security violations or incidents.

7.1.11 The Participating Service Provider shall ensure that the proposed system shall provide cryptographic mechanisms to protect the integrity of the audit log or record.

**7.2 Audit Log Reporting**

7.2.1 The Participating Service Provider shall leverage on logs service from CSP for automation of the generation of reports to maintain the integrity of the reports and to make sure that the generated reports are not tampered with.

7.2.2 The Participating Service Provider shall work with the Company and provide a secure approach of importing OS, application, database and security device logs into the Company's Security Information and Event Management (SIEM) system to enable a near real-time analysis of security alerts, unless it is deemed by the Company as not required for the proposed system.

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

7.2.4 The Participating Service Provider shall provide the Company with a 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 Central Log Management**

7.3.1 The Participating Service Provider shall propose to subscribe native logs service from CSP to monitor, store, and access log files. This service shall centralize the logs from all systems, applications, and CSP services that consume within the proposed system.

7.3.2 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 |

**7.4 Security Monitoring**

7.4.1 The Participating Service Provider shall propose to subscribe security monitoring services from CSP to facilitate the prompt detection of anomalous activities, unless it is deemed by the Company that the proposed system shall integrate with the Company's security operations center (SOC) monitoring services and the Participating Service Provider shall facilitate the integration activity.

7.4.2 The Participating Service Provider shall propose website defacement-monitoring services from CSP marketplace and ensure that it performs timely detection of defacement and recovery from the defacement for all internet-accessible systems:

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

7.4.3 The Participating Service Provider shall investigate and address all security alerts and alarms raised by the security monitoring service or 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) Data mining;
(b) Malware attacks;
(c) DoS/DDoS attacks;
(d) Web application attacks;
(e) Unauthorized access; and
(f) Password guessing attacks.

## 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 or Offensive Security 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 Registered Penetration Tester;
(ii) CREST Certified Web Application Tester;
(iii) CREST Certified Infrastructure Tester;
(iv) Offensive Security Certified Professional; or
(v) Offensive Security Web Expert.

(c) The selected penetration test service provider shall be an independent party that has no prior involvement with the proposed system that is in the test scope.

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.

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 leverage on the Company's vulnerability management solution to ensure that all vulnerabilities within the proposed system are addressed before system commissioning. In the event that the Company's vulnerability management solution is not available, the Participating Service Provider shall propose a vulnerability management solution for the Company's approval. The Company's approval

of a new vulnerability management solution is needed.

8.2.2 The Participating Service Provider shall ensure that the application software, operating system, virtual machines and network infrastructure within the proposed system are scanned according to the frequency shown below:

| Component | Frequency |
|---|---|
| **Application Software** | Annually |
| **Operating System** | Quarterly |
| **Network** | Quarterly |

8.2.3 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)** | TWO (2) weeks |
| **Medium (Severe)** | ONE (1) month |
| **Low (Moderate)** | TWO (2) months |

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

### 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 conducts 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 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).

8.4.2 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.

8.4.3 In the absence of the SOC 2 Type 2 report, the Participating Service Provider shall provide any of the certifications as per **Clause 1.1.3 (b)** as an acceptable alternative third party audit requirement:

## 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 that all components in the proposed system (including all hardware [e.g. servers, workstations, laptops, network devices, security devices]) 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**<br>Includes higher risk assets that have broad attack surface or high risk impact | (a) Internet-facing ICT systems (including internet-facing infrastructure, servers, software) in the Internet Zone | Critical* / High | ONE (1) month |
| | | Medium / Low | TWO (2) months |
| | (b) CII Systems | Critical* / High | TWO (2) months |
| | | Medium / Low | THREE (3) months |
| | (c) Internal infrastructure systems on the intranet (e.g., core switch, core firewall, hypervisor) | All** | TWELVE (12) months |
| **Asset Type B**<br>Intranet ICT application systems | (a) ICT systems using Windows platforms (including End User Computing (EUC)) | All** | THREE (3) months. For Windows EUC, co-existence testing is required before deployment |
| | (b) ICT systems using non-Windows platforms | All** | SIX (6) months |

| Type of Asset | Type of System | Type of Patch | Deployment upon Availability of Patch |
|---|---|---|---|
| | (c) ICT systems which 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 validating 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 which 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) and/or Ministry of Health (MOH). In addition, emergency patch will also be 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 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.

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

9.1.7 The Participating Service Provider shall maintain an up-to-date inventory of the services 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 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; 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 (“Chain of Custody”) 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 informed, before any security incident 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 update 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 Systems Change Management**

9.3.1 The Participating Service Provider shall adhere 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.

9.3.2 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.

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

9.3.4 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.

**9.4 Business Continuity Management**

9.4.1 The Participating Service Provider shall seek confirmation from the Company on the need to establish a Business Continuity Plan to ensure continuous operation of the proposed system with minimum disruption, in the case of major service disruption.

**9.5 Account, Access Rights and Activities Review**

9.5.1 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 |
|---|---|
| **List of inactive/suspended accounts** | Quarterly |
| **All accounts in Mission Critical systems** | Half-yearly |
| **All accounts in Business Critical and Standard systems** | Annually |

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.

9.5.2 The review procedures implemented shall cover the following scenarios:

(a) Staff resignation/ retirement;
(b) Termination;
(c) Staff Transfer;
(d) Role change with same company;
(e) Role changes within same department;
(f) Extended leave; and
(g) External party user resignation/redeployment.

9.5.3 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.

9.5.4 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.

9.5.5 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.

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

9.5.7 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 3.2.5**, **3.2.6 and 3.2.7** 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 Contract, 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 Contract or expiry or termination of the Contract, 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 Contract (for a maximum of FORTY-FIVE (45) days beyond the expiry of the Contract) 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.