INFORMATION, COMMUNICATION, SECURITY AND TECHNOLOGY (ICST) POLICY

Profluid Pty Ltd ICST Policy sets out the standard of behaviour expected of employees when using ICST services and outlines appropriate behaviour when referring to the company or where employees are identifiable as being associated with the company on external sites. This Policy must be used in conjunction with the Security Policy (DISP).

Profluid Pty Ltd is committed to:

- To comply with the following four requirements of the ASD Essential 8: application whitelisting, patch applications, restrict administrative privileges, and patch operating systems.
- Professional, ethical, and responsible use of ICT at all locations including client premises and afterhours use.
- Providing a safe workplace for management, staff, contractors, and others using the company's ICT facilities.
- Safeguarding the privacy and confidentiality of information received, transmitted, or stored electronically.
- Ensuring that the use of the company's ICT facilities complies with all policies and relevant government legislation.
- Maintaining a Security Register (SR).
- Accountable in ensuring an appropriate system of risk, oversight and management is maintained.
- Ensure any sensitive and classified materials entrusted to Profluid Pty Ltd are safeguarded at all times.
- Facilitating annual security awareness training of personnel.
- Reporting security incidents and fraud incidents, and contact reports.
- Providing management, staff, contractors and others with online information, resources, and communication tools to support the effective operation of the service.

This Policy applies to all aspects of the use of ICT including, but not limited to:

- Internet usage.
- Electronic mail (email).
- Electronic bulletins/ notice boards/ discussion/ news groups.
- Weblogs (blogs)/ social networking/ chat boards.
- File transfer, file sharing and file storage including the use of end-point data storage devices (devices capable of storing information/ data i.e., USB sticks, hard drives, laptops etc.).
- Video conferencing.
- Streaming media.
- Instant messaging.
- Portable communication devices including mobile and cordless phones.

Official information:

- Any Defence related official information is classified in accordance with the Australian Government Security Classification System (AGSCS) and protected in a manner that prevents unauthorized access by or disclosure to, those who do not have a need-to-know and the appropriate security clearance.
- Profluid Pty Ltd personnel using classified material are to ensure that there is no deliberate or casual inspection or oversight by unauthorized persons. All classified material is to be secured in an approved security container when not in actual use or under direct supervision of an appropriately cleared person with a need-to-know.
- A protective marking assigned to official information indicates the consequence of unauthorized disclosure. It identifies the level of protection that must be provided during use.

All personnel and users must comply with all requirements of this Policy. All personnel must be aware of their responsibilities in the protection of information and assets. Any breach of this Policy, within or outside of working hours, may result in disciplinary action which may include termination of employment. Other action that may be taken by the company include, but are not limited to, issuing a warning, suspension, or disconnection of access to all or part of the company's computer network, whether permanently or on a temporary basis.

Our Policy will be made available to any interested party via our website at: https://profluid.com.au/

APPROVED: 29 March 2021
REVISION No.: 0
REVIEWED: 16 November 2023

Jerome Monteiro
Managing Director