Information Security Policy

Version No.:	2.0
Version date:	February 2022
Review date:	February 2025
Policy owner:	Director Finance

1 Purpose

The purpose of this policy is to:

1.1 protect personal information that Unison holds or that is accessed by Unison staff from government agency databases, from misuse, interference, loss or unauthorised access, modification and disclosure.

2 Scope

2.1 This policy applies to all Unison staff, including employees, contractors and volunteers.

2.2 Unison must comply with the *Privacy Act 1988* (Cth) and the Australian Privacy Principles (APPs) outlined therein, particularly APP 11 – Data security.

2.3 Through contractual agreements with DFFH in Victoria, Unison is also mandated to comply with the Information Privacy Principles (IPPs) under the P*rivacy and Data Protection Act 2014* (Vic) (PDP Act) and the Health Privacy Principles (HPPs) under the *Health Records Act 2001* (Vic). This particularly applies to personal information contained in systems managed by Government agencies and accessed by Unison staff, including;

- **a** Specialist Homelessness Information Platform (SHIP) – client management system for IAP and PRAP;
- **b** Victorian Housing Register (VHR);
- **c** Housing Integrated Information Program (HiiP);
- **d** Centrelink.

3 Policy Statement

Principles.

3.1 Unison acknowledges that security to protect personal information from being handled inappropriately is necessary to ensure privacy of personal information. Security will be achieved through:

- **a** Requiring that staff do not share their credentials with anyone else, so only authorised people can view, create, amend or delete information;
- **b** Training staff to use systems necessary to perform their work so data integrity is maintained;
- **c** Ensuring only authorised people have access to personal information held in Government agency systems, for approved purposes

d Working with our contracted IT Management services provider to protect Unison-managed systems from misuse, interference or unauthorised access

e Monitoring staff user accounts and user permissions to ensure all users are legitimate and active

Application.

3.2 Data Security

Unison applies the Risk Management Framework to all parts of the business including information security, and takes a proactive approach to identify, assess and manage Information Communication Technology (ICT) risks.

The Director Finance holds overall accountability for data security, but the Business Systems Administrator and Unison's contracted IT Management Services provider are responsible for the management and monitoring of systems and processes linked to data security.

Processes in place to effectively manage data security include:

a Cloud based environment allowing secure and reliable access to business applications from anywhere

b Software security: business applications hosted in secure data centres not accessible to end users, and end users unable to download software

c Patch management of servers: latest security patches from Microsoft applied as they become available

d Passwords policy, forcing users to change to a new password that must satisfy the password complexity requirements at a set frequency

e Controlled Multi Factor Authorisation access to systems

f Issue of standard devices (phone and computers) and phasing out of BYO device for work purposes. Laptops and Desktops encrypted with BitLocker

g Antivirus: the environment is protected from virus and malware infection using Bitdefender as provided by KMT Group. The software is configured to actively scan files on access, along with scheduled daily scans of common file locations

h Spam filters on emails

i Advanced Threat Protection (ATP)

j Business Continuity Planning for disruption due to or resulting in ICT or system failure

k Regular backups that can be restored quickly (Datto Backupify)

l Oversight and monitoring, including advanced monitoring of security issues (e.g. failed login attempts and virus outbreaks) by contracted IT Management Services provider

m Airwatch Mobile device management to monitor Unison issued mobile devices.

3.3 Permissions

a Access to business applications, and permissions within those applications, is granted based on roles and work requirements.

b The Business System Administrator is responsible for managing and monitoring permissions and access privileges to Unison business applications to ensure users are legitimate and active. The relevant system super-user is responsible for managing and monitoring permissions and access privileges to Government Agency systems (SHIP, HiiP).

3.4 **User Responsibilities**

a All staff are required to comply with the Code of Conduct and Information Communication Technology Use Policy.

b Staff are responsible for maintaining the security of their devices, as well as logins and passwords to both Unison and third-party business applications. All ICT devices must be password protected. Knowingly disclosing passwords to others is considered a serious breach and may lead to disciplinary procedures.

c Staff should also be aware of their responsibilities in relation to appropriate handling, use, sharing and releasing of information – see Information Security Procedure, Information Privacy Policy, and Information Privacy Procedure.

3.5 Information Sharing

a Unison may use or disclose personal information with third-party contractors for a purpose related to the primary purpose of collection, e.g. for the purpose of conducting maintenance or providing 24/7 helpdesk.

b Unison will require that those third-party contractors protect this data from misuse, interference, loss or unauthorised access, modification and disclosure from the time of receipt, and inform Unison immediately should they become aware of a data breach.

3.6 Training and Awareness

a Privacy training, incorporating data security, is mandatory for all staff. Principles will be reinforced regularly, particularly after a data breach incident.

b Staff will be trained in the proper use of business applications required in the course of their job as part of their induction process.

c Contractors will be reminded of their obligations in relation to data security regularly

3.7 Incidents

a Suspected inappropriate or illegal usage of the network, any business application or Unison ICT equipment must be reported to the relevant Manager immediately, who will escalate as appropriate. Any data breach will be managed in accordance with the Privacy – Data breach Management procedure.

b Incidents resulting from system or network failure will be managed in collaboration with our contracted IT Management Services provider and reviewed to ensure Unison learn from them and strengthen/improve systems where necessary to reduce vulnerabilities and exposure to threats.

4 Glossary

Misuse: personal information is misused if it is used in a way that contravenes the Australian Privacy Principles (APPs), namely APP 6 – Use & disclosure, or the Information Privacy Principles (IPPs), namely, IPP 2 – Use and Disclosure.

Loss: personal information is lost where its physical whereabouts is unknown (including both hard and soft copy formats), or there has been a failure to preserve or maintain it. Information that has been intentionally destroyed or de-identified does not constitute a loss.

Unauthorised access, modification and disclosure: accessing information involves viewing it in some form; modification refers to changing, removing or adding components to the original information; and disclosing information involves making it accessible or visible to others. Access, modification or disclosure of information will be regarded as 'unauthorised' where an individual has no authority to access, modify or disclose the information; exceeds their authority by acting beyond their power; or misuses their authority in pursuit of an ulterior motive.

5 Related links

- **a** Charter of Human Rights and Responsibilities Act 2006
- **b** Information Privacy Policy
- **c** Information Privacy Procedure
- **d** Information Privacy – Data breach procedure
- **e** Information Communication Technology Use Policy
- **f** Staff Code of Conduct

6 Review

This policy will be reviewed every three years as delegated by the responsible Executive.