Data Security Policy

Life Care Consultants Ltd (Life Care) provide a secure method of data management and transfer that meets New Zealand security and privacy policies and enables client organisations to move towards compliance with NZ legislation, regulations, and Codes of Practice. Specifically, this includes:

- The New Zealand Protective Security Requirements (PSR) including the Information Security Manual (NZISM); and
- Follow all protective security protocols for the full duration of engagement; and
- Life Care and any of their sub-contracted providers must not undermine the protective security capability of the client; and
- Requirements of the Official Information Act 1982; and
- All legal jurisdictions in which its data will be stored, processed, or transmitted and provisions undertaken to ensure the data sovereignty, confidentiality and integrity of client data; and
- Indication of ability for the solution to support multi-factor authentication, especially for privileged or high access roles or where integrated authentication is not in use.

Purpose

A data protection policy (DPP) is dedicated to standardising the use, monitoring, and management of data. The main goal of the policy is to protect and secure all data consumed, managed, and stored by Life Care Consultants.

Scope

This data security policy statement applies to all of Life Care (or a person acting on behalf of Life Care). It serves to clarify how we collect, use, store, disclose, update, and destroy individual's personal information in New Zealand. Life Care Consultants is a NZ Limited Company, New Zealand Registered Company Number 714730.

Compliance regulations help to ensure that clients privacy requests are carried out by companies, and companies are responsible to take measures to protect private user data.

Definition

Personal Information means information about an identifiable individual.

Who is responsible for the security of personal information and confidential data?

The Systems Manager ensures Life Care's processes concerning the personal data of its staff, customers, providers, or any other individual is managed in compliance with the applicable data protection rules. The Systems Manager is also **r**esponsible for educating the company and its employees about compliance, training staff involved in data processing, and overall responsibility of governance of privacy practice.

Training staff involved in managing security and privacy of data, including in relation to what to do in the event of a data breach (including but not limited to personal data)

Data protection training at Life Care involves the following topics for staff:

1. Handling Personal Information Requests - The individual's identity must be verified and referenced against the data in your possession, we are not to provide data relating to other persons without their explicit permission, and how to gain that permission in writing.
2. Phishing – Life Care staff are advised not to disclose personal information about our clients or users to anyone over the phone; written communication for the request is required from the approved client manager.
3. Dealing with Customers – Keeping our customers and users up to date regarding the use of their data, and ensuring consent is obtained before collecting or processing data. The "User Access Agreement Consent" form is to be signed prior to the release of data.
4. Password and Two Factor Authentication – Access is granted only after successfully presenting two or more pieces of evidence to an authentication mechanism.
5. Breach Reporting – Life Care staff are trained to report any security breach to their manager or supervisor as soon as any breach is detected.
6. Risk Assessment – Identifying sensitive data and ensuring such data has additional safeguards to ensure its processing does not present a breach risk and access controls are in place to prevent unauthorised devices.
7. Confidentiality – Staff are informed of the consequences of a neglectful approach towards data security and the requirement to adhere to confidentiality policies.
8. New Hires – New staff are acquainted with privacy best practices and, during their induction to Life Care, complete the online Privacy ABC and Health ABC on the eLearning Site of the Office of the Privacy Commissioner.
9. Security Policies – Reviewed annually.

Life Care Consultants meets industry best practice expectations in terms of privacy and information security for personal or classified data, including for detecting and responding to information security or privacy breaches.

Relevant Life Care policies include the following:

1. Password and Two Factor Authentication – access is granted only after successfully presenting two or more pieces of evidence to an authentication mechanism.
2. Breach Reporting - Once Life Care discovers a privacy breach, inform IT Service Provider CodeBlue to contain it immediately, resolve the issue and provide root cause analysis to ensure no gap in security.
3. Early warning system – managed by IT Service Provider CodeBlue.
4. Risk Assessment – Undertake risk assessment, specify risks to be mitigated, and collaborate with statistical methods and data specialists to determine appropriate continentalization and de-identification techniques.
5. Confidentiality – User Access Agreement Consent form - signed by clients.

