Information Security Policy

Flui Technologies Senior Leadership Team fully supports and endorses the establishment of and adherence to all company policies. As Operations Director of this Business Unit, it is my responsibility to ensure the safety, security, resilience, and continuity of Flui Technologies operations.

I ask all employees to familiarise themselves with this policy and actively participate in its implementation and be a part of our commitment to excellence – Grant Cockburn, Operations Director, Flui Technologies.

The confidentiality, integrity and availability of information are critical to the functioning and good governance of Flui Technologies. Failure to adequately secure information increases the risk of financial and reputational losses.

This Information Security Policy outlines Flui Technologies' approach to information security management. It outlines the guiding principles and responsibilities necessary to safeguard the security of the information systems and will be applied to all electronic information assets for which Flui Technologies are responsible. Supporting policies, procedures and guidelines provide further details.

Flui Technologies is specifically committed to preserving the confidentiality, integrity and availability of documentation and data supplied by, generated by and held on behalf of third parties pursuant to the carrying out of work agreed by contract.

Policy Aims:

- Provide an information security framework covering all Flui Technologies' information systems (including but not limited to all Cloud environments, onsite and offsite computers, storage, mobile devices, networking equipment, software, and data) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems. It requires that the resources required to manage such systems will be made available, and that Continuous improvement of Flui Technologies' systems and tools will be undertaken.
- Provide the principles by which a safe and secure information systems environment can be established for staff and any other authorised users.
- Ensure that all users understand their responsibilities for protecting the confidentiality and integrity of the data that they handle.
- Protect the availability of services provided by Flui Technologies to ensure users can access information or systems when needed.
- Protect Flui Technologies from liability or damage through the misuse of its IT facilities.
- Maintain data and other confidential information provided by suppliers at a level of security commensurate with its classification, including upholding any legal and contractual requirements around information security.

Commitment:

- Flui Technologies is committed to protecting the confidentiality, integrity and availability of its information and information systems to minimise the risk of security breaches.
- It is also committed to providing staff education, training and awareness for information security and to ensuring the continued success of the business.
- It is Flui Technologies' Policy that the information it manages shall be appropriately secured to protect against unauthorised access and processing, breaches of confidentiality, failures of integrity or interruptions to the availability of that information and to ensure appropriate legal, regulatory and contractual compliance.
- Flui Technologies is committed to improving software security via development and continuous improvement of secure frameworks.
- Flui Technologies is committed to reviewing asset compliance for Endpoint, Anti-Virus and Patching Compliance to improve cyber resilience within the business.

Responsibility:

- All Flui Technologies' employees, third parties and collaborators on Flui Technologies projects or services will be users of Flui Technologies' information. This carries with it the responsibility to abide by this Policy, any supporting policies, procedures and relevant legislation. No individual should be able to access information to which they do not have a legitimate access right. Notwithstanding systems in place to prevent this, no individual should knowingly contravene this Policy, nor allow others to do so.

Information Security Policy

- Vesta IT and Human Resource teams are responsible for the corporate information systems (e.g. HR/Registry/Finance/IT services), both manual and electronic, that support Flui Technologies' business. This includes ensuring that data is appropriately stored, that the risks to data are appropriately understood and either mitigated or explicitly accepted, that the correct access rights have been put in place, with data only accessible to the right people, and ensuring there are appropriate back-up, retention, disaster recovery and disposal mechanisms in place.

- Project Managers are responsible for the security of information produced, provided, or held in the course of carrying out research, consultancy or knowledge transfer activities. This includes ensuring that data is appropriately stored, that the risks to data are appropriately understood and mitigated, that the correct access rights have been put in place, with data only accessible to the right people, and ensuring there are appropriate backup, retention, disaster recovery and disposal mechanisms.

- Service Owners and Security Leads are responsible for the security of live services.

- The Managing Director signs off Flui Technologies' contracts.

- Infrastructure Engineers are responsible for ensuring that the provision of Flui Technologies' IT infrastructure, Cloud environments and applications is consistent with the demands of this Policy and any other Flui Technologies' security-related policies.

Compliance:

- Information shall be classified according to an appropriate level of confidentiality, integrity and availability and in accordance with relevant legislative, regulatory and contractual requirements. Flui Technologies shall maintain an Information Classification Scheme, detailed in the Information Classification Policy, to help manage and protect its information assets. All data created, received or retained must be protected according to Flui Technologies' approved data classification.

- Flui Technologies recognises the importance of the principle of Least Privilege in managing access to information systems. Flui Technologies will maintain an Access Control Policy. Access controls will be implemented and maintained in accordance with the Access Control Policy. Information should be both secure and available to those with a legitimate need for access in accordance with its classification level. Procedures for granting and elevating access to shall be managed under formal Change Control.

- Flui Technologies will maintain a Business Continuity and Disaster Recovery Framework (BCDR). Flui Technologies' BCDR Framework shall outline the Regular Business Continuity Risk Assessments that must be conducted to identify and analyse potential threats and vulnerabilities that may impact Flui Technologies' operations. Mitigation strategies will be developed and implemented to address identified risks. This plan shall include measures to ensure the continuity of critical business processes and the recovery of IT systems in the event of a disaster. Flui Technologies confirms its commitment to maintaining and regularly testing the BCDR framework.

- A Security Training Policy will be maintained to provide guidelines for training requirements for employees.

- Breaches of this, or any other security-based Policy must be reported in accordance with Security Incident Management Procedures.

- Information security provision and the Policies that guide it will be regularly reviewed, including using annual external audits and penetration testing.

- All Flui Technologies' suppliers must abide by this Information Security Policy or otherwise be able to demonstrate corporate security policies and/or appropriate information security certifications (e.g. ISO 27001, Cyber Essentials Plus) providing equivalent assurance. This includes when accessing or processing assets, whether on site or remotely when subcontracting to other suppliers.

- Cloud services used to process personal data will be expected to have ISO 27001 certification or equivalent controls, with adherence to the standard considered the best way of a supplier proving that it has met the GDPR principle of privacy by design, and that it has considered information security throughout its service model.

- Any request for exceptions, where the standards of security cannot be demonstrated to meet ISO27001 will be considered individually by the Senior Leadership Team.

Information Security Policy

- All assets (data, software, processing equipment and IT services) will be identified and owners documented. The owners are responsible for the maintenance and protection of those assets in accordance with Flui Technologies' Asset and Configuration Management procedure.

The Information Security Policy is reviewed once every six months.

Signature: *Jayne Gough*
Compliance and Risk Manager

Signature: *Sue Rhodes*
Head: Risk and Knowledgebase

Date: 04/08/2026

Document ID	Version and Date	Changes	Updated By	Approved By	Data Classification
ISMS/POL/010	Version 3.7 August 2026	Role updates	J Gough	Sue Rhodes Head: Risk and Knowledgebase	Classified Internal/Business