rehabhire&sales

YOUR LEADING HEALTHCARE EQUIPMENT PARTNER

INFORMATION SECURITY POLICY

Approved by: Samantha Putkunz
Version: 2.1
Date: 27 April 2026
Review: Annually

CONTENTS

320 Lorimer Street Port Melbourne Victoria 3207
1300 000 030 • contact@rehabhire.com.au • rehabhire.com.au
ABN 80 139 444 492 • ACN 139 444 492 • NDIS Provider Number 405 000 8554

1. PURPOSE AND SCOPE

This Information Security Policy establishes the principles, responsibilities, and practices that Rehab Hire & Sales Pty Ltd and Rehab Installation Pty Ltd (collectively 'the Company') apply to protect the confidentiality, integrity, and availability of all information assets.

This Policy applies to all information held in any format digital, physical, or verbal, including personal information, sensitive health information, client records, financial data, and business information. All employees, contractors, volunteers, and third parties with access to Company information or systems must comply.

2. INFORMATION SECURITY PRINCIPLES

We manage information security based on three core principles:

- Confidentiality: Information is accessible only to those authorised to access it
- Integrity: Information is accurate, complete, and protected from unauthorised modification
- Availability: Information is accessible to authorised users when required

We apply a risk-based approach proportionate to the sensitivity of information involved.

3. ACCESS CONTROL

3.1 User Access

- All staff are issued individual user accounts. Shared login credentials are prohibited
- Access rights are reviewed when a staff member changes role or leaves the Company
- Access to client health information and funding data is restricted to staff directly involved in service delivery

3.2 Password Management

- All system passwords must meet minimum complexity requirements (minimum 12 characters, upper/lowercase, numbers, and symbols)
- Passwords must not be shared, written down, or stored in unsecured formats
- Multi-factor authentication (MFA) is required for all cloud-based systems where available
- Passwords must be changed immediately if compromise is suspected

4. PHYSICAL SECURITY

- Client files and physical records are stored in locked cabinets at a separate location accessible only to Directors and the Managing Partner
- Visitors to our premises are signed in and supervised at all times
- Hard copy documents containing personal or sensitive information must be shredded, not placed in general waste
- Portable devices (laptops, tablets, phones) containing client information must be secured when not in use and not left unattended in vehicles
- Physical access to server or IT infrastructure areas is restricted to authorised personnel only

5. IT AND DIGITAL SECURITY

5.1 Systems and Software

- All Company devices must run supported, up-to-date operating systems with current security patches applied
- Antivirus and endpoint protection software is installed and maintained on all Company devices
- Software must only be installed with management approval. Unauthorised installation is prohibited

5.2 Network Security

- Company networks are protected by firewalls and monitored for unusual activity
- Staff must not access Company systems or client data via unsecured public Wi-Fi without an approved VPN
- Remote access to Company systems must use secure, approved methods only

5.3 Email and Communications

- Personal or sensitive client information must not be sent by unencrypted email unless necessary, and only to verified recipients
- Staff must be vigilant for phishing emails. Suspicious emails must be reported immediately and not clicked, forwarded, or responded to
- Client information must not be shared via personal email accounts, SMS, or personal messaging apps

5.4 Cloud and Data Storage

- Client data must only be stored in Company approved, Australian hosted cloud systems
- Data must be backed up regularly and backup integrity tested periodically

6. HANDLING SENSITIVE AND HEALTH INFORMATION

Given the nature of our services, we regularly handle health and disability-related data

- Only access health or disability information where directly required for service delivery
- Never discuss client health or personal information in public areas or on unsecured channels
- Obtain appropriate consent before sharing client health information with third parties where required
- Follow the Company's Privacy Policy at all times available at rehabhire.com.au
- Be aware that breaches involving health information may constitute an eligible data breach under the NDB scheme and must be reported immediately to Directors, the Managing Partner and/or Senior Management

7. DATA RETENTION AND DISPOSAL

- Personal information is retained only for as long as required for the purpose of collection, or as required by applicable law
- When personal information is no longer required it must be securely destroyed, physical records shredded, digital records permanently deleted
- A data retention schedule is maintained internally and reviewed when required

8. SECURITY INCIDENTS AND BREACH RESPONSE

All staff must immediately report any suspected or confirmed security incident to their direct Manager, the Directors, Managing Partner and/or the ICT Team

This includes:

- Lost or stolen devices containing personal information
- Accidental disclosure of client information to an unauthorised party
- Suspected phishing attacks or malware infection
- Unauthorised access to systems or files; misdirected emails containing personal information
- Email forwarded to the incorrect person/s when client details and/or sensitive details are included

Upon notification, the Company will contain the incident, assess the risk of harm, notify affected individuals and review controls to prevent recurrence. Failure to report a security incident is a serious and reportable breach of this Policy.

9. STAFF RESPONSIBILITIES AND TRAINING

All staff are responsible for the security of information they access in the course of their work. Specific responsibilities include:

- Complete our cyber security training when required
- Comply with this Policy and all related policies at all times
- Report security concerns, incidents, or suspected breaches immediately to: techservices@rehabhire.com.au
- Not access, copy, or disclose information beyond what is required for their role

Breaches of this Policy may result in disciplinary action up to and including specific training where gaps are apparent, formal warnings, termination and may be referred to relevant authorities where a legal obligation exists.

10. THIRD PARTIES AND CONTRACTORS

Third parties and contractors who access Company systems or client information must be subject to contractual confidentiality obligations, must only access information required for their specific engagement, and must notify us immediately of any security incident. All Company information must be returned or destroyed at the end of their engagement.

11. REVIEW, COMPLIANCE, AND CONTACT

This Policy will be reviewed annually or following a significant security incident.

Queries should be directed to:

Samantha Putkunz
Managing Partner

320 Lorimer Street, Port Melbourne VIC 3207

t: 1300 000 030
e: techservices@rehabhire.com.au | samantha@rehabhire.com.au