Reference		**Version**	1
Distribution	CTI	**Document Type:**	Policy
Responsible	Andrew Lewis	**Created**	17 March 2022
Author	Paul Cavicchia	**Review Due**	20 June 2024
File name			

DATA SECURITY POLICY

ISO 27001 ISMS Policies & Procedures

Version	Date	Author	Approved by	Review Due	Summary of Changes
1	17/03/2022	Paul Cavicchia	Andrew Lewis	30/6/2024	Initial Version

Approved: _____

Andrew Lewis (CEO)

Date: _____

Reference		**Version**	1
Distribution	CTI	**Document Type:**	Policy
Responsible	Andrew Lewis	**Created**	17 March 2022
Author	Paul Cavicchia	**Review Due**	20 June 2024
File name			

Employee requirements

1.0 Purpose

CTI must protect restricted, confidential or sensitive data from loss to avoid reputation damage and to avoid adversely impacting our customers. The protection of data in-scope is a critical business requirement, yet flexibility to access data and work effectively is also critical.

It is not anticipated that this technology control can effectively deal with the malicious theft scenario, or that it will reliably detect all data. Its primary objective is user awareness and to avoid accidental loss scenarios. This policy outlines the requirements for data leakage prevention, a focus for the policy and a rationale.

2.0 Scope

1. Any employee, contractor or individual with access to **the CTI's** systems or data.
2. Definition of data to be protected:
    - PII (Personal Identifiable Information)
    - Financial
    - Restricted
    - Sensitive
    - Confidential
    - IP (Intellectual Property

3.0 Policy – Employee requirements

1. You need to complete **CTI's** security awareness training on induction and agree to uphold the Acceptable Use Policy
2. If you identify an unknown, un-escorted or otherwise unauthorized individual in **CTI** you need to immediately notify any of the Executive Team members.
3. Visitors to **CTI must sign in and sign out** and must be escorted by an authorized employee at all times. If you are responsible for escorting visitors, you must restrict them to appropriate areas.
4. You are required not to reference the subject or content of sensitive or confidential data publicly, or via systems or communication channels not controlled by **CTI**. For example, the use of external e-mail systems not hosted by **CTI** to distribute data is not allowed.
5. Please keep a clean desk. To maintain information security, you need to ensure that all printed in-scope data is not left unattended at your workstation.
6. You need to use a secure password on all **CTI** systems as per the password policy. These credentials must be unique and must not be used on other external systems or services.
7. Terminated employees will be required to return all records, in any format, containing personal information.
8. You must immediately notify **the CEO** in the event that a device containing in-scope data is lost (e.g. mobiles, laptops etc).
9. In the event that you find a system or process which you suspect is not compliant with this policy or the objective of information security you have a duty to inform **the RTO Manager** so that he can take appropriate action.

10. If you have been assigned the ability to work remotely you must take extra precaution to ensure that data is appropriately handled. Seek guidance from **the RTO Manager** if you are unsure as to your responsibilities.
11. Please ensure that assets holding data in-scope are not left unduly exposed, for example visible in the back seat of your car.
12. Data that must be moved within **CTI** is to be transferred only via business provided secure transfer mechanisms (e.g. encrypted USB keys, file shares, email etc). **CTI** will provide you with systems or devices that fit this purpose. You must not use other mechanisms to handle in-scope data. If you have a query regarding use of a transfer mechanism, or it does not meet your business purpose you must raise this with **SimpleBiz IT support.**
13. Any information being transferred on a portable device (e.g. USB stick, laptop) must be encrypted in line with industry best practices and applicable law and regulations. If there is doubt regarding the requirements, seek guidance from **SimpleBiz IT support**
14. All Newfurn owned property, including documents, photos, images, designs, plans etc, must be stored on SDRIVE network in the appropriate folders and NOT stored locally on employee computers.

Data Leakage Prevention – Data in Motion

Background to this policy

Data leakage prevention is designed to make users aware of data they are transferring which may be sensitive or restricted in nature.

1.0 Purpose

CTI must protect restricted, confidential or sensitive data from loss to avoid reputation damage and to avoid adversely impacting our customers. The protection of in-scope data is a critical business requirement, yet flexibility to access data and work effectively is also critical.

It is not anticipated that this technology control can effectively deal with the malicious theft scenario, or that it will reliably detect all data. Its primary objective is user awareness and to avoid accidental loss scenarios. This policy outlines the requirements for data leakage prevention, a focus for the policy and a rationale.

2.0 Scope

1. Any **CTI** device which handles customer data, sensitive data, personally identifiable information or company data. Any device which is regularly used for e-mail, web or other work-related tasks and is not specifically exempt for legitimate business or technology reasons.
2. The **CTI** information security policy will define requirements for handling of information and user behaviour requirements. This policy is to augment the information security policy with technology controls.
3. Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk assessment must be conducted by **SimpleBiz**

3.0 Policy

1. **CTI's** data leakage prevention (DLP) technology will scan for data in motion.
2. The DLP technology will identify large volumes (thus, of high risk of being sensitive and likely to have significant impact if handled inappropriately) of in-scope data.

