Government of South Australia

Department of the Premier and Cabinet Circular

PC042 – Cyber Security Incident Management

January 2016

Table of Contents

1. PURPOSE

1.1 This Circular addresses the requirements for Agencies to manage, report and respond to cyber security incidents in coordination with the Control Agency for ICT Failure.

2. BACKGROUND

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

2.2 Agencies have obligations in the management and reporting of security incidents under ISMF Standard 140 – Across Government Cyber Security Incident Reporting Scheme, where agencies are required to have procedures in place for the management and reporting of security incidents.

3. SCOPE

3.1 This Department of the Premier and Cabinet Circular 'PC042 Cyber Security Incident Management' applies to South Australian Government public sector agencies (as defined in the *Public Sector Act 2009*). Public sector agencies are herein referred to as "Agencies".

3.2 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.

4. AGENCY CYBER SECURITY INCIDENT MANAGEMENT PROCEDURES

4.1 Agencies must have current cyber security incident management procedures that address the requirements of the Protective Security Management Framework (PSMF), Information Security Management Framework (ISMF) Standard 140 Notifiable Incidents – Across Government Cyber Security Incident Reporting Scheme, and this Circular.

5. WORKING WITH THE CONTROL AGENCY FOR ICT FAILURE

5.1 Agency Chief Executives must nominate an executive, and a back-up in the event that the nominated executive is not available (this may or may not be a person acting in the executive's absence), who will be accountable for reporting incidents to the Control Agency for ICT Failure in accordance with the Across Government Cyber Security Incident Reporting Scheme.

5.2 A Duty Executive[1] (or delegate) of the Control Agency for ICT Failure, under the ICT Incident Management Framework and ICT Support Plan, can direct workers of an Agency to conduct in a particular manner in the containment/response to cyber security incidents.

5.3 Failure of an individual to comply with this Circular or 'ISMF Standard 140 Notifiable Incidents - Across Government Cyber Security Incident Reporting Scheme', will be considered contravention of/failure to comply with a lawful and reasonable direction and thus misconduct in contravention of the Code of Ethics, and as such may be

[1] A Duty Executive is defined in the ICT Incident Management Framework as an Executive within the Department of the Premier and Cabinet tasked with the overarching leadership of incident management operations.

referred to both the agency Chief Executive and the Commissioner for Public Sector Employment for determination of disciplinary action.

6. REFERENCES

- Government of South Australia Premier and Cabinet Circular PC030 – Protective Security Management Framework
- Government of South Australia Information Security Management Framework (ISMF)
- ISMF Standard 140 Notifiable Incidents – Across Government Cyber Security Incident Reporting Scheme
- Code of Ethics for the South Australian Public Sector
- *Emergency Management Act 2004*
- ICT Support Plan