MINISTRY OF HEALTH
SINGAPORE

Clinic Management System (CMS) Cybersecurity (CS) requirements for Software as a service (SaaS)

These prevailing requirements are expected to be put in place and will be reviewed from time to time to address evolving cybersecurity risks.

No.	Recommended Controls*
Product feature where CMS applications are provided as a service (SaaS).	
1	The CMS solution shall backup its configuration and data that it stores. The backup data shall be encrypted with cryptographic algorithms and key lengths that follow the recommendations from NIST or equivalent. Access controls shall be in place to monitor and control access to the backup data.
2	The CMS solution shall allow its backup data be kept offline.
3	The CMS solution shall authenticate all login personnel through multi-factor authentication (MFA).
4	The CMS solution shall support the use of strong password (e.g. at least 12 characters long and includes upper case, lower case, and/or special characters).
5	The CMS solution shall allow CMS administrator to suspend inactive accounts (e.g. not used for at least 90 days).
6	The CMS solution shall allow CMS administrator to apply the principle of least privilege to all accounts (e.g. users, services) so as to ensure excessive privileges are not granted. The CMS solution should implement Attribute-Based Access Control (ABAC) using multiple attributes such as role, location, authentication method, IP address, mutual authentication and/ or Role-Based Access Control (RBAC) mechanism that enforces access to all parts of the CMS.
7	The "out-of the box" default installation of the CMS solution shall log all user access and be able to link all activities to individual users.
8	The CMS solution shall provide automated security-related logs to facilitate event reconstruction and incident investigation.
9	The CMS solution shall store logs at secured locations to protect the integrity and ensure availability of the logs. It should have the capability to store logs in 3rd party solution.
10	The CMS solution shall generate logs that are readable in ASCII plaintext or UTF8.
11	The CMS solution shall ensure only authorised personnel is able to access the logs.
12	The CMS solution shall ensure processes involving data-in-motion, such as backup or migration, is protected with encryption.
13	CMS Provider shall establish backup strategies (e.g. scope and frequency for data backups is determined and implemented, etc.) and aligned with RPO (Recovery Point Objective) and RTO (Recovery Time Objective).

Ministry of Health, Singapore
College of Medicine Building
16 College Road
Singapore 169854
TEL (65) 6325 9220
FAX (65) 6224 1677
WEB www.moh.gov.sg

CMS provider's responsibilities on its production and development environment.	
14	CMS Provider shall backup the CMS solution's configuration, source code and data that it stores. The backup data shall be encrypted with cryptographic algorithms and key lengths that follow the recommendations from NIST or equivalent. Access controls shall be in place to monitor and control access to the backup data.
15	CMS Provider shall ensure the backup data is kept offline.
16	CMS Provider shall conduct annual testing of data recoverability to validate effectiveness of disaster recovery plans.
17	CMS Provider shall maintain an asset inventory for its CMS solution and development environment, including 3rd party software and tools deployed.
18	CMS Provider shall update the asset inventory at least annually, and ensure no end-of-life (EOL) products are used.
19	CMS Provider shall implement tracking of expiry dates for all digital assets, such as certificates, software licenses, etc, for renewal.
20	CMS provider shall implement a version control system where developers can roll back to a previous version in the event of any show-stopping bug gets discovered.
21	CMS Provider shall have vulnerability management processes to identify and manage vulnerabilities in the CMS solution, production and development environment.
22	CMS Provider shall perform security testing (such as Vulnerability Assessment / Penetration Testing) on the CMS solution and production environment before commissioning, periodically and upon major changes.
23	CMS Provider shall remediate identified vulnerabilities that have a risk rating of "High". The risk rating should be based on industry best practices as well as consideration of potential impact. For example, criteria for the rating may include consideration of the CVSS base score, and/or the classification by the provider, and/or impact to application functionality.
24	CMS Provider shall implement whitelisting of peripherals (e.g. only authorized USB drives) to prevent bypassing of authentication resulting in unauthorised administrative access.
25	CMS Provider shall ensure non-root credentials are used for day-to-day administration and put in place a process for dual authorisation when the use of root credentials is required.
26	CMS Provider shall implement multi-factor authentication (MFA) for physical access to the room that host the CMS solution and the room that host terminal(s) that has/have access to the CMS solution.
27	CMS Provider shall practise the use of strong password (e.g. at least 12 characters long and includes upper case, lower case, and/or special characters).
28	CMS Provider shall ensure proper account management is established, authorised and maintained. Proper account management include, but not limited to: 1. Inventory of accounts (for user, administrator, third-party, and service accounts); 2. Process with the necessary approvals to grant and revoke access; 3. Process to regularly review accounts that are expired or unused; 4. Process to remove accounts that are expired, unused, shared, duplicate and invalid; 5. Requirement that govern the use of administrator account (i.e. Administrator account shall only be accessed to perform administrator functions with approval from the senior management.);