In-scope data is defined as:

a) Credit card details, bank account numbers and other financial identifiers

b) E-mail addresses, names, addresses and other combinations of personally identifiable information

c) Documents that have been explicitly marked with the '**CTI** Confidential' string.

d) Contracts, Service Agreements and Membership Agreements

3. DLP will identify specific content, i.e.:
    a. Sales data – particularly forecasts, renewals lists and other customer listings
    b. Exports of personally identifiable information outside controlled systems
4. DLP will be configured to alert the user in the event of a suspected transmission of sensitive data, and the user will be presented with a choice to authorize or reject the transfer. This allows the user to make a sensible decision to protect the data, without interrupting business functions. Changes to the DLP product configuration will be handled through CTI, IT change process and with security management approval, to identify requirements to adjust the information security policy or employee communications.
5. DLP will log incidents centrally for review SimpleBiz will conduct first level triage on events, identifying data that may be sensitive and situations where its transfer was authorized and there is a concern of inappropriate use. These events will be escalated to HR to be handled through the normal process and to protect the individual.
6. Where there is an active concern of data breach, the IT incident management process is to be used with specific notification provided to SimpleBiz
7. Access to DLP events will be restricted to a named group of individuals to protect the privacy of employees. A DLP event does not constitute evidence that an employee has intentionally, or accidentally lost data but provides sufficient basis for investigation to ensure data has been appropriately protected.

4.0 Technical guidelines

Technical guidelines identify requirements for technical implementation and are typically technology specific.

1. The technology of choice is managed by SimpleBiz as required.
2. The product will be configured to identify data in motion to Browsers, IM Clients, E-mail clients, Mass storage devices and writable CD media.

5.0 Reporting requirements

1. Immediate reports of incidents will be provided to the CEO
2. Six Monthly report showing % devices compliant with DLP policy

Workstation Full Disk Encryption

Background to this policy

Full disk encryption is now a key privacy enhancing technology which is mandated my many regulatory guidelines.

1.0 Purpose

CTI must protect restricted, confidential or sensitive data from loss to avoid reputation damage and to avoid adversely impacting our customers. A collection of global regulations also requires the protection of a broad scope of data, which this policy supports by restricting access to data hosted on Newfurn's network and devices.

As defined by numerous compliance standards and industry best practice, full disk encryption is required to protect against exposure in the event of loss of an asset. This policy defines requirements for full disk encryption protection as a control and associated processes.

2.0 Scope

1. All **CTI** workstations – desktops, laptops, iPads and mobile phones
2. All **CTI** virtual machines.
3. Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk assessment must be conducted by SimpleBiz

3.0 Policy

1. All devices in-scope will have full disk encryption enabled.
2. **CTI**'s Acceptable Use Policy (AUP) and security awareness training must require users to notify SimpleBiz if they suspect they are not in compliance with this policy as per the AUP.
3. The AUP and security awareness training must require users to notify SimpleBiz and the CEO of any device which is lost or stolen.
4. Encryption policy must be managed, and compliance validated by SimpleBiz
5. Where management is not possible and a standalone encryption is configured (only once approved by a risk assessment), the device user must provide a copy of the active encryption key to SimpleBiz.
6. SimpleBiz/Newfurn has the right to access any encrypted device for the purposes of investigation, maintenance or the absence of an employee with primary file system access. Induction, AUP and security awareness training will advise users of this requirement.
7. The encryption technology must be configured in accordance with industry best practice to be hardened against attacks.
8. All security related events will be logged and audited by SimpleBiz to identify inappropriate access to systems or other malicious use.
9. The SimpleBiz help desk will be permitted to issue an out-of-band challenge/response to allow access to a system in the event of failure, lost credentials or other business blocking requirements. This challenge/response will be provided only in the event that the identity of the user can be established using challenge and response attributes documented in the password policy.
10. Configuration changes are to be conducted through SimpleBiz change control process, identifying risks and noteworthy implementation changes to security management.

4.0 Technical guidelines

Technical guidelines identify requirements for technical implementation and are typically technology specific.

1. Strong, industry best practice defined cryptographic standards must be employed. AES-256 is an approved implementation.
2. The BIOS will be configured with a secure password (as defined by password policy) that is stored by IT. The boot order will be fixed to the encrypted HDD. If an override is required by a user for maintenance or emergency use, the helpdesk can authenticate the user and then provide the password for the BIOS. The objective being to avoid an attacker cold booting and attacking the system.
3. Synchronization with Windows credentials will be configured so that the pre boot environment is matched to the user's credentials and only one logon is required.
4. A pre boot environment will be used for authentication. Credentials will be used to authenticate the user in compliance with Newfurn's password security policy

5.0 Reporting requirements

1. A monthly report that identifies the % of encrypted systems versus assets in-scope
2. A monthly report that identifies the compliance status of managed, encrypted systems
3. A monthly report that identifies the number of lost assets and validation that lost devices have been handled appropriately.