Document History:			
Issue level	**Page No(s)**	**Date**	**Brief details of amendment(s) to policy**
1	All	22/10/24	First issue of policy

Purpose
The purpose of this policy is to set out the information security policies that apply to the organisation to protect the confidentiality, integrity, and availability of data.

Scope
All employees and third-party users.

Principle
Information security is managed based on risk, legal and regulatory requirements, and business need.

Chief Executives Statement of Commitment
"As a company, information processing is fundamental to our success and the protection and security of that information is a board level priority. Whether it is employee information or customer information we take our obligations under the GDPR and Data Protection Act 2018 seriously. We have provided the resources to develop, implement and continually improve the information security management appropriate to our business."

Introduction
Information security protects the information that is entrusted to us. Getting information security wrong can have significant adverse impacts on our employees, our customers, our reputation, and our finances. By having an effecting information security management system, we can:

- Provide assurances for our legal, regulatory, and contractual obligations
- Ensure the right people, have the right access to the right data at the right time
- Provide protection of personal data as defined by the GDPR
- Be good data citizens and custodians

Information Security Objectives

- To ensure the confidentiality, integrity and availability of organisation information including all personal data as defined by the GDPR based on good risk management, legal regulatory and contractual obligations, and business need.
- To provide the resources required to develop, implement, and continually improve the information security management system.
- To effectively manage third party suppliers who process, store, or transmit information to reduce and manage information security risks.
- To implement a culture of information security and data protection through effective training and awareness.

Information Security Roles and Responsibilities
Co-ordination: The organisation co-ordinates information security management across the company network via the IT Department.
Security Officer: The organisation's Information Security Manager is responsible for ensuring policies and procedures are in place to cover all aspects of ICT systems and Information security. All policies will be communicated across the organisation to ensure good working practices and to minimise the risk to the organisation's reputation.

Directors: Are responsible for ensuring that ICT systems and information within their service areas are managed in accordance with the organisation's ICT Security Policy. Day to day responsibility for the management of ICT systems and information may be delegated to staff designated as information or system owners within departments.

Users of resources: It is the responsibility of any individual or third-party having access to the organisation's ICT systems and information to comply with the organisation's ICT Security Policy, associated guidelines and procedures and to take adequate steps to safeguard the security of the ICT systems and information to which they have access. Any suspected or actual security weakness, threats, events or incidents must be immediately reported to the IMS Administrator and be recorded on an Improvement report.

Monitoring
Compliance with the policies and procedures of the information security management system are monitored via the Management Review Team, together with independent reviews by both Internal and External Audit on a periodic basis.

Legal and Regulatory Obligations
The organisation takes its legal and regulatory obligations seriously and these requirements are recorded in the document Legal and Contractual Requirements Register

Training and awareness
Policies are made readily and easily available to all employees and third-party users. A training and communication plan is in place to communicate the policies, process, and concepts of information security. Training needs are identified, and relevant training requirements are captured in the document Competency Matrix.

Continual Improvement of the Management System
The information security management system is continually improved. The continual improvement policy sets out the company approach to continual improvement and there is continual improvement process in place.

Policy Compliance

Compliance Measurement
The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions
Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Continual Improvement
The policy is updated and reviewed as part of the continual improvement process.

POLICY APPROVAL:		
I confirm the contents of this procedure are correct and are approved for Audiebant Limited.		
Signature: D C Buckley	**Position: Technology Director**	**Date: 25/03/2025**

Annex A Reference:

Ref	Control	Objective
5.1	Policies for information security	Information security policy and topic specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.