Annex A-CMS
(normative)

Cyber Essentials mark for Clinic Management System (CMS) Vendors – Requirements

A-CMS.1 Introduction

The Ministry of Health (MOH) oversees the healthcare sector in Singapore. MOH also licenses and regulates all healthcare establishments such as hospitals, nursing homes, clinical laboratories, medical and dental clinics. Cybersecurity is critical to the provision of quality and safe healthcare services in ensuring patient safety and welfare.[1] To this end, CSA and MOH have worked on an extension of the Cyber Essentials mark that is targeted at Clinic Management Solution (CMS) Vendors under the MOH CMS tiering framework. This extension of Cyber Essentials mark is referred to as "Cyber Essentials for CMS Vendors".

This document described the CMS cybersecurity requirements for software-as-a-service (SaaS) and non-SaaS implementations.

A-CMS.2 Additional terms and definitions

For the purposes of this annex, the following terms and definitions apply.

A-CMS.2.1 CMS implemented as software-as-a-service (SaaS)

CMS applications and product features are provided as a service.

A-CMS.2.2 CMS implemented as non-SaaS

CMS applications and product features are deployed as a standalone application installed on a workstation/desktop/laptop.

A-CMS.3 Cyber Essentials mark for CMS vendor

A-CMS.3.1 Boundary of scope and statement of scope

The scope of assessment and certification shall cover at least the following:

- The production and development environment for CMS vendor providing SaaS solution; and
- The development environment for CMS vendor providing non-SaaS solution.

[1] Cybersecurity for Healthcare Providers by Ministry of Health (MOH)

The requirements for Cyber Essentials mark shall apply to all devices, systems[2] and software that are within this boundary of scope.

A-CMS.3.2 Pre-certification preparation by the CMS vendor

Prior to engaging a certification body, the CMS vendor shall complete the guided self-assessment template required for Cyber Essentials mark certification for CMS vendor.

This consists of a list of requirements and recommendations that the CMS vendor shall assess and indicate if these have been implemented in the organisation.

A-CMS.3.3 Independent assessment by certification body

Following the completion of its self-assessment, the CMS vendor shall approach any of the certification bodies appointed by CSA and MOH for independent assessment and issuance of the Cyber Essentials mark certification for CMS vendor.

For the organisation to be certified for Cyber Essentials mark for CMS vendor, the organisation shall meet all the requirements in the Cyber Essentials mark as well as the additional requirements required by MOH. [3]

A-CMS.4 Provisions for Cyber Essentials for CMS vendor

Following shows the provisions for Cyber Essentials for CMS vendor.

Clause	Provisions in Cyber Essentials	Additional provisions for CMS vendor for clinic
A.1 Assets: People – Equip employees with know-how to be the first line of defence		
A.1.4 (a)	Requirement	Requirement
A.1.4 (b)	Requirement	Requirement
A.1.4 (c)	Recommendation	Recommendation
A.1.4 (d)	Recommendation	Recommendation
A.1.4 (e)	Recommendation	Recommendation
A.2 Assets: Hardware and software – Know what hardware and software the organisation has and protect them		
A.2.4 (a)	Requirement	Requirement NOTE: – The asset inventory shall include 3rd party software and tools deployed. – The asset inventory shall track expiry of all digital assets, such as certificates, software licenses, software renewal, etc.

[2] For CMS vendor that adopts cloud-based software, the scope of assessment and certification shall include such cloud-based services.