Policies and procedures secure and maintain systems, and process data (including personal and confidential data) related to the client organisation.

Client data is stored on the Cohort Application; the vendor agrees upon the following procedures and security:

1. Encryption
   Any information at rest within the Cohort Hosted Solution will, under normal circumstances, not be visible and will be encrypted to AES-128 using Self Encrypting Drives (SEDs). All-access is under restricted physical and logical security.
   The Cohort Hosted Solution is delivered using web browser technologies to provide the end-user with a secure and seamless experience. The solution is accessed over a secure HTTPS connection, deployed with secure protocols up to TLS 1.2, using a standard internet browser. SSL certificates are issued from a trusted 3rd party root CA – DigiCert.
2. Backup
   Backups for Azure-hosted Cohort v10 SaaS instances are backed up across Availability Zones to deliver geographic redundancy and resilience. Azure Resiliency Information (link).
3. Firewall
   A multi-layer firewall implementation approach is to protect the infrastructure. A perimeter firewall protects the Internet and the DMZ segment. The firewall implicitly denies any inbound traffic to the web servers other than HTTPS from the Internet and RDP (development and support) connections from the corporate VLAN.
   An additional firewall segregates the DMZ, secure DMZ and internal hosting VLAN. This firewall also securely publishes the web server located in the secure DMZ via reverse proxy.

The firewall will implicitly deny any inbound traffic to the database server other than inbound SQL traffic (end-user data) from the web server and inbound RDP (development and support) connections from the corporate VLAN.

4. Server hardening
   Using Microsoft tools and best practices, any internet-facing servers are hardened to minimise any potential attack surface. This a Cohort function, Microsoft accredited software employees, and CRB checked.
5. Patch Updates
   Patching is applied monthly to both Microsoft and VMWare and on a staggered six-monthly basis to server hardware, firewalls and switches, and SAN hardware. Notification is required. Patching is a mixture of alerts from ISO and vendor portals. Microsoft WSUS automatically downloads and distributes security hotfixes to Microsoft servers and applications. Patches are installed in the test environment before being released onto production systems and aim to have hotfixes installed within 48hrs of release unless the severity dictates otherwise.
6. Anti-virus
   Host-based anti-virus software is installed on all Windows servers within the host Cohort environment and is configured to update and perform full scans on a scheduled basis automatically. Vendor-supplied tools are used for centralised management and updating.
   Endpoint Anti-virus is installed on devices. It offers strong protection against all forms of malware, ransomware, spyware, and phishing websites.
7. Penetration testing
   The Cohort v10 application is penetration tested by an external CREST/CHECk accredited organisation. The Azure cloud infrastructure is penetration tested by Microsoft

Risk Management Methodology – ISO 27001

1. Identify the risks - define threats the business is exposed to in its operating environment.
2. Analyse the risk - assess the likelihood of occurrence and impact of risks.
3. Evaluate or rank the risk - evaluate the quality of existing controls.
4. Treat the risk - assess risks and determine responses.
5. Monitor and review the risk.

Privacy Impact Assessment (PIA)

This process is conducted through Cohort.

Storage of any commercially sensitive digital personal data

Cohort Software Limited has partnered with Blue Chip Customer Engineering Limited to provide a fully resilient and eco-friendly data centre that delivers co-location services for the Cohort Private Cloud infrastructure.

Access to the data centre is restricted to pre-authorised personnel only. Both changes to the nominated personnel and general access are subject to approval by the Data Centre Change Control System.

Public access to the data centre, even by authorised personnel, requires 24 hours advance notice; emergency access for critical issues must be agreed upon by predefined and specifically authorised Cohort Software personnel.

Visitors attending the site must provide government-issued photographic identification to substantiate their identity.

Last updated: April 2023