	6. Requirement that govern the use of third-party or contractors account (i.e. Third parties/contractors can access only the information and systems required for their job role. Such access shall be removed once they no longer require them. Third-party or contractors shall sign a non-disclosure agreement form and the form should include disciplinary action(s) for failure to abide by the agreement.); 7. Requirement to apply the principle of least privilege to all accounts (e.g. users, services) to ensure excessive privileges are not granted; 8. Requirement to change all default passwords and replace with a strong passphrase, e.g. it should be at least 12 characters long and includes upper case, lower case, and/or special characters; 9. Requirement to disable and/or lock out account after multiple failed login attempts, e.g. after 10 failed login attempts; and 10. Requirement to change password of the account in the event of any suspected compromise.
29	CMS Provider shall ensure clear segregation of duties for privileged roles in the CMS such as network, operating system, database, log management and security administrators to address risks associated with user-role conflict of interest.
30	CMS Provider shall establish access control matrix for CMS's underlying infrastructure, with roles and responsibilities clearly documented.
31	CMS Provider shall implement process for onboarding and offboarding of joiners, movers and leavers.
32	CMS Provider shall ensure security posture checks (e.g. check that anti-malware is installed and definitions updated and OS patches are updated) are carried out for devices used for administration before granting access to the network.
33	CMS Provider shall store logs at secured locations to protect the integrity and ensure availability of the logs.
34	CMS Provider shall ensure only authorised personnel is able to access the logs; operations personnel should not have access to logs to prevent risk of tampering or deletion.
35	CMS Provider shall provide documentation that has information on the log formats, to facilitate log review.
36	CMS Provider shall esure a log review process is defined, documented and implemented to detect suspicious activities and early indicators of security breaches.
37	CMS Provider shall ensure security logs are generated and monitored timely to detect suspicious or malicious activity (e.g. unusual administrative activities during off peak hours, creation of unknown administrator accounts, escalating privileges for user accounts, lateral traversal across multiple segments and attempted download/upload by single system within a short period, disabling security controls such as disable audit log etc.)
38	CMS Provider shall ensure security monitoring mechanisms are in place to monitor all security related events for timely detection of suspicious events or malicious activities.
39	CMS Provider shall ensure measures (e.g. firewall, network Access Control List (ACL), security groups) are implemented to block unauthorised traffic and to prevent medical data from being exfiltrated by attackers.
40	CMS Provider shall implement a Web Application Firewall (WAF) to mitigate threats (e.g. OWASP Top 10) from external sources.

41	CMS Provider shall ensure that terms on unauthorised disclosure of information are included within the CMS provider's employment contracts and contractual agreement with their business partners (e.g. providing the maintenance services).
42	CMS Provider shall put in place security awareness programs for their staff.
43	CMS Provider shall ensure that audit reports of the policies, operations and processes of the CMS are made available to the customer.
44	CMS Provider shall put in place incident response plan to assist healthcare provider in responding to their obligations under prevailing legislative or regulatory requirements.

*As at 25 Aug 2022

--End--

Ministry of Health, Singapore
College of Medicine Building
16 College Road
Singapore 169854
TEL (65) 6325 9220
FAX (65) 6224 1677
WEB www.moh.gov.sg

Ministry of Health, Singapore
College of Medicine Building
16 College Road
Singapore 169854
TEL (65) 6325 9220
FAX (65) 6224 1677
WEB www.moh.gov.sg