

2023

Public Skills Australia

INFORMATION MANAGEMENT PLAN

Information Management Plan

Purpose

1. To outline the Information Management Plan for the Public Skills Australia Board, CEO, executive team, and staff.

Objectives

2. To outline Public Skills Australia's approach to information management and cyber-security, and the responsibilities of Public Skills Australia Board, CEO, executive team, and staff to comply with these arrangements.

Scope

3. This policy is to be read in conjunction with the Constitution of Public Safety Skills Australia Limited and all Public Skills Australia policies; no policy is a standalone document.
4. All Public Skills Australia policies are to be read in conjunction with following Australian Government Department of Employment and Workplace Relations (DEWR) documents:

Jobs and Skills Councils Code of Conduct

Jobs and Skills Councils Integrity Framework

Jobs and Skills Councils Performance Framework

Jobs and Skills Councils Program Guidelines

Performance and Monitoring Framework (under development)

Training Package Organising Framework (TPOF).

5. All Public Skills Australia policies apply to staff and Company office holders, as well as contractors, subcommittees, networks, and working groups when undertaking work on behalf of Public Skills Australia.

Preferred future state

6. As a newly appointed jobs and skills council (JSC) currently in its establishment phase, the approach to information management and cyber-security will be iterative and dynamic. As the Company grows, ICT systems will be strengthened and developed as required as Public Skills Australia moves into Stage 2 and staff requirements increase.
7. Currently, Public Skills Australia has a service-level agreement (the Agreement) in place with the Australasian Fire and Emergency Service Authorities Council Limited (AFAC). This Agreement includes consultancy and support for a range of functions that will assist in advancing Public Skills Australia to its preferred future state.

8. Public Skills Australia has software, including a Microsoft Office package, email system management, and internet access, at the AFAC offices, via the secure AFAC network. Additionally, Public Skills Australia has purchased IT hardware, such as laptops, keyboards, and mice, for current Public Skills Australia staff, contractors, and secondees.
9. The Agreement currently proposes a range of ICT solutions, which will be organised during the establishment phase:
 - systems architecture, security policies, service level agreements (SLA)
 - cloud-based laptop management
 - Microsoft Defender for Endpoint for threat detection
 - Microsoft 365 for email and collaboration.
10. Public Skills Australia has commenced scoping its preferred future state around ICT systems. This initial discovery phase to understand key information management and security requirements includes the following:
 - Corporate systems – finance, customer relationship management, human resource management. This includes scoping a stakeholder engagement platform in response to the departmental requirement for a feedback register and open consultation.
 - Corporate files and data management – likely via SharePoint as part of the Microsoft tenancy.
 - User and data security – consideration of cyber-related insurance as advised by the Public Skills Australia Company Secretary and industry sectors, such as defence and police, who have training products that are not for public access.
 - The standard operating environment and office facilities – Microsoft software package (E3 or E5) to provide MS Teams, emails and a suite of other Microsoft products. Printing, wi-fi, and internet access will be considered as Stage 2 staff requirements increase.
 - Collaboration tools – access to MS Teams, which is already provided under the current agreement and Microsoft licensing, is the preferred online meeting tool.
 - Website and domain name – currently established, with expansion and further development continuing.
 - Telephony services.
 - Cloud-based infrastructure, including backup, storage, and network environment, which will be situated inside Australia; no data will be transferred or stored outside of Australia.
 - Managed service provider for IT help and support (via the State of Victoria's preferred provider list).
 - Anti-virus and MailGuard requirements.

Public Skills Australia commitments

11. Through its Information Security Management Plan, Public Skills Australia will strive to:

- ensure its information security practices are documented, communicated, and maintained, in compliance with relevant laws and legislation, and manage any issues arising
- understand the security risks to its information assets and business operations, and take precautions comparable with the risks to the business
- ensure Public Skills Australia contractors, subcontractors and external partners manage information in line with this policy.

12. Public Skills Australia will communicate employee responsibilities to employees.

Employee responsibilities

13. Public Skills Australia employees should ensure that they are the first line of defence against information management and cyber-security risks. Public Skills Australia expects employees to:

- access Public Skills Australia information only when there is a legitimate business need
- understand which information is sensitive, and act accordingly and in line with the Public Skills Australia Privacy Policy
- ensure they do not leave sensitive information unattended or accessible to others
- notify the Business Operations Manager immediately if any suspicious activities are observed or if they are concerned that information has been inappropriately accessed
- ensure they are running Public Skills Australia approved software as provided by the Public Skills Australia Agreement.

Reviewing this policy

14. This policy will be reviewed when applicable and within 3 years.