SACSF/R2.0

GOVERNMENT RULING ON CYBER SECURITY

SACSF Ruling 2 - Storage and processing of South Australian Government information in outsourced or offshore ICT arrangements

Background

Chief executives have ultimate accountability for all security matters within their agencies. Such accountability is derived from Cabinet Circular No. 30, the Protective Security Framework amended from time to time.

The South Australian Cyber Security Framework (SACSF) provides a framework for an assured information security environment, utilising risk management and other processes and principles stipulated in the PSMF.

The SACSF applies to all Official Information, and all information of which the South Australian Government or any of its Agencies has custody, where that information is processed, stored or communicated by ICT equipment.

Purpose

What this ruling is about:

- it describes how South Australian Government information is managed in alignment with the Cabinet approved expectations stipulated in the Protective Security Framework
- it identifies certain restrictions and considerations that apply to South Australian Government information when considering an offshore ICT arrangement.

Ruling

South Australian Government information may be outsourced or offshored in ICT arrangements subject to a risk assessment being undertaken that considers the three dimensions of classification and protective (or dissemination limiting) markings that are described by the Protective Security Framework, specifically Confidentiality, Availability and Integrity requirements. The ultimate decision to accept or tolerate residual risks associated with outsourcing and offshoring arrangements remains with the Agency Chief Executive, as stated in the Protective Security Framework.

Is there any information that cannot be outsourced or offshored?

Security Classified Information that uses Protective Markings

Information that is PROTECTED, SECRET or TOP SECRET cannot be processed or stored outside of Australia. Personnel including those working for or operating on behalf of suppliers must have a corresponding security vetting (a.k.a. clearance) to work with or maintain associated systems and services with this information.

Critical Services

Critical Services may have an extremely high Availability or Integrity classification. In such instances, it is a matter for the agency to assure itself that the proposed arrangements will meet these requirements.

Information about State Government Critical Information Infrastructure (SGCII), including metadata, cannot be stored offshore in whole of government purchasing arrangements without the express written consent of the State's Principal Contract Administrator. (Refer extracted clause 43.8 from the State's purchasing agreements below)

Critical Services can be categorised as either Essential or Important:

Essential Services

- Essential Services are those services (whether provided by a public or private undertaking) without which the safety, health or welfare of the community or a section of the community would be endangered or seriously prejudiced[1].

  Essential Services are directly related to:

  - continuity of executive government
  - directly combating identified threats
  - physical survival of the community

Important Services

- Important Services are those services that are directly related to the social, physical or economic safety and security of the State.

Provisions for location of information and associated services in whole of government purchasing arrangements

There are certain provisions embedded in whole of government ICT purchasing agreements to establish restrictions on location of information while maintaining flexibility for individual agencies to manage their information and its location effectively. In effect, the premise applied by these clauses is that Security Classified Information (i.e. PROTECTED and higher) and Information including metadata about SGCII cannot be stored offshore without express written consent of the State Principal Contract Administrator, and that other agency information cannot be stored offshore without the consent of the relevant Agency chief executive. The following clauses within Schedule 17 of the eProjects panel agreement are demonstrative of whole of government ICT services arrangements:

[1] South Australian Essential Services Act, 1981

Location and Storage of Data

- The Supplier must not send or store State Data, Customer Data, Personal Information, other related data/information that uses or requires the use of '*protective markings*' as described in the Protective Security Framework (i.e. security classified information) outside of Australia.
- The Supplier must not send or store State Data, Customer Data, or other related data or information associated with State Government Critical Information Infrastructure outside of Australia without the express written consent of the State's Principal Contract Administrator. The approval of the State's Principal Contract Administrator may be given conditionally.
- If the State's Principal Contract Administrator does not provide an unconditional approval under clause 43.8, then the Parties must, at either Party's request, negotiate with a view to resolving the issues that arise for the Supplier because of the withholding of the approval, or the imposition of conditions, as the case may be.
- The Supplier must not send or store Customer Data outside of Australia without the express written consent of the Customer's chief executive (or his or her delegate). The approval of the Customer's chief executive (or his or her delegate) may be given conditionally.
- If the Customer's chief executive (or his or her delegate) does not provide an unconditional approval under clause 43.10, then the Customer and the Supplier must negotiate with a view to resolving the issues that arise for the Supplier because of the withholding of the approval, or the imposition of conditions, as the case may be.

Furthermore, individual Customer Agreements acknowledge the above provisions from the Purchasing Agreement by way of the clause below:

Location and Storage

- The Supplier acknowledges that the requirements of clauses 43.7, 43.10 and 43.11 of the Purchasing Agreement apply in respect to Customer Data.

References, links and additional information

- PCO30 Protective Security Management Framework
- South Australian Cyber Security Framework
- Information Privacy Principles Instruction (Cabinet Administrative Instruction 1/89) issued as Premier and Cabinet Circular No. 12
- Australian Government Protective Security Policy Framework (PSPF)

Document Control

ID	SACSF\R2.0 *Previously DPC/R4.2*
Version	v1.4
Classification/DLM	OFFICIAL
Compliance	Mandatory
Original authorisation date	November 2019 (minor changes only, under review)
Last approval date	November 2019 (minor changes only, under review)
Next review date	January 2020