**Mind Mend Health - As-Built Document**

**1. System Overview**

Client Name: MindMend Health Pty Ltd

Implementation Date: 12/05/25

Implementation Team: Olivia Mercer (GRC Lead), Taylor Brooks (Policy Owner), Amir Qureshi (Risk Manager), Jordan Lee (Security Lead), Priya Desai (Technical Lead)

**2. Compliance Frameworks**

* ISO 27001:2022 [Enabled]
* SOC 2 [Disabled]
* GDPR [Disabled]
* PCI DSS [Disabled]
* Custom Framework [Disabled]

**3. Module Configuration Status**

3.1 Core Modules

* Personnel:
  + Configured via