[3] Provisional list of Clinic Management System (CMS) Cybersecurity (CS) Requirements by Ministry of Health (MOH)

Clause	Provisions in Cyber Essentials	Additional provisions for CMS vendor for clinic
		– The asset inventory shall be reviewed at least once a year.
A.2.4 (b)	Recommendation	Recommendation
A.2.4 (c)	Recommendation	Recommendation
A.2.4 (d)	Requirement	Requirement NOTE: – The asset inventory shall include 3rd party software and tools deployed.
A.2.4 (e)	Recommendation	Recommendation
A.2.4 (f)	Recommendation	Recommendation
A.2.4 (g)	Requirement	Requirement
A.2.4 (h)	Requirement	Requirement NOTE: – This requirement is deemed as met, as no EOS asset shall be allowed for the CMS vendor.
A.2.4 (i)	Requirement	Requirement
A.2.4 (j)	Requirement	Requirement
A.2.4 (k)	Requirement	Requirement
A.2.4 (l)	Requirement	Requirement
A.2.4 (m)	Recommendation	Recommendation
A.3 Assets: Data – Know what data the organisation has, where they are and secure the data		
A.3.4 (a)	Requirement	Requirement
A.3.4 (b)	Recommendation	Recommendation
A.3.4 (c)	Requirement	Requirement NOTE: – CMS vendor shall also establish process(es) to protect data-in-motion, such as backup or migration.
A.3.4 (d)	Requirement	Requirement NOTE: – The terms on unauthorised disclosure of information shall be included within the CMS vendor's employment contracts and contractual agreement with its business partners (e.g., providing the maintenance services).
A.3.4 (e)	Requirement	Requirement
A.4 Secure/Protect: Virus and malware protection – Protect from malicious software like viruses and malware		
A.4.4 (a)	Requirement	Requirement
A.4.4 (b)	Requirement	Requirement

Clause	Provisions in Cyber Essentials	Additional provisions for CMS vendor for clinic
A.4.4 (c)	Requirement	Requirement
A.4.4 (d)	Requirement	Requirement
A.4.4 (e)	Recommendation	Recommendation
A.4.4 (f)	Requirement	Requirement NOTE: – CMS vendor providing SaaS solution shall implement a Web Application Firewall (WAF) to mitigate threats (e.g., OWASP Top 10) from external sources.
A.4.4 (g)	Recommendation	Recommendation
A.4.4 (h)	Recommendation	Recommendation
A.4.4 (i)	Recommendation	Recommendation
A.4.4 (j)	Requirement	Requirement
A.4.4 (k)	Requirement	Requirement
A.4.4 (l)	Requirement	Requirement
A.5 Secure/Protect: Access control – Control access to the organisation's data and services		
A.5.4 (a)	Requirement	Requirement
A.5.4 (b)	Requirement	Requirement
A.5.4 (c)	Requirement	Requirement
A.5.4 (d)	Requirement	Requirement NOTE: – 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. – CMS vendor 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. – CMS vendor shall establish access control matrix for CMS's underlying infrastructure, with roles and responsibilities clearly documented. – CMS vendor shall ensure that only authorised personnel is able to access the logs; operations personnel should not have access to logs to prevent risk of tampering or deletion.
A.5.4 (e)	Requirement	Requirement
A.5.4 (f)	Requirement	Requirement

Clause	Provisions in Cyber Essentials	Additional provisions for CMS vendor for clinic
A.5.4 (g)	Requirement	Requirement
A.5.4 (h)	Requirement	Requirement
A.5.4 (i)	Requirement	Requirement NOTE: – CMS vendor providing SaaS solution 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.
A.5.4 (j)	Recommendation	Recommendation
A.5.4 (k)	Recommendation	Requirement
A.5.4 (l)	Requirement	Requirement
A.5.4 (m)	Requirement	Requirement
A.5.4 (n)	Requirement	Requirement
A.5.4 (o)	Recommendation	Requirement NOTE: – The CMS solution shall authenticate all login personnel through multi-factor authentication (MFA).
A.5.4 (p)	Recommendation	Recommendation
A.6 Secure/Protect: Secure configuration – Use secure settings for the organisation's hardware and software		
A.6.4 (a)	Requirement	Requirement NOTE: – CMS vendor shall have vulnerability management processes to identify and manage vulnerabilities in the CMS solution, as well as production and development environments. – CMS vendor shall perform security testing (such as Vulnerability Assessment / Penetration Testing) on the CMS solution and production environment before commissioning, periodically and upon major changes. – CMS vendor 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 vendor, and/or impact to application functionality.
A.6.4 (b)	Requirement	Requirement
A.6.4 (c)	Requirement	Requirement
A.6.4 (d)	Requirement	Requirement
A.6.4 (e)	Requirement	Requirement
A.6.4 (f)	Recommendation	Requirement

