Project 2: Risk Assessment

This project documents the risk assessment process for Southern Motion Physiotherapy. It identifies threats to critical assets, assesses their likelihood and potential impact, and prioritises them to guide risk treatment decisions. The assessment supports the clinic's efforts to reduce risk exposure, improve controls, and meet compliance expectations.

# Risk Criteria

Risks are assessed using two dimensions: Likelihood and Impact, each rated on a scale from 1 to 5. The Risk Rating is calculated as Likelihood × Impact.

Likelihood and Impact scale:

|  |  |  |
| --- | --- | --- |
| Rating | Likelihood | Impact |
| 1 | Rare | Negligible |
| 2 | Unlikely | Minor |
| 3 | Possible | Moderate |
| 4 | Likely | Major |
| 5 | Almost Certain | Critical |

Risk Rating Levels:

|  |  |
| --- | --- |
| Risk Rating | Level |
| 1–4 | Low |
| 5–9 | Medium |
| 10–15 | High |
| 16–25 | Critical |

# Risk Assessment Table

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Asset Affected | Risk Description | Likelihood | Impact | Risk Rating | Risk Level | Existing Controls | Suggested Treatment |
| PMS / EHRs | Unauthorised access to patient data | 4 | 5 | 20 | Critical | Passwords, basic access controls | Implement MFA, access logs |
| Clinic Laptops | Theft or loss of endpoint devices | 3 | 4 | 12 | High | Passwords | Device encryption, cable locks |
| Wireless Router | Misconfigured router leading to network breach | 3 | 4 | 12 | High | Changed default password | Firewall rules, config reviews |
| Microsoft 365 Email | Phishing attacks targeting staff | 4 | 3 | 12 | High | Basic training | Phishing simulations, spam filter |
| Cloud Backup Service | Data recovery failure | 2 | 4 | 8 | Medium | Automated weekly backups | Regular testing & validation |
| Xero Accounting Software | Financial fraud or unauthorised access | 3 | 5 | 15 | High | Login credentials only | Role-based access, MFA |
| Mobile Devices | Accidental data exposure from unlocked phones | 3 | 3 | 9 | Medium | PIN locks | MDM policy, remote wipe |
| Client Contact Info | Accidental email sent to wrong recipient | 3 | 2 | 6 | Medium | Manual double-checks | Email DLP, confirmation pop-ups |

# Risk Acceptance Justification

Risk: Accidental exposure of client contact data via email  
Justification: The clinic accepts this medium-level risk due to current operational limitations. Existing manual double-checks reduce likelihood. A longer-term solution (DLP) is being considered as part of future upgrades.