Premier and Cabinet Circular

PC042 – CYBER SECURITY INCIDENT MANAGEMENT

Effective from September 2024

Contents

Purpose

This circular outlines how agencies are required to report, manage and respond to cyber security incidents in coordination with the Department of Treasury and Finance (DTF) as both the Hazard Risk Reduction Leader and Control Agency for Cyber Crisis.

Context

Under the *Emergency Management Act 2004* (the Act), the Department of Treasury and Finance (DTF) is designated as the Hazard Risk Reduction Leader and Control Agency for Cyber Crisis. Cyber Security, Office of the Chief Information Officer (OCIO), DTF, is responsible for these roles.

As the Hazard Risk Reduction Leader, DTF coordinates the comprehensive planning process relating to cyber hazards (risk prevention, preparedness, response and recovery).

As the Control Agency for Cyber Crisis, DTF is responsible for taking control of a response to cyber emergencies, which can include tasking and coordinating other agencies in accordance with the needs of the situation.

Authority and accountability

This circular applies to all South Australian Government public sector employees and organisations or individuals providing services to government agencies.

When an emergency is declared under the Act, the powers and functions of authorised officers supersede those in this circular.

Chief Executives must ensure their agency reports suspected incidents to the South Australian Government Cyber Security Watch Desk (the Watch Desk).

Agency Security Executive's and IT Security Advisers are expected to oversee the development and management of their agency's reporting processes.

Application

Cyber Security reporting, obligations and procedures

Agencies are required to have current procedures in place to:

- address requirements of the SA Protective Security Framework and SA Cyber Security Framework (SACSF)
- manage and report cyber security events and incidents, including reporting to the Watch Desk – *refer to contact details on page 5*.

Reporting cyber security events and incidents to the Watch Desk:

- ensures DTF has an accurate, up-to-date understanding of threats and issues.

- ensures critical events are identified and responded to as soon as possible
- helps DTF deliver on its obligations as the Control Agency for Cyber Crisis under the South Australian emergency management arrangements.

Cyber security incident reporting under this circular works in parallel with agencies' own internal processes and should not be considered a substitute for internal incident management responsibilities.

Note: guidance on terms, abbreviations and how to report cyber security incidents to DTF is in the SACSF and the Control Agency for Cyber Crisis Incident Management Framework (the Framework).

Working with the Hazard Risk Reduction Leader and Control Agency for Cyber Crisis

As the Cyber Crisis Hazard Risk Reduction Leader, DTF is responsible for overseeing the comprehensive planning process relating to a cyber crisis. To achieve this, it has the authority to bring together any required Commonwealth, state, local or non-government entities needed, including those with roles and functions outlined in the State Emergency Management Plan (SEMP)[1].

If there is a threat or incident, the Control Agency will determine the appropriate level and nature of response as per the Framework.

The State Controller[2] (or Deputy) and the SA Government Chief Information Security Officer[3] (or Deputy) of the Control Agency for Cyber Crisis can direct workers of an agency, supplier or non-government personnel that provides services[4] to government agencies to act in certain way to prevent, respond to and recover from cyber security incidents being managed under the Framework. Actions may include, but are not limited to:

- accessing or providing access to government information
- directing workers of any agency or supplier to government to conduct actions in a particular manner, such as:
    - stopping any work or operation
    - shutting off or removing any government equipment and/or device that may store or transmit government data

[1] https://www.DTF.sa.gov.au/responsibilities/security-emergency-and-recovery-management/state-emergency-management-plan/State-Emergency-Management-Plan-2022.pdf

[2] The State Controller (a role performed by the Government Chief Information Officer, OCIO, DTF) is responsible for the overall operation of the Control Agency for Cyber Crisis. The State Controller is an Authorised Officer appointed under Section 17 of the Emergency Management Act 2004. In addition to the authority detailed in this Circular, an Authorised Officer has statutory powers under the Emergency Management Act 2004 and will enact these upon the declaration of an identified Major Incident, Major Emergency or Disaster (s25 the Act). A number of Deputy State Controllers are appointed also.

[3] The SA Government Chief Information Security Officer (CISO) is the cyber security lead for SA Government. The CISO is an executive position within Cyber Security, OCIO, DTF, and supports the State Controller in the operation of the Control Agency for Cyber Crisis.

[4] Suppliers won't be directed to undertake action outside of what they are contracted to supply to government.

    - protecting government data, systems and equipment
- participating in a whole of government collaborative incident response effort, including participation in an incident management team, and
- coordinating media and communications.
- coordination of government consequence from a cyber-Incident.
- coordination of cyber threat intelligence

Failure to comply with this circular will be considered as contravention of/failure to comply with a lawful and reasonable direction and thus misconduct. This may be referred to the agency Chief Executive, DTF Chief Executive, the Commissioner for Public Sector Employment or other relevant bodies for disciplinary action.

Exemptions

Any exemption must be approved by Cabinet. The Cabinet Submission needs to outline why the exemption is required, the proposed alternative action and what the agency will do to continue to meet their cyber security obligations.

The Watch Desk must be notified of any submission for exemption via watchdesk@sa.gov.au.

Monitoring and compliance

Under the SACSF, agencies are required to submit annual security attestations to provide an overall update on their cyber security posture and the planned work program to continue to uplift it. This information will be presented to the Senior Leadership Council and Cabinet each year.

Distribution and publication

The circular will be published on the DPC website. Cabinet Office will distribute the circular to all Chief Executives across government.

Document control

Review number: 2.1
Review date: September 2024

Date of approval: May 2020
Next review date: September 2025

For more information

South Australian Cyber Security Watch Desk, Cyber Security, Office of the Chief Information Officer, DTF
T: 1300 244 168

E: watchdesk@sa.gov.au

W: https://www.security.sa.gov.au/