**Southern Motion Physiotherapy**  
**Security Policies Document**

**1. Acceptable Use Policy**

**Purpose**

To outline acceptable use of technology resources at Southern Motion Physiotherapy to protect patients, employees, and the clinic from security risks and legal liabilities.

**Scope**

Applies to all employees, contractors, and third-party service providers who use the clinic’s technology resources.

**Policy**

* Clinic-provided devices must only be used for authorised business purposes.
* Personal use (e.g., checking personal email) is permitted during breaks only and must not compromise security.
* Users must not install unauthorised software.
* Accessing inappropriate content (e.g., adult content, gambling) is strictly prohibited.
* Use of USB storage devices is restricted and must be approved by management.

**2. Access Control Policy**

**Purpose**

To ensure that access to systems and patient data is granted appropriately and securely.

**Scope**

Covers access to all systems containing confidential clinic or patient information.

**Policy**

* Access is granted based on the principle of least privilege.
* All staff must have individual user accounts.
* Use of Multi-Factor Authentication (MFA) is mandatory.
* Accounts must be reviewed quarterly and deactivated promptly when no longer needed.
* Shared accounts are prohibited.

**3. Data Protection and Privacy Policy**

**Purpose**

To protect the privacy and confidentiality of patient data in compliance with Australian Privacy Principles (APPs).

**Scope**

Applies to all handling of patient records and personal information.

**Policy**

* Patient data must be stored securely in encrypted systems.
* Access to patient data is strictly on a need-to-know basis.
* Physical records must be locked when not in use.
* Staff must complete annual privacy training.
* Data must not be shared with third parties without explicit patient consent.

**4. Incident Response Policy**

**Purpose**

To ensure a quick, effective, and orderly response to information security incidents.

**Scope**

Covers all types of security incidents, including data breaches, malware infections, and unauthorised access.

**Policy**

* All employees must report incidents immediately to the Clinic Director.
* A preliminary assessment must be completed within 24 hours.
* Incidents must be documented in an incident log.
* If a breach involves patient data, the Office of the Australian Information Commissioner (OAIC) must be notified.
* Post-incident reviews will be conducted to improve defences.

**5. Backup and Recovery Policy**

**Purpose**

To ensure the integrity and availability of critical clinic data through regular backups.

**Scope**

Applies to all electronic records and systems managed by the clinic.

**Policy**

* Full system backups must be performed weekly.
* Incremental backups must occur daily.
* Backups must be stored securely and encrypted.
* Backup restoration tests must be conducted quarterly.
* Backup failures must be reported immediately to the Practice Manager.

**6. Policy Compliance Checklist**

**Purpose**

To evaluate and ensure consistent adherence to clinic security policies.

| **Policy Area** | **Compliance Criteria** | **Compliant? (Yes/No)** | **Responsible Party** | **Review Frequency** |
| --- | --- | --- | --- | --- |
| Acceptable Use Policy | Are all users aware of what constitutes acceptable/unacceptable use? |  | Practice Manager | Quarterly |
|  | Are personal use restrictions communicated and followed? |  |  |  |
|  | Are USB device approvals tracked? |  | IT Consultant / Manager |  |
| Access Control Policy | Are user accounts reviewed quarterly? |  | Practice Manager | Quarterly |
|  | Is MFA enabled for all systems? |  | IT Consultant |  |
|  | Are shared accounts disabled? |  |  |  |
| Data Protection and Privacy Policy | Are physical records locked when not in use? |  | All Staff | Monthly |
|  | Is data encryption in place? |  | IT Consultant |  |
|  | Has privacy training been completed this year? |  | HR/Practice Manager | Annually |
| Incident Response Policy | Are incidents reported and logged consistently? |  | All Staff | Ongoing |
|  | Was the last incident review documented? |  | Clinic Director | After each incident |
| Backup and Recovery Policy | Are daily and weekly backups occurring on schedule? |  | IT Consultant | Weekly |
|  | Has the last backup restore test been conducted successfully? |  | IT Consultant | Quarterly |

**7. Security Awareness Training Plan**

**Purpose**

To reduce human error-related security risks by ensuring all staff at Southern Motion Physiotherapy understand their cybersecurity responsibilities and best practices.

**Scope**

Applies to all employees, including part-time and contracted staff, who access clinic systems or data.

**Training Objectives**

* Increase staff awareness of common cyber threats (phishing, malware, social engineering).
* Promote secure behaviour (strong passwords, safe internet use, recognising suspicious emails).
* Ensure understanding of policies (acceptable use, access control, incident reporting).

**Training Components**

| **Training Module** | **Description** | **Delivery Method** | **Frequency** |
| --- | --- | --- | --- |
| Introduction to Cybersecurity | Overview of common threats and why security matters | Onboarding presentation | New hires |
| Password Security | Creating strong passwords and using MFA | Online module | Annually |
| Email & Phishing Awareness | How to detect and report suspicious emails | Interactive e-learning | Quarterly |
| Data Privacy & Handling | Understanding APPs and handling patient data securely | In-person workshop | Annually |
| Acceptable Use & Device Security | Rules for safe use of clinic systems, mobile devices, and internet access | Staff handbook review | Annually |
| Incident Reporting Procedure | How and when to report incidents, with real-life examples | Role-play / simulation | Bi-annually |

**Roles & Responsibilities**

* **Clinic Director**: Approves the training programme.
* **Practice Manager**: Coordinates training schedules, tracks completion.
* **IT Consultant**: Delivers technical content and conducts phishing simulations.
* **All Staff**: Attend training, apply knowledge, and report security incidents.

**Tracking & Compliance**

* Training completion is logged in staff files.
* Staff who miss deadlines receive follow-up reminders.
* Completion rates are reviewed quarterly and reported to the Clinic Director.

**Evaluation**

* Pre- and post-training quizzes to measure effectiveness.
* Annual phishing simulations to test awareness.
* Feedback surveys to improve future sessions.