Premier and Cabinet Circular

PC042 – CYBER SECURITY INCIDENT MANAGEMENT

Effective from 1 July 2020

Contents

Premier and Cabinet Circular PC042 Cyber Security Incident Management

This Circular addresses the requirements for Agencies to report, manage and respond to cyber security incidents in coordination with the Control Agency for Cyber Crisis (the Control Agency).

1 Background

1.1 Pursuant to the *Emergency Management Act 2004*, the Department of the Premier and Cabinet (DPC) is designated as the Control Agency for Cyber Crisis. The responsibilities of the Control Agency are managed by the Office for Cyber Security (within ICT and Digital Government, DPC).

1.2 Control Agencies have the responsibility to take control of the response to emergencies of a specific type. Authority for control carries with it the responsibility for tasking and coordinating other organisations in accordance with the needs of the situation.

2 Scope

2.1 This Circular applies to South Australian Government public sector agencies (as defined in the *Public Sector Act 2009* – herein referred to as "Agencies"), suppliers to the South Australian Government, and non-government personnel that provide services to government agencies.

2.2 Should there be a declaration of an emergency under the *Emergency Management Act 2004*, the powers and functions of authorised officers under that Act would supersede those assumed under this Circular.

3 Cyber Security Reporting, Obligations and Procedures

3.1 Agencies must have current security incident management procedures that address requirements of the SA Protective Security Framework and SA Cyber Security Framework (SACSF).

3.2 Agencies must have procedures in place for the management and reporting of cyber security events and incidents, including reporting to the DPC as the Control Agency.

3.3 General guidance on terms, abbreviations and how to report cyber security events and incidents to the DPC is located within the SACSF and the Control Agency for Cyber Crisis Incident Management Framework (the Framework).

3.4 Cyber security incident reporting under this Circular will work in parallel with all agencies own internal processes for incident handling and response and shall not be considered a substitute for internal incident management responsibilities.

3.5 Reporting of cyber security events and incidents to the DPC assists its obligations as the Control Agency for Cyber Crisis under the South Australian emergency management arrangements.

4 Working with the Control Agency for Cyber Crisis

4.1 Agency Chief Executives will be ultimately accountable for their Agency reporting incidents to the Control Agency. Agency Security Executive's and IT Security Advisers would be expected to oversee the development and management of the Agencies reporting process.

4.2 The Control Agency will determine the appropriate level of response as per the Framework.

4.3 The State Controller[1] (or Deputy) and the SA Government Chief Information Security Officer[2] of the Control Agency for Cyber Crisis can direct workers of an Agency, Supplier or non-government personnel that provides services to government agencies to act in a particular manner in the containment of, or response to, cyber security incidents being managed under the Framework. Actions may include, but are not limited to:

a) Accessing or providing access to government information.
b) Directing workers of any agency or supplier to government to conduct actions in a particular manner, which may include:
    i. stopping any work or operation
    ii. shutting off or removing any government equipment and/or device that may store or transmit government data.
    iii. protecting government data, systems and equipment.
c) Participating in a whole of government collaborative incident response effort including participation in an incident management team.

4.4 Failure of an individual to comply with this Circular, will be considered in contravention of/failure to comply with a lawful and reasonable direction and thus misconduct. This may be referred to the agency Chief Executive, DPC Chief Executive, the Commissioner for Public Sector Employment or other relevant bodies for determination of disciplinary action.

5 References

- Premier and Cabinet Circular PC030 – Protective Security Policy Framework
- The South Australian Cyber Security Framework (SACSF)
- Control Agency for Cyber Crisis Incident Management Framework
- *Emergency Management Act 2004*

1 The State Controller (a role performed by the Executive Director, ICT and Digital Government, DPC) 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.

2 The SA Government Chief Information Security Officer (CISO) is the cyber security lead for SA Government. The CISO is an executive position within the Office for Cyber Security, ICT and Digital Government, DPC, and supports the State Controller in the operation of the Control Agency for Cyber Crisis.

Document Control

Review number: 1
Review date: May 2020

Date of approval: 22 June 2020
Next review date: July 2022

For more information

Office for Cyber Security
ICT & Digital Government
T: 1300 244 168

E: OfficeForCyberSecurity@sa.gov.au
W: dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars