Toffs overview for CSA Cyber Essentials mark

The Cyber Essentials mark is a cybersecurity certification for organisations that are embarking on their cybersecurity journey. Developed by the Cyber Security Agency of Singapore (CSA), it serves to recognise that the organisation has put in place good cyber hygiene practices to protect their operations and their customers against common cyber-attacks.

Toffs Technologies, in collaboration with the CSA SG Cyber Safe Partnership Programme, offers the below services to enable the organisation to address measures in attaining the Cyber Essentials mark.

How TOFFS Technologies enables enterprises to address CSA Cyber Essentials mark

Measures in Cyber Essentials	'Base' Services	Additional/ Optional Services*
ASSETS • **People** Equip your employees to be your first line of defence	Annual cybersecurity awareness training [1]	
ASSETS • **Hardware and Software** Know what hardware and software you have	Asset discovery and inventory management of hardware using PRTG (PaessierRouter Traffic Grapher or equivalent)	
ASSETS • **Data** Know what data you have, where they are and who has access to your data	Data management access, control policies and framework Establish procedures to dispose data securely	*Data management and internet protection for IoT / Operational Technology sensors and systems[2]* *Internet protection for web and mobile applications using Toffs ZeroDownTIme Cloud Security & WAF (Web Application Firewall or equivalent)*

SECURE/PROTECT • **Virus/Malware Protection** Protect yourself from malicious software	Secure endpoints with application control and anti-malware (SecureAge APlus or equivalent)	*Real-time managed endpoint detection and response (ReaQta or equivalent)* *Manage firewall rules and configuration*
SECURE/PROTECT • **Access Control** Control who has access to your data and services	User access management policies and framework and establish appropriate user access and password policies	*User and Entity Behaviour Analytics (UEBA) and monitoring of privileged accounts (InsiderSecurity or equivalent)*

SECURE/PROTECT ● **Secure Configuration** Use secure settings for your hardware and software	Enable logs management in systems for audit purposes and review security configuration of assets 2	*Vulnerability scans to verify compliance (SecureAge APlus or equivalent)*

UPDATE ● **Update your software**	Guide users to perform patching and upgrades of software on a regular basis	*24x7 SOC monitoring with patch management and response 2*

BACKUP ● **Back up your essential data**	Configure appropriate data backup policies	*Provide a backup solution with encryption for sensitive data*

RESPOND ● **Know what to do and how to recover from a cyber incident**	Guide organisation designated person to use the templates for incident response 3	*24x7 incident response team from Toffs Security Operations Centre*

https://go.gov.sg/cyber-essentials-partners
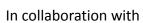
Enterprises should refer to CSA's website for more information on Cyber Essentials

1 –Complemented by [CSA Cybersecurity Toolkit for Employees](#)
2 –May need to be complemented by additional tools and/or processes
3 –Provided for in [CSA Cybersecurity Toolkit for IT Teams](#)

In collaboration with   **SG CYBER SAFE** | **PARTNERSHIP PROGRAMME**   **TOFFS** Technologies
where speed and security matters

This information sheet is developed in collaboration with Cyber Security Agency of Singapore (CSA) as part of its [SG Cyber Safe Partnership Programme](#) to generate awareness and raise the cybersecurity posture of local businesses, individuals and the community. Please note that CSA does not endorse or recommend any particular organisation, individual, product, process, or service that is linked to the SG Cyber Safe partnership programme. Neither can CSA assure the quality of the work of any organisation or individual linked to the SG Cyber Safe partnership programme.

Contact: info@toffstech.com   www.toffstech.com