ISO 27001:2013

Information Security Policy for Chaffinch Green Limited

Last Modified:	30/06/2021
Modifier:	
Version:	1.0
Document URL:	ISO 27001:2013 - 2021 Information Security Policy

Purpose

The purpose of this document is to provide a description of the aims, objectives and overall structure of the Information Security Management System (ISMS).

Objectives

The objective of Information Security is to ensure business continuity and minimise business disruption by preventing and mitigating the impact of Information Security incidents.

In particular, information assets are protected in order to ensure:

- **Confidentiality** - protection against unauthorised disclosure or loss
- **Integrity** - protection of assets against unauthorised or accidental modification
- **Availability** – of information assets to authorised users as required to achieve objectives.

Document Scope

This Policy applies to all business functions within the scope of the ISMS and covers the information, information systems, networks, physical environment (including cloud based and directly hosted services) and products and services.

The Policy applies to all employees, contractors and third parties supporting these business functions.

Responsibilities

Managing Director/CEO:	Overall responsibility for Information Security. Responsible for ensuring that the appropriate levels of resources are made available to support the Information Security function.
Management:	Ensure their employees and contractors comply with this Policy.
Information Security Manager:	Operational responsibility for procedural matters, legal compliance, maintenance and updating of documentation, promotion of security awareness, liaison with external organisations, incident investigation and management reporting.
Data Protection Officer:	Day-to-day responsibility for data protection.
IT Staff:	Responsibility for technical matters, including technical documentation, systems monitoring, technical incident investigation and liaison with technical contacts at external organisations.
Employees and Contractors:	Responsibility for safeguarding assets, including locations, hardware, software, systems or information in their care and to report any suspected breach in security.

Principles

The Information Security Policy is the means by which the Company meets the requirements of ISO/IEC 27001:2013 relating to its business risks. It specifies the requirements for the implementation of appropriate security controls to meet identified risks relating to the activities of the Company.

The implementation and continuing control of this system are fundamental to all work undertaken by the Company. The procedures established are adopted and practised by all employees at every level.

The Company has adopted the process approach for developing, implementing and improving the effectiveness of its ISMS.

The Company, in adopting the process approach is committed to:

- Understanding business information Security requirements and the need to establish Policies and Objectives for Information Security
- Implementing and operating controls in the context of managing the Company's overall business risk
- Monitoring and reviewing the performance and effectiveness of the ISMS
- Continual improvement based on objective measures
- Communicating throughout the Company the importance of meeting all relevant statutory and regulatory requirements specifically related to its business activities
- Ensuring that adequate resources are determined and provided to monitor and maintain the ISMS.

Information Security

Information Security aspects are taken into account in all daily activities, processes, plans, projects, contracts and partnerships entered into by the Company.

Awareness and compliance to Information Security procedures as set out in the various Policies and guideline documents are a requirement of employees and a clause to this effect is set out in the Contracts of Employment.

Copies of all Information Security Policies are made available to all employees.

Breach of the Information Security Policies and procedures by employees may result in disciplinary action, including dismissal.

Employees are advised and trained on general and specific aspects of Information Security, according to the requirements of their function within the Company. The Contract of Employment includes a condition covering confidentiality regarding Company business.

A Business Continuity Plan is in place. This is maintained, tested and subjected to regular review.

Statutory and regulatory requirements are met and monitored for ongoing changes.

Further Policies and Directives such as those for access, acceptable use of email and the Internet, malware protection, backups, passwords, systems monitoring etc. are in place, maintained and are regularly reviewed.

This Information Security Policy is reviewed at least annually and may be amended in order to ensure its continuing viability, applicability and legal compliance and with a view to achieving continual improvement in the ISMS.

The ISMS and Information Security operations are subject to continuous improvement through a program of internal and external audits and risk assessments.

Non-disclosure/Confidentiality Agreements are entered into as appropriate with third-party companies.

Amendment History

Version	Modified On	Modified By	Comments
1.0	30/06/2021	Colene Boskovic	