Clause	Provisions in Cyber Essentials	Additional provisions for CMS vendor for clinic
		NOTE: – The "out-of-the-box" default installation shall log all user access and be able to link all activities to individual users. – The CMS solution shall provide automated security-related logs to facilitate event reconstruction and incident investigation. – The CMS solution shall generate logs that are readable in ASCII plaintext or UTF-8. – 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. – CMS vendor shall store logs at secured locations to protect the integrity and ensure availability of the logs. – CMS vendor shall provide documentation that has information on the log formats, to facilitate log review. – CMS vendor shall ensure that a log review process is defined, documented and implemented to detect suspicious activities and early indicators of security breaches. – CMS vendor shall ensure that 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.) – CMS vendor shall ensure that security monitoring mechanisms are in place to monitor all security related events for timely detection of suspicious events or malicious activities
A.6.4 (g)	Recommendation	Recommendation
A.6.4 (h)	Recommendation	Recommendation
A.7 Update: Software updates – Update software on devices and systems		
A.7.4 (a)	Requirement	Requirement NOTE: – CMS vendor, who is supplying CMS application to healthcare service provider, shall notify Licensees[4] the availability of updates/patches, and deliver those updates/patches to the Licensees in a secure and prompt

[4] Licensee refers to clinics licensed under the Healthcare Services Act 2020, and the Private Hospitals and Medical Clinics Act 1980.

Clause	Provisions in Cyber Essentials	Additional provisions for CMS vendor for clinic
		manner, if possible, guide/assist the Licensee to ensure the updates/patches are implemented successfully.
A.7.4 (b)	Recommendation	Recommendation
A.7.4 (c)	Recommendation	Recommendation
A.7.4 (d)	Recommendation	Recommendation
A.8 Backup: Back up essential data – Back up the organisation's essential data and store them offline		
A.8.4 (a)	Requirement	Requirement NOTE: – CMS vendor shall establish backup strategies (e.g. scope and frequency for data backups is determined and implemented, etc.) and aligned with RPO. – CMS vendor 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.
A.8.4 (b)	Requirement	Requirement
A.8.4 (c)	Recommendation	Recommendation
A.8.4 (d)	Recommendation	Recommendation
A.8.4 (e)	Requirement	Requirement
A.8.4 (f)	Recommendation	Recommendation
A.8.4 (g)	Requirement	Requirement NOTE: – The backup shall include configuration, source code and data. – The backup shall be encrypted with cryptographic algorithms and key lengths that follow the recommendations from NIST or equivalent.
A.8.4 (h)	Requirement	Requirement NOTE: – CMS vendor providing non-SaaS solution shall also ensure that the solution has the feature to allow its backup data be kept offline.
A.8.4 (i)	Recommendation	Recommendation
A.8.4 (j)	Requirement	Requirement NOTE: – The backup shall be encrypted with cryptographic algorithms and key lengths that follow the recommendations from NIST or equivalent.
A.8.4 (k)	Recommendation	Requirement

Clause	Provisions in Cyber Essentials	Additional provisions for CMS vendor for clinic
A.9 Respond: Incident response – Be ready to detect, respond to, and recover from cybersecurity incidents		
A.9.4 (a)	Requirement	Requirement NOTE: – CMS vendor providing SaaS solution shall also put in place incident response plan to assist healthcare provider in responding to their obligations under prevailing legislative or regulatory requirements.
A.9.4 (b)	Requirement	Requirement
A.9.4 (c)	Recommendation	Recommendation
A.9.4 (d)	Recommendation	Recommendation