First published in the Government *Gazette*, www.egazette.gov.sg, on 29 October 2026 at 5 pm.

No. S 791

CYBERSECURITY ACT 2018

CYBERSECURITY (ENTITIES OF SPECIAL CYBERSECURITY INTEREST) REGULATIONS 2026

ARRANGEMENT OF REGULATIONS

Regulation

1. Citation and commencement
2. Information to ascertain if criteria for entity of special cybersecurity interest fulfilled
3. Information relating to system of special cybersecurity interest
4. Report of cybersecurity incident affecting entity of special cybersecurity interest

---

In exercise of the powers conferred by section 48 of the Cybersecurity Act 2018, the Minister for Digital Development and Information, Josephine Teo, who is charged with the responsibility for cybersecurity, makes the following Regulations:

Citation and commencement

1. These Regulations are the Cybersecurity (Entities of Special Cybersecurity Interest) Regulations 2026 and come into operation on 30 October 2026.

Information to ascertain if criteria for entity of special cybersecurity interest fulfilled

2. For the purposes of section 18A(2) of the Act, a notice to provide relevant information to the Commissioner must be given in writing in the form set out for that purpose on the Internet website at https://www.csa.gov.sg.

Information relating to system of special cybersecurity interest

3. For the purposes of section 18D(1) of the Act, a notice to the entity of special cybersecurity interest to furnish information must be given in writing in the form set out for that purpose on the Internet website at https://www.csa.gov.sg.

Report of cybersecurity incident affecting entity of special cybersecurity interest

4.—(1) For the purposes of section 18F(1) of the Act, the entity of special cybersecurity interest must notify the Commissioner of the occurrence of a prescribed cybersecurity incident in respect of the system of special cybersecurity interest within the following prescribed periods and in the following prescribed form and manner:

(*a*) within 24 hours after becoming aware of the occurrence — by submitting the following details in the manner specified in paragraph (2):

(i) the system of special cybersecurity interest to which the incident relates;

(ii) the nature of the incident, including —

(A) a statement whether the incident —

(AA) resulted in a breach in the availability, confidentiality or integrity of the entity's data; or

(AB) had a significant impact on the business operations of the entity;

(B) a description of when and how the incident occurred; and

(C) a description of the data stored on the system of special cybersecurity interest to which the incident relates;

(iii) the resulting effect that has been observed, including the effect on the entity and its business operations;

(iv) the name, designation, organisation and contact number of the individual submitting the notification;

(*b*) within 72 hours after becoming aware of the occurrence — by providing, to the fullest extent practicable, the following supplementary details in writing, in the form set out for that purpose on the Internet website at https://www.csa.gov.sg:

(i) any updates and supplementary details in respect of the details submitted under sub-paragraph (*a*);

(ii) the cause of the incident;

(iii) the impact of the incident on the system of special cybersecurity interest to which the incident relates;

(iv) the remedial measures that have been taken;

(*c*) within 30 days (including any Sunday and public holiday) after the submission mentioned in sub-paragraph (*b*) is made — by providing a final incident report containing the following details in writing in the form set out for that purpose on the Internet website at https://www.csa.gov.sg:

(i) the details submitted under sub-paragraphs (*a*) and (*b*);

(ii) to the fullest extent practicable, any updates and supplementary details in respect of the information submitted under sub-paragraphs (*a*) and (*b*).

(2) The manner of submission mentioned in paragraph (1)(*a*) is submission —

(*a*) by calling the telephone number specified by the Commissioner; or

(*b*) if the entity is unable to submit the details in the manner set out in sub-paragraph (*a*) within a reasonable time —

(i) by text message to the telephone number specified by the Commissioner; or

(ii) in writing, in the form set out for that purpose on the Internet website at https://www.csa.gov.sg, to the electronic address specified by the Commissioner.

(3) For the purposes of section 18F(1) of the Act, the following incidents are prescribed cybersecurity incidents in respect of a system of special cybersecurity interest:

(*a*) any unauthorised hacking of the system of special cybersecurity interest to gain unauthorised access to or control of the system of special cybersecurity interest;

(*b*) any installation or execution of unauthorised software, or computer code, of a malicious nature on the system of special cybersecurity interest;

(*c*) any man-in-the-middle attack, session hijack or other unauthorised interception by means of a computer or computer system of communication between the system of special cybersecurity interest and an authorised user of the system of special cybersecurity interest;

(*d*) any denial of service attack or other unauthorised act or acts carried out through a computer or computer system that adversely affects the availability or operability of the system of special cybersecurity interest.

(4) In this regulation, "interception", in relation to a communication to or from a system of special cybersecurity interest, includes —

(*a*) listening to or the recording of the communication; and

(*b*) acquiring the substance, meaning or purport of that communication.

Made on 28 October 2026.

CHNG KAI FONG
Permanent Secretary
(Cybersecurity),
Prime Minister's Office,
Singapore.

[CSA.0007.200003; 2020-1629; AG/LEGIS/SL/70A/2025/2]