Central Data Networks “FindMI” Security Policy

Purpose

The purpose of this Security Policy is to advise ways in which Central Data Network Staff will manage all aspects of security, from password creation, data and network security, to privacy and physical security. This document is available to FindMI customers on request and is used by staff as the basis on which management decisions regarding privacy and security are made, as well as forming the foundation for more specific security policies.

Governance – Central Data Networks

Central Data Networks agrees to follow the directives and rulings of government appointed bodies concerned with setting standards for security policy. Central Data Network staff members are required to follow these directives and rulings on the company’s behalf.

Ownership, management, responsibilities

Central Data Networks Privacy Officer – Managing Director

The Managing Director (MD) of Central Data Networks has overall responsibility for ensuring all relevant standards, laws, acts, and other external and internal legislation and policies regarding patient and client privacy are adhered to at all times.

Central Data Networks Security Officer – Chief Technology Officer

The Chief Technology Officer (CTO) has overall responsibility for Information Technology within Central Data Networks. Including the provision and security of infrastructure, applications and communications, and the management of Information Technology projects. Some responsibilities may be delegated to other staff as applicable. This role is also responsible for maintaining private information security, and compliance to the relevant information security standards and best practice guidelines.

Policy review

All policies are regularly monitored and reviewed to ensure they remain relevant to all applicable international standards, laws and legislation, Central Data Networks business aims and objectives, and in the event of the introduction of new or upgraded technology. This policy is reviewed at least annually by Central Data Networks Information Security Steering Committee.

Policy compliance – Central Data Networks

This policy is monitored for compliance by the CTO and may include random and scheduled inspections. Compliance with the Security Policy and all other Central Data Networks policies is mandatory.

Exceptions

Any exception to this policy or any other Central Data Networks security related policy must be approved by the CTO in advance.

Partnerships

Promoting security consciousness amongst customers and vendors, Central Data Networks takes every opportunity it can to promote awareness of the importance of security and privacy within its extensive customer base, and to all vendors whose systems, data and/or networks integrate with Central Data Network's in any way.

Trusted third parties

No third parties can work on the Central Data Networks infrastructure, system or network unless they are contractors bound by declarations and security adherence as defined in other relevant policies. Additionally, all Central Data Networks customers must adhere to security requirements as laid out in contracts, terms of service, and all other relevant commercial agreements.

Additional security policies

Various Central Data Networks policies and documents are directly associated with, and/or referenced in, this Security Policy. Please contact the CTO for further details.

Refer to the following sections for the purpose of some relevant policies.

Acceptable Use Policy

The purpose of the Acceptable Use Policy is to outline the acceptable use instructions for staff regarding the use of Central Data Networks computer equipment, systems, networks and applications. This policy protects Central Data Networks Ltd, and every Central Data Networks client and staff member from potential risks including virus attacks, compromise of network systems and services, reputational damage and legal action.

Access Control Policy

The purpose of the Acceptable Use Policy is to ensure that all computer systems and networks owned or managed by Central Data Networks are operated in an effective, safe, ethical and lawful manner. This policy also ensures the prevention of unauthorised access through managed controls, to create a secure computing environment.

Business Continuity Planning/Disaster Recovery Policy

The purpose of the Business Continuity Planning/Disaster Recovery (BCP/DR) Policy is to ensure the appropriate resources are provided to enable Central Data Networks to prepare for, respond to, and recover from disruptive incidents when they arise. This policy includes requirements and strategies for planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving

Central Data Networks BCP/DR capability.

The scale of events covered by this policy range from minor or partial system unavailability (business continuity) through to total system loss (disaster recovery).

Communication and Mobile Devices Policy

The purpose of the Communication and Mobile Devices Policy is to ensure acceptable use of mobile devices (including mobile phones) and communication systems used for business activities.

Computer Systems and Equipment Use Policy

The purpose of the Computer Systems and Equipment Use Policy is to advise users of, and ensure compliance to, Central Data Networks requirements regarding the acceptable use of technology provided to staff.

Cyber Crime and Security Incidents Policy

The purpose of the Cyber Crime and Security Incident Policy is to ensure the correct procedures are followed should systems be affected by a security incident.

Hardware Management Policy

The purpose of the Hardware Management Policy is to ensure the correct procedures are followed regarding the purchase, deployment, maintenance and replacement of computer hardware and other devices.

Information Management Policy

The purpose of the Information Management Policy is to ensure management and storage of data and information does not comprise the electronic information repositories of Central Data Networks.

Personnel Management Policy

The purpose of the Personnel Management Policy is to ensure the risks of security breaches or threats caused by Central Data Networks personnel are minimised or eliminated. It also ensures that all personnel using and managing Central Data Networks computer systems and networks are sufficiently vetted according to strict security requirements, and that they act in a responsible and ethical manner.