ISOPro Privacy & Client Data Sovereignty Statement

ISOPro is aware of the following laws related to privacy and information security:

- Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act of 2012
- The Australian Privacy Principles outlined in the Act and Regulations
- The Notifiable Data Breaches under Part IIIC of the Privacy Act
- NSW Child Protection (Working with children) Act 2012 (and similar of the various States)

ISOPro makes no claim of ownership of client data.

We act in the capacity of a cloud service provider for the limited purpose of performing the services of storing and ensuring the client may access their information including personal information of employees and clients.

Under the Australian Privacy Act and Principles

Under the Australian Privacy Principles, ISOPro is not an APP Entity and is therefore not subject to the requirements of the Act and Regulations.

Under B.144 of the Regulations, as applicable to the APP (i.e. ISOPro's client):
In limited circumstances, providing personal information to a contractor to perform services on behalf of the APP entity may be a **use**, rather than a **disclosure** (see paragraph B.63–B.68). This occurs where the entity does not release the subsequent handling of personal information from its effective control.

For example, if an entity provides personal information to a cloud service provider for the limited purpose of performing the services of storing and ensuring the entity may access the personal information, this may be a 'use' by the entity in the following circumstances:

- a binding contract between the entity and the provider requires the provider only to handle the personal information for these limited purposes
- the contract requires any subcontractors to agree to the same obligations, and
- the contract gives the entity effective control of how the information is handled by the provider.

Issues to consider include whether the APP entity retains the right or power to access, change or retrieve the information, who else will be able to access the information and for what purposes, the security measures that will be used for the storage and management of the personal information (see also APP 11.1, Chapter 11) and whether the information can be retrieved or permanently deleted by the entity when no longer required or at the end of the contract.

Under the Notifiable Data Breaches (NDB) Scheme

Under our ISO27001 certification-related procedures, ISOPro binds itself to advise a client, as soon as practically possible, of any information security event including a suspected or actual data breach. This is part of ISOPro's Security Incident Response Procedure.

With regards to the NDB Scheme.

- The client is the" APP Entity"

  The NDB Scheme is only applicable to APP entities that meet NBD Scheme eligibility criteria
- The Personally Identifiable Information (PII) held by ISOPro does not belong to ISOPro but to the client under
- The ISOPro service delivery agreement.
- Under the client agreement, ISOPro is a "cloud service provider for the limited purpose of performing the services of storing and ensuring the (APP) entity may access the personal information".

Consequently, ISOPro cannot report Notifiable Data Breaches to the Office of the Australia Information Commissioner (OAIC) and the obligation falls on the client (unless they do not meet the eligibility criteria). ISOPro will work closely with the client to jointly prepare and will contractually bind itself to support the client's data breach response plan.

Under various Working with Children Acts

In the event of a client retaining PII of under-age persons, ISOPro staff, who may have access to the information, are not deemed to carry out "child-related work" as defined by Section 6 of the NSW Child Protection (Working with children) Act 2012 (or similar State Acts) and are exempt from requiring a Working with Children clearance.

Client USER and USER SESSION information ISOPro holds

USER INFORMATION

Client staff, contractors and others who are ISOPro system users are controlled by the client's System Administrators.
The contact information held in ISOPro for the sole purpose of verification and access to the system is:

- First name (must be unique)
- Surname
- Email address (must be unique).

SESSION INFORMATION

In addition to these details, ISOPro logs the following info during each user session:

- IP address (which may be used to determine approximate geolocation)
- Browser Agent
- Screen size, operating system, browser language setting, device details
- For mobile devices: Device name, Device Identifier, Model, Make, Operating System

Other contractual obligations

Only users authorised by ISOPro's top management have access to client's ISOPro-based data.
These staff members are identified by name and approved by the client System Administrators via our "Information Security Agreement".
These agreements are reviewed regularly and clients are advised of all staff changes related to their data.
Clients can withhold approval on reasonable grounds.

ISOPro will not release or divulge ISOPro-based client information to any 3 rd party, other than as required by law, without the written permission of the client's authorised representative(s) as identified in the "Information Security Agreement" or as formally provided by the client.