Security obligations for contracted service providers (social services)

Introduction

The Department of Children, Youth Justice and Multicultural Affairs (the department) partners with contracted service providers (contractors) to deliver services. The *Service Agreement - Standard Terms* creates certain obligations on contractors in the social services context, including in relation to information privacy, confidentiality, record-keeping, and information security.

Clause 18 requires contractors to comply with the *Information Privacy Act 2009* which includes the obligation in Information Privacy Principle 4 – *Storage and security of personal information* to ensure that documents containing personal information are protected against loss, unauthorised access, use, modification or disclosure, and any other misuse.

In addition, clause 18 of the Service Agreement provides:

> *18.1 If You collect or have access to Personal Information[1] for the purposes of the Service Agreement, You must: …*
>
> *(i) comply with such other privacy and security measures as We reasonably notify You about from time to time.*

What security standards?

The department is required to comply with Information Standard 18 (IS 18:2018) and ISO 27001 and expects that contractors will provide an equivalent level of security in relation to the personal and confidential information they handle.

Resources

Guidance about how to meet these obligations is available from many sources, including:

1. Australian Cyber Security Centre

The Australian Cyber Security Centre (ACSC) is based within the Australian Signals Directorate (ASD) and provides advice to individuals, small and medium organisations, large enterprises and government about how to protect your business online.

This guidance includes strategies about how to prevent and respond to cyber incidents, ensure appropriate levels of education and awareness for your workforce, managing supply chain risks, and communicating the importance of good cyber security to executives and customers.

For example:

- *Advice and guidance for small and medium organisations*
- *Advice and guidance for large organisations*
- *The Essential Eight (baseline mitigation strategies)*

[1] *Personal information* is information or opinion (including information or opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion (s12 *Information Privacy Act 2009*).

2. Office of the Information Commissioner

The Queensland Office of the Information Commissioner (OIC) is an independent statutory body whose functions include promoting information privacy in the community and within government.

The OIC provides a range of online services and information and resources to help community and government understand their rights and responsibilities under the IP Act. The OIC provides information and advice about privacy through their enquiries service and their website.

OIC publications about information security include:

- *Security, accuracy and relevance*
- *Basic guide to IPP4*
- *Protection and security of personal information*
- *Portable storage devices and information privacy*
- *Achieving effective privacy and information security training*
- *Cloud computing and the privacy principles*
- *Mobile apps and services on smart devices*
- *Sending personal information out of Australia*
- *IP addresses, Google Analytics and the privacy principles*

3. Office of the Australian Information Commissioner

The Office of the Australian Information Commissioner (OAIC) has functions in relation to promoting and upholding privacy and information access rights under the federal *Privacy Act 1988* (Cth). The OAIC provides information and advice about privacy to individuals, businesses and government agencies through their enquiries team and their website.

Although your contract requires you to comply with the Queensland *Information Privacy Act 2009,* some of the guidance provided on the OAIC website may be useful, particularly if you are otherwise required to comply with the federal Privacy Act. For example:

- *Guide to securing personal information*
- *Privacy management framework: enabling compliance and encouraging good practice*