**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.