# ISO 27001:2022 Scoping Statement

**Organisation:** MindMend Health Pty Ltd
**Headquarters:** 22 Elgin Street, Carlton, VIC 3053, Australia

**Information Security Management System Scope Statement**
This ISMS is scoped to MindMend operations around the development, support, operations and provision of a virtual mental health service platform.

The scope encompasses all functions, systems, processes and personnel involved in the design, delivery and ongoing support of the following:

- Virtual Therapy
- Clinical Analytics
- Patient Insights

**The following departments deliver these services:**
- **Clinical** (Dr. Nina Hayes – MedRecordPro, MindMend Portal)
- **Engineering** (Priya Desai – GitHub, Jira, Snyk, AWS, Datadog)
- **Product** (Daniel Kim – Jira, Confluence, Segment)
- **Customer Support** (Lucy Chen – Zendesk, Twilio, Slack)
- **HR** (Laura Simmons – Employment Hero, Google Workspace)
- **Finance** (Mia Zhang – Xero, Stripe, Google Sheets)
- **Legal & Compliance** (Olivia Mercer – Drata, KnowBe4, Google Drive)
- **Marketing** (Jasper Quinn – Mailgun, HubSpot, Canva)

This scope includes all supporting infrastructure, internal information systems, cloud services, personnel, and third-party platforms used in providing, managing, and improving the above services. It incorporates technical, administrative, and virtualised controls designed to ensure:

- Confidentiality of client and company data
- Integrity of systems and information
- Availability of systems and services
- Secure operation of information assets
- Compliance with regulatory, contractual and customer requirements.

MindMend Health is a fully remote business with team members across Australia. It's infrastructure and systems are mainly cloud-hosted, utilising AWS as it's core cloud provider. The company's control environment encompasses remote employee endpoints, cloud services, and third-party integrations.

**Technology Platforms and Tools in Scope:**
- Cloud Infrastructure: AWS
- Email and Productivity: Google Workspace
- Identity and Access Management (IAM): Okta
- Communication Platform: Slack

- Endpoint Protection: CrowdStrike Falcon
- Mobile Device Management (MDM): Kandji
- Security Awareness Training: KnowBe4
- Vulnerability Scanning: Qualys
- Observability and Monitoring: Datadog
- Cloud Security Posture Management: Wiz
- Code Repository and Software Development: GitHub, Jira, Snyk
- HR Management: Employment Hero
- Customer Support: Zendesk, Twilio
- Marketing Communications: Mailgun, HubSpot, Canva
- Finance Systems: Xero, Stripe
- Clinical Management Systems: MedRecordPro, MindMend Portal
- Governance, Risk and Compliance (GRC) Management: Drata
- Document Management and Collaboration: Confluence, Google Drive, Google Sheets

**Exclusions:**
Based on the business's operational context, the following controls have been deemed not applicable following Annex A of ISO 27001:2022.

- **A.7.3—Securing Offices, Rooms, and Facilities:** Mindmend Health is a fully remote business, So It does not have any offices, rooms, or facilities to secure. MindMend Health uses AWS as its primary infrastructure provider, so the physical security controls related to securing facilities rest with AWS.
- **A.7.4 - Physical security monitoring:** As a fully remote business, MindMend Health does not have any offices, rooms, or facilities to monitor for unauthorised physical access. MindMend Health uses AWS as its primary infrastructure provider, so the responsibility for physical security monitoring rests with AWS.
- **A.7.5 - Protecting against physical and environmental threats:** MindMend Health is a fully remote business, so it does not need to guard against physical and environmental threats, such as natural disasters and other intentional or unintentional risks to its infrastructure. MindMend Health utilises AWS as its primary infrastructure provider, so the responsibility for protecting against these physical and environmental threats falls to AWS.
- **A.7.11 - Supporting Utilities:** MindMend Health is a fully remote business, so it does not need to protect its information processing facilities from power failures and other disruptions caused by failures in supporting utilities. Since MindMend Health utilises AWS as its main infrastructure provider, any power failures and disruptions caused by failures in supporting utilities are AWS's responsibility.
- **Third-party vendors and service providers** beyond the boundary of MindMend Health’s direct operational control, excluding those governed by the organisation's Vendor Management Policy or bound by explicit contractual security obligations.

**Purpose of Certification:**
The implementation and certification of ISO 27001:2022 aim to reinforce MindMend Health’s security posture, ensure compliance with regulatory requirements, safeguard client and patient data and support strategic growth through enhanced credibility with enterprise healthcare clients.

## ***Mind Mend Health Pty Ltd***

*MindMend Health is a fast-growing digital health startup founded in 2020, offering virtual mental health services across Australia. It provides an AI-powered therapy matching platform integrated with telehealth, analytics, and compliance tools for healthcare providers. With a fully remote team and operations across three Australian states, MindMend is aiming to achieve ISO 27001 certification within the next 12 months to strengthen its security posture and attract enterprise healthcare clients.*