INFORMATION SECURITY POLICY

ISO 27001 ISMS Policies & Procedures

Version	Review Date	Author	Approved by	SCHEDULED REVIEW DATE	Summary of Changes
1	1 December 2020	Paul Cavicchia	Andrew Lewis	19 Oct 2021	This Policy extends to CTI RTO

Approval

Name	Position	Signature	Date
Andrew Lewis	CEO		19 October 2020

Policy Overview

This policy is based on ISO 27001:2013 the recognised international standard for information security. This standard ensures that the organisation complies with the following security principles:

- **Confidentiality**: all sensitive information will be protected from unauthorised access or disclosure;
- **Integrity**: all information will be protected from accidental, malicious and fraudulent alteration or destruction; and
- **Availability**: information services will be available throughout the times agreed with the users and be protected against accidental or malicious damage or denial of service.

CTI is committed to ensuring that all these aspects of information security are complied with to fulfil its statutory functions.

CTI Compliance with Newfurn's security policies and procedures is mandatory for all personnel.

The Chief Executive Officer (CEO) approves this policy. The Executive Team (ET) has the responsibility for ensuring that the policy is implemented and adhered to.

The security policy confirms CTI's commitment to continuous improvement and highlights the key areas to effectively secure its information.

Policy Detail

Executive Team Responsibilities and commitment

The Executive Team are committed to satisfy all applicable requirements within this policy and to the continual improvement of the ISMS, and therefore have established this information security policy so that:

- It is appropriate to the purpose of the organisation
- It includes information security objectives and provides the framework for setting continual information security objectives;

This information security policy shall be:

- available as documented information;
- be communicated within the organisation; and
- be available to interested parties, as appropriate.

Leadership and Commitment

Top management will continue to demonstrate leadership and commitment with respect to the information security management system by:

- Ensuring the information security policy and information security objectives ae established and are compatible with the strategic business direction of the organisation;
- Ensuring the integration of the information security management system requirements into the organisation's processes;
- Ensuring that the resources (technology, time, staff, training, financial) needed for the information security management system are available;
- Communicating the importance of effective information security management and of conforming to the information security management system requirements;
- Ensuring that the information security management system achieves its intended outcomes;

- Directing sand supporting persons to contribute to the effectiveness of the information security management system;
- Promoting continual improvement; and supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

Information Security Objectives

Information security objectives have been established and are compatible with the strategic direction of the organisation, the key objective is to work in line with the sections of the best practice standard ISO 27001:2013 detailed below.

Furthermore, security objectives will be set by management as an ongoing task and at ISMS Management Review Meetings and an Information Security Objectives Policy will be produced and implemented as part of the ISMS.

Management Objectives for Information Security will be continually set and monitored to ensure they are achieved.

Newfurn will seek to continually improve the information security management system in line with a PLAN-DO-CHECK-ACT to improve process embedded within its ISMS.

ISMS-DOC-06.2-Information Security Objectives-22022021

Organisation of Information Security

The importance attached to information security within Newfurn is demonstrated through the Monthly Executive Team Review (METR); the function of the METR is outlined below:

- Reviewing and progressing strategic security issues;
- Assessing the impact of new statutory or regulatory requirements imposed on Newfurn;
- Monitoring the effectiveness of the Information Security Management System from the results of IT Health checks and penetration testing;
- Recommending and endorsing changes to the ISMS.

The METR meets regularly to address the above activities in order to assure the continuing effectiveness of Newfurn's ISMS.

Human Resource Security

All employees must 'sign up' to the Staff Handbook which requires them to work in accordance with all policies and procedures which includes information security specific requirements. Furthermore, an "Acceptable Use Policy" ensures that employees are made aware that they are required to follow best practices regarding information security established by Newfurn. There is also a procedure for all employees that leave Newfurn (including temporary and contract employees) to disable their network account and recover all items of property.

All new employees (permanent, temporary and contractors) must be trained on procedures in the areas described above as part of their induction programme. Ongoing training must be provided in the form of a programme of regular updates and training sessions by the Executive Team, this is delivered by way of Minutes of QETR to all staff.

Asset Management

Employees must be aware of, and must follow a number of controls and procedures, which exist to limit access to confidential information. The IT Contractor (SimpleBiz) are responsible for both establishing and maintaining robust logical access controls

Cryptography

Where cryptographic controls are employed by Newfurn, a policy on the use of cryptographic controls for protection of information must be developed and implemented.

Physical and environmental Security

Staff must be aware of and must follow the detailed set of measures, controls and procedures that exist to ensure adequate control of physical security. These include:

- Building alarm systems;
- Restricted access to the building and further restricted access within it;
- Secure drawers, fireproof safes and storage;
- Clear desk policy
- Clear screen policy

Operations Security

Newfurn will ensure correct and secure operations of information processing facilities.

Communications Security

Staff must be aware that the use of technology and communications are established, controlled and managed by SimpleBiz and the HR Department. SimpleBiz and the HR Department are responsible for ensuring that the appropriate security measures and processes are in place. SimpleBiz and Newfurn will ensure that security around the network, mobile and remote working are adequately protected.

System Acquisition, Development & Maintenance

The Executive Team must ensure that the appropriate information security processes are included in all projects.

Supplier Relationships

Information security requirements for mitigating the risks associated with supplier's access to the organisation's assets must be agreed with the supplier and documented.

Information Security Incident Management

Security incident management records must be maintained, updated and monitored by SimpleBiz. All employees must be aware of what constitutes an actual or potential security incident, how to report the incident and who to report the incident to.

The responsibility for the oversight of breaches of technical and physical security rests with the Executive Team.

Information Security Aspects of Business Continuity Management

The organisation must ensure a consistent and effective approach to the management of major information security incidents, including communication on security events and weaknesses and the implications for business continuity management.

Compliance

Newfurn must avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any requirements.

Newfurn must take technical and organisation measures to protect personal data against accidental or unlawful destruction, or accidental los or alteration, and unauthorised disclosure or access. In particular, Newfurn takes measures that are intended to ensure that:

- Anyone managing and handling person data understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling persona data is appropriated training to do so; and
- Everyone managing and handling person data is appropriately supervised.

Review

This document must be reviewed at least annually by its "Person Responsible". The Person Responsible must ensure that correct version number is applied to the document once the review has taken place.

Enforcement

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