First published in the Government *Gazette*, www.egazette.gov.sg, on 15 October 2025 at 7 pm.

No. S 680

CYBERSECURITY ACT 2018

CYBERSECURITY (SYSTEMS OF TEMPORARY CYBERSECURITY CONCERN) REGULATIONS 2025

ARRANGEMENT OF REGULATIONS

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 (Systems of Temporary Cybersecurity Concern) Regulations 2025 and come into operation on 31 October 2025.

Information to ascertain if computer, etc., fulfils criteria of system of temporary cybersecurity concern

2.—(1) For the purposes of section 17A(2) of the Act, a notice to provide relevant information to the Commissioner under that provision must be given in writing in the form set out on the Internet website at https://www.csa.gov.sg.

(2) The Commissioner may by notice under section 17A(2) of the Act require a person who appears to be exercising control over a

computer or computer system, to provide to the Commissioner the following information relating to that computer or computer system as is relevant for the purpose of ascertaining whether the computer or computer system fulfils the criteria of a system of temporary cybersecurity concern:

(*a*) the name and location of the computer or computer system;

(*b*) the function that the computer or computer system is employed to serve;

(*c*) the type of service (if applicable) that the computer or computer system has a role in making available in Singapore, and the role performed by the computer or computer system;

(*d*) the person or persons, or other computer or computer systems, that the computer or computer system mentioned in the notice serves;

(*e*) information relating to the design of the computer or computer system, including the parameters and key components of the computer system, as specified in the notice;

(*f*) if the computer or computer system is a virtual computer or virtual computer system, information relating to the physical computing resources used for the simulation of the virtual computer or virtual computer system, including identifying information relating to the cloud computing service provider where the physical computing resources used for the simulation of the virtual computer or virtual computer system are provided by a cloud computing service provider;

(*g*) the name, address, contact and business registration number (if applicable) of the person to whom the notice is given;

(*h*) if the person to whom the notice is given is not the owner of the computer or computer system, the name, address, contact and business registration number (if applicable) of the owner;

(*i*) any other information that the Commissioner may require in order to ascertain whether the computer or computer system fulfils the criteria of a system of temporary cybersecurity concern.

(3) In this regulation, "location", in relation to a computer or computer system that is a virtual computer or virtual computer system, means the location of the physical computing resources deployed for the simulation of the virtual computer or virtual computer system.

Information relating to system of temporary cybersecurity concern

3.—(1) For the purposes of section 17D(1) of the Act, a notice to the owner of a system of temporary cybersecurity concern to furnish information required under that provision must be given in writing in the form set out on the Internet website at https://www.csa.gov.sg.

(2) The Commissioner may by notice under section 17D(1) of the Act require the owner of the system of temporary cybersecurity concern to provide to the Commissioner —

(*a*) the following information on the design, configuration and security of the system of temporary cybersecurity concern:

(i) a network diagram depicting every key component and interconnection in the system of temporary cybersecurity concern, and any external connection and dependency that the system of temporary cybersecurity concern may have;

(ii) for every key component in the system of temporary cybersecurity concern, the following details:

(A) its name and description;

(B) its physical location;

(C) any operating system and version;

(D) any key software and version;

(E) its internet protocol address and any open port, if the component is internet facing;

(F) the name and address of the operator, if the owner is not the operator;

(iii) the types of data processed on or stored in the system of temporary cybersecurity concern;

(iv) the name and contact of every individual having overall responsibility for the cybersecurity of the system of temporary cybersecurity concern;

(*b*) the following information on the design, configuration and security of any other computer or computer system under the owner's control that is interconnected with or that communicates with the system of temporary cybersecurity concern:

(i) the name and description of that other computer or computer system;

(ii) the physical location of that other computer or computer system;

(iii) the name and address of its operator, if the owner is not the operator;

(iv) a description of any function provided by that other computer or computer system;

(v) the types of data exchanged with the system of temporary cybersecurity concern;

(vi) the operating system and version;

(vii) the key software and version;

(viii) how that other computer or computer system is interconnected with or communicates with the system of temporary cybersecurity concern, including the communication protocol of that other computer or computer system with the system of temporary cybersecurity concern;

(*c*) the name of any outsourced service provider supporting the system of temporary cybersecurity concern, and the nature of the outsourced service; and

(*d*) any other information that the Commissioner may require in order to ascertain the level of cybersecurity of the system of temporary cybersecurity concern.

(3) In this regulation, "physical location" —

(*a*) in relation to a key component of a system of temporary cybersecurity concern that is a virtual computer or virtual computer system, means the physical location of the physical computing resources deployed for the simulation of the key component of the virtual computer or virtual computer system; or

(*b*) in relation to a computer or computer system that is a virtual computer or virtual computer system, means the physical location of the physical computing resources deployed for the simulation of the virtual computer or virtual computer system.

Report of cybersecurity incident in respect of system of temporary cybersecurity concern

4.—(1) For the purposes of section 17F(1) of the Act, where a cybersecurity incident mentioned in section 17F(1)(*a*), (*b*) or (*c*) of the Act occurs, the owner of a system of temporary cybersecurity concern must notify the Commissioner of the occurrence of the cybersecurity incident in the following form and manner:

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

(i) the system of temporary cybersecurity concern which the cybersecurity incident relates to;

(ii) the name and contact number of the owner of the system of temporary cybersecurity concern;

(iii) the nature of the cybersecurity incident, whether it was in respect of the system of temporary cybersecurity concern or an interconnected computer or computer system, and when and how it occurred;

(iv) the resulting effect that has been observed, including how the system of temporary cybersecurity concern or any interconnected computer or computer system has been affected;

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

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

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

(ii) the cause of the cybersecurity incident;

(iii) the impact of the cybersecurity incident on the system of temporary cybersecurity concern or any interconnected computer or computer system, or on the business operations of the owner of the system of temporary cybersecurity concern;

(iv) what remedial measures have been taken;

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

(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 details mentioned in paragraph (1)(*a*) must be submitted —

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

(*b*) if the owner 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 on the Internet website at https://www.csa.gov.sg, to the electronic address specified by the Commissioner.

(3) For the purposes of section 17F(1)(*a*), (*b*) and (*c*) of the Act, the following are prescribed cybersecurity incidents in respect of a system of temporary cybersecurity concern or an interconnected computer or computer system:

(*a*) any unauthorised hacking of the system of temporary cybersecurity concern or the interconnected computer or computer system to gain unauthorised access to or control of the system of temporary cybersecurity concern or interconnected computer or computer system;

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

(*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 temporary cybersecurity concern or the interconnected computer or computer system, and an authorised user of the system of temporary cybersecurity concern or the interconnected computer or computer system, as the case may be;

(*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 temporary cybersecurity concern or the interconnected computer or computer system.

(4) In this regulation —

"interception", in relation to a communication to or from a system of temporary cybersecurity concern or an interconnected computer or computer system, includes —

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

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

"interconnected computer or computer system" means any computer or computer system under the control of the owner of a system of temporary cybersecurity concern, or under the control of a supplier to the owner, that is interconnected with or that communicates with the system of temporary cybersecurity concern.

Made on 13 October 2025.

JOSEPH LEONG WENG KEONG
Permanent Secretary
(Cybersecurity),
Prime Minister's Office,
Singapore.

[CSA.0007.200003; 2020-1629; AG/LEGIS/SL/70A/2020/5]