Information Security 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.

Managing Director's 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." - P James, Director.

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 Defined

Information security is defined as preserving

Confidentiality	Access to information is to those with appropriate authority ***The right people with the right access***
Integrity	Information is complete and accurate ***to the right data***
Availability	Information is available when it is needed ***at the right time***

Information Security Policy Framework

The information security management system is built upon an information security policy framework. In conjunction with this policy, we maintain a suit of additional policies such as:

- Data Protection Policy
- Data Retention Policy
- Clear Desk & Clear Screen Policy
- Business Continuity Policy

Information Security Roles and Responsibilities

Information security is the responsibility of everyone to understanding and adhere to the policies, follow process and report suspected or actual breaches.

Monitoring

The organisation takes its legal and regulatory obligations seriously. Compliance our legal and regulatory obligations, together with our compliance with the policies and procedures of the information security management system are monitored via the Managing Director.

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 ensure that training needs are identified, and relevant training is provided.

This policy and matters arising from it are reviewed annually and are the responsibility of Peter James, Director.