[Company]

INFORMATION SECURITY POLICY

The policy for information security

1 Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	[DATE]		Document first created

2 Document Contents Page

3 Information Security Policy

3.1 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.

3.2 Scope

All employees and third-party users.

3.3 Principle

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

3.4 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.” [Chief Executive Officer Name and Date and Signature]

3.5 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

3.6 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.

3.7 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***

3.8 Information Security Policy Framework

The information security management system is built upon an information security policy framework. In conjunction with this policy, the following policies make up the policy framework:

- DP 01 **Data protection Policy**
- DP 02 **Data Retention Policy**
- IS 01 **Information Security Policy** (this policy)
- IS 02 **Access Control Policy**
- IS 03 **Asset Management Policy**
- IS 04 **Risk Management Policy**
- IS 05 **Information Classification and Handling Policy**
- IS 06 **Information Security Awareness and Training Policy**
- IS 07 **Acceptable Use Policy**
- IS 08 **Clear Desk and Clear Screen Policy**
- IS 09 **Mobile and Teleworking Policy**
- IS 10 **Business Continuity Policy**
- IS 11 **Backup Policy**
- IS 12 **Malware and Antivirus Policy**
- IS 13 **Change Management Policy**
- IS 14 **Third Party Supplier Security Policy**
- IS 15 **Continual Improvement Policy**
- IS 16 **Logging and Monitoring Policy**

- IS 17 **Network Security Management Policy**
- IS 18 **Information Transfer Policy**
- IS 19 **Secure Development Policy**
- IS 20 **Physical and Environmental Security Policy**
- IS 21 **Cryptographic Key Management Policy**
- IS 22 **Cryptographic Control and Encryption Policy**
- IS 23 **Document and Record Policy**
- IS 24 **Significant Incident Policy and Collection of Evidence**
- IS 25 **Patch Management Policy**
- IS 26 **Cloud Service Policy**
- IS 27 **Intellectual Property Rights Policy**

3.9 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. Specific roles and responsibilities for the running of the information security management system are defined and recorded in the document **Information Security Roles Assigned and Responsibilities**

3.10 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.

3.11 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**

3.12 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.**

3.13 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.

4 Policy Compliance

4.1 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.

4.2 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.

4.3 Non-Compliance

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

4.4 Continual Improvement

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