Office of the Registrar General - Mandatory Minimum Specifications

Data Access Regime Value Added Resellers (VAR)

Subject to the terms and conditions of a VAR Licensee's Data Access Sub-Licence Agreement (Data Sub-Licence), the State of South Australia's (the State) mandatory minimum specifications for VAR Licensees are set out below.

VAR Licensee's must at all times:

A. be compliant with the South Australian Cyber Security Framework (SACSF);
B. have satisfactorily passed a technical security audit; and
C. ensure that those whom obtain access to or use of the State's data via a VAR, such as its customers and contractors (Downstream Users) are informed of, comply with and do not breach a VAR Licensee's Data Sub-Licence.

VAR Licensees must ensure that their data security arrangements protect State data from unauthorised access and ensure that it is not collected, held, used, disclosed, stored and processed in a manner contrary to the terms of the Data Access Sub-Licence Agreement and applicable laws.

Without limitation and before the commencement of a VAR Licensee's Data Sub-Licence, a VAR Licensee must ensure that:

1 Information Security Management Systems (ISMS)

The VAR Licensee has established an Information Security Management System that conforms to the principles of AS/NZS ISO/IEC 27001 (AS 27001).

The scope of the ISMS (processes, systems and geographic locations) must be documented and include a Statement of Applicability as defined under AS 27001, as follows "Statement of Applicability" is a documented statement describing the control objectives and controls that are relevant and applicable to the VAR Licensee's ISMS.

2 Information Security Policy

The VAR Licensee has established an Information Security Policy document that is approved by its Senior Management, which includes a commitment to the protection of information and sets out their approach to managing information security. The policy must, at a minimum implement the control(s) described in clause A.5 of AS 27001.

3 Classification requirements

The VAR Licensee has classified the information in the State data to suitably reflect its importance, degree of sensitivity and protection requirements, and specified when such classifications must be periodically reviewed.

Once assigned a classification, the information must be appropriately handled to adhere to protection controls for confidentiality, integrity and availability as well as any other special handling measures applicable to the defined classification of the information.

The classification of each information asset must be documented and align with clause 6.6.2 of the AS ISO/IEC 20000.2 standard encompassing service management.

4 Workforce Management Security

The VAR Licensee has undertaken security checks on its personnel and established a process for undertaking the same at the recruitment stage and periodically during an individual's engagement.

The VAR Licensee's personnel have been adequately screened, commensurate to the sensitivity of information being handled.

The VAR Licensee has defined its personnel's security roles and responsibilities in accordance with its information security policy and ensure that information security policies are readily accessible and formally communicated to all of its personnel on a periodic basis.

5 Access Control

The VAR Licensee has established and documented its business requirements, policies and guidelines to implement access control mechanisms for its information assets.
The access control mechanisms for an information asset reflect the value of the asset to the VAR Licensee and any specific privacy or other information privacy requirements necessary based on the nature of the asset.

A VAR Licensee has implemented the control(s) and must implement the guidance described in clause 11.1.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 9.1.1 of the ISO/IEC 27002:2013 standard).

6 Protection of the Data

The VAR Licensee has established policies and procedures to ensure that access to State data supplied pursuant to its Data Sub-Licence does not compromise in any way the security and integrity of the State data or the privacy of any personal information, so that it is not:

- Accessed by any unauthorised person(s); or
- Modified or reconstituted in any way, other than as contemplated by the Data Sub-Licence.

Ensure that the warning and copyright statement as set out in in the Data Sub-Licence (clause 3.3) are displayed on all copies of the State data.

7 Privacy

The VAR Licensee's collection, holding, use, disclosure, storage and processing of personal information provided to, accessed or acquired by the VAR in connection with the Data Sub-Licence:

- Complies with all Privacy Laws;
- Complies with any requirements specified by the State relating to personal information from time to time;
- Complies with the Information Privacy Principles as if the VAR Licensee and Downstream Customers were entities to which the Information Privacy Principles apply; and
- Does not cause the VAR Licensee or a Downstream Customer to breach any obligations it owes in respect of Personal Information, including under any Privacy Law the Information Privacy Principles.

Privacy Law means:

- the *Privacy Act 1988* (Cth);
- the Australian Privacy Principles under the *Privacy Act 1988* (Cth); and
- any other Law or guideline, order or direction made by a Government agency or other authorised body under any Law relating to privacy, data protection, surveillance, direct marketing, data security or the handling of personal information or data.

Information Privacy Principles means the State of South Australia's PC012 - Information Privacy Principles (IPPS) Instruction dated 20 June 2016, as updated, amended or superseded from time to time.