Privacy and Personal Data Protection Policy

DOCUMENT CLASSIFICATION	Public
DOCUMENT REF	ISMS-DOC-A18-5
VERSION	1.0
DATED	14 September 2023
DOCUMENT AUTHOR	M Parker
DOCUMENT OWNER	Managing Director

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
1.0	14/09/23	Peter Sanderson	Conversion of ISO Policy for web use

Distribution

NAME	TITLE
All staff and contractors	

Approval

NAME	POSITION	SIGNATURE	DATE

Contents

Tables

1 Introduction

In its everyday business operations OneTeam IT makes use of a variety of data about identifiable individuals, including data about:

- Current, past and prospective employees
- Customers
- Users of its websites
- Subscribers
- Other stakeholders

In collecting and using this data, the organisation is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

The purpose of this policy is to set out the relevant legislation and to describe the steps OneTeam IT is taking to ensure that it complies with it.

This control applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to OneTeam IT systems.

The following policies and procedures are relevant to this document:

- Information Classification Procedure
- Information Labelling Procedure
- Records Retention and Protection Policy
- Acceptable Use policy
- Electronic Messaging Policy
- Internet Acceptable Use Policy
- Information Security Incident Response Procedure
- Information Security Roles, Responsibilities and Authorities

2 Privacy and personal data protection policy

2.1 The General Data Protection Regulation

The Australian Privacy Act 1988 (APA) is one of the most significant pieces of legislation affecting the way that OneTeam IT carries out its information processing activities. Significant fines are applicable if a breach is deemed to have occurred under the APA, which is designed to protect the personal data of citizens of Australia. It is OneTeam IT's policy to ensure that our compliance with the APA and other relevant legislation is clear and demonstrable at all times.

2.2 Definitions

Personal information is defined as: *"any information or an opinion relating to an identified or identifiable natural person (''individual'); whether or not the information or opinion is true and whether or not the information is recorded in material form.*

Unlike British Law, there is no distinction between holding or processing the information. The exception to this is where an individual holds personal information relating to their household affairs.

2.3 Australian Privacy Principles

There are a 13 Privacy Principles listed within AP Act 1988 – the Summary definitions with respect to these principles are as follows:

APP 1 — Open and transparent management of personal information Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 — Anonymity and pseudonymity Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 — Collection of solicited personal information Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4 — Dealing with unsolicited personal information Outlines how APP entities must deal with unsolicited personal information.

APP 5 — Notification of the collection of personal information Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 — Use or disclosure of personal information Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 — Direct marketing An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 — Cross-border disclosure of personal information Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 — Adoption, use or disclosure of government related identifiers Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

APP 10 — Quality of personal information An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 — Security of personal information An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 — Access to personal information Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 — Correction of personal information Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

2.4 Principles relating to processing of personal data

There are several fundamental principles upon which the APA is based.

These dictate that personal data shall be:

1. **Processed** lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').
2. **Collected** for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation').
3. **Adequate**, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').
4. **Accurate** and, where necessary, kept up to date ('accuracy')
5. **Kept** in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation').
6. **Processed** in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against

accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

In addition, the entity shall be responsible for and be able to demonstrate compliance with all of these principles ('accountability').

OneTeam IT must ensure that it complies with all these principles both in the processing it currently carries out and as part of the introduction of new methods of processing such as new IT systems. The operation of an information security management system (ISMS) that conforms to the ISO/IEC 27001 international standard is a key part of that commitment.

2.5 Rights of the individual

The data subject also has rights under the APA. These consist of:

- The right to be notified of collection
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Each of these rights must be supported by appropriate procedures within OneTeam IT that allow the required action to be taken within the timescales stated in the APA.

These timescales are shown in Table 1.

DATA SUBJECT REQUEST	TIMESCALE
The right to be informed	When data is collected or as soon as practicable after the data is collected
The right of access	Within a "reasonable period" after the request is made
The right to rectification	Within a "reasonable period" after the request is made

Table 1: Timescales for data subject requests

2.6 Consent

Unless it is necessary for a reason allowable in the APA, consent must be obtained from a data subject to collect and process their data. This may be the individual or a responsible person if the individual is a child under the definition of the Family Law Act. Transparent information about our usage of their personal data must be provided to individuals at the time that consent is obtained and their rights regarding their data explained, such as the

right to withdraw consent. This information must be provided in an accessible form, written in clear language and free of charge.

If the personal data are not obtained directly from the data subject, then this information must be provided within a reasonable period after the data are obtained.

2.7 Transfer of personal data

Transfers of personal data outside the Australia must be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the APP 8.

It may be necessary for specific contractual terms to be used to cover international transfers. Where possible, these should be based upon standard contractual clauses (SCCs) made available by the relevant authority.

2.8 Breach notification

It is OneTeam IT's policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the APA and the process outlined in *Personal Data Breach Notification Procedure*, where a breach is known to have occurred which is likely to result in a risk of serious harm to individuals, the relevant supervisory authority will be informed within 30 days. This will be managed in accordance with our *Information Security Incident Response Procedure* which sets out the overall process of handling information security incidents.

2.9 Addressing compliance to the Aust.InformationCommissioner

The following actions are undertaken to ensure that OneTeam IT complies at all times with the accountability principle of the Privacy Act 1988:

- The legal basis for processing personal data is clear and unambiguous
- All staff involved in handling personal data understand their responsibilities for following good data protection practice
- Training in data protection has been provided to all staff
- Rules regarding consent are followed
- Routes are available to individual wishing to exercise their rights regarding personal data and such enquiries are handled effectively
- Regular reviews of procedures involving personal data are carried out
- The following documentation of processing activities is recorded:
- Organisation name and relevant details
- Purposes of the personal data processing
- Categories of individuals and personal data processed
- Categories of personal data recipients
- Personal data retention schedules
- Relevant technical and organisational controls in place

These actions will be reviewed on a regular basis as part of the management review process of the information security management system.

2.10 Our obligations as a cloud service provider

In addition to holding personal data on our own account, OneTeam IT also stores and processes the personal data of our cloud customers. In doing so, there are a number of additional obligations that must be fulfilled to allow our customers to stay within the law. Our policy in this area is informed by ISO/IEC 27018 – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors which, as well as recommending specific enhancements to ISO/IEC 27001 controls, also provides the following policy guidance:

- We must provide our customers with the facilities to meet their obligations under law in activities such as accessing, amending and erasing individuals' PII
- We must only use the cloud customer's PII for their purposes, not our own
- The customer must be informed if we are required by law to disclose any of their data, unless we are prohibited from doing so
- Details of disclosures must be recorded
- We must tell our customers if we use sub-contractors to process their PII
- We must tell our customers if their PII is subject to unauthorized access
- It must be clear in which country or countries the customer's PII is stored

Additional recommendations stated in ISO/IEC 27018 are also included in the relevant policies and procedures within the ISMS.