Information Security Policy

Section 1 - Overview

(1) This Policy sets out our commitment to protecting our information, information assets, products and services through appropriate governance, practices and controls.

(2) We recognise that effective information security is fundamental to maintaining the trust of our clients and other stakeholders, meeting our legal and contractual obligations, and supporting the reliable delivery of our products and services. We are committed to preserving the confidentiality, integrity and availability of our information and information assets through the implementation of security measures that are proportionate to the risks they address.

Section 2 - Scope

(3) This Policy applies to our information, information assets, products and services, and to all activities undertaken by or on our behalf that may affect their security.

Section 3 - Policy

(4) We will:

a. protect the confidentiality, integrity and availability of our information and information assets through appropriate administrative, physical and technical controls;
b. identify, assess and manage information security risks as part of our ongoing governance and operational activities;
c. seek to eliminate information security risks wherever reasonably practicable and, where risks cannot reasonably be eliminated, implement controls to prevent, reduce or otherwise mitigate those risks, having regard to the nature of the risk, the level of the threat, applicable legal and contractual obligations, and relevant commercial considerations;
d. implement information security controls that are proportionate to the level of risk presented to our information, information assets, products and services;
e. ensure access to our information and information assets is authorised and limited to legitimate business requirements;
f. protect confidential information and sensitive information from unauthorised access, use, disclosure, modification, loss or destruction;
g. identify, assess and respond to vulnerabilities and security incidents in a timely and appropriate manner;
h. undertake penetration tests and other security assurance activities appropriate to the level of risk presented by our products, services and information assets;
i. maintain arrangements that support the continuity, resilience and recovery of our products, services and business operations following a security incident or other disruptive event;
j. ensure our personnel understand their information security responsibilities and are supported in fulfilling those responsibilities;

k. require third parties acting on our behalf to maintain information security practices appropriate to the services they provide and the risks they present; and
l. monitor, review and continually improve our information security governance, practices and controls.

Section 4 - Procedures

(5) Refer to the Associated Information page for more information.

Section 5 - Guidelines

(6) Nil.

Part A - Definitions

(7) Definitions applicable to this Policy are contained in the Corporate Glossary.

Status and Details

Status	Current
Effective Date	26th June 2026
Review Date	26th December 2028
Approval Authority	Director
Approval Date	26th June 2026
Expiry Date	Not Applicable
Responsible Manager	Joanne Auld Director
Author	Joanne Auld Director
Enquiries Contact	Joanne Auld Director

Glossary Terms and Definitions

"Confidential Information" - Means information that is not publicly available and which, if disclosed, accessed, altered or destroyed without authorisation, could reasonably be expected to prejudice the interests of the Organisation, its clients, business partners or other stakeholders. Confidential Information includes, but is not limited to, commercial information, contractual information, intellectual property, security information, technical information, financial information, and personal information that is not otherwise publicly available.

"Information Asset" - Means any information, regardless of form or medium, together with the systems, applications, infrastructure, services or components used to create, collect, process, store, transmit, protect or dispose of that information, where the loss, compromise or unavailability of the asset could affect the Organisation or its stakeholders.

"Penetration Test" - Means an authorised security assessment conducted using techniques intended to identify and validate vulnerabilities by attempting to compromise systems, applications, infrastructure, networks or other Information Assets under controlled conditions.

"Security Incident" - Means an actual or suspected event that compromises, or has the potential to compromise, the confidentiality, integrity or availability of Information Assets, Products, Services or the Organisation's operations, or otherwise results in a breach of security controls, policies or legal obligations.

"Sensitive Information" - Means information that requires protection because unauthorised access, use, disclosure, modification or destruction could reasonably be expected to result in harm to an individual, the Organisation, a client, business partner or other stakeholder, whether or not the information is classified as Confidential Information. Sensitive Information includes personal information, security credentials, authentication information, financial information, commercially valuable information and other information identified by the Organisation as requiring additional protection.

"Vulnerability" - Means a weakness, deficiency or flaw in a system, application, process, configuration, control or operational practice that may be exploited to adversely affect the confidentiality, integrity or availability of information or other information assets, the security or operation of the Organisation, or the rights, interests or wellbeing of individuals or other stakeholders.

"Information" - Means knowledge or data, regardless of form or medium, including electronic, physical, verbal or

visual information.

"Information Security" - Means the preservation of the confidentiality, integrity and availability of Information Assets through the implementation of appropriate administrative, physical and technical controls.

"Risk" - Means the effect of uncertainty on objectives, including circumstances that may adversely affect the Organisation's ability to achieve its strategic, operational, legal, financial or security objectives.

"Control" - Means a measure, safeguard, process, practice or mechanism implemented to modify, reduce or manage Risk.

"Product" - Means any software, platform, module, component, application or other offering developed, licensed, supplied or maintained by the Organisation.

"Service" - Means any activity performed by or on behalf of the Organisation for the benefit of a client or stakeholder, including support, implementation, consulting, hosting, maintenance or managed services.

"Stakeholder" - Means an individual, organisation or other entity that: has a legal, contractual, regulatory or governance relationship with the Organisation; receives, provides or supports the provision of the Organisation's Products, Services or business operations; has rights, information or legitimate interests that the Organisation is responsible for protecting or respecting; or may be directly affected by the Organisation's activities or decisions in a manner recognised by law, contract or the Organisation's governance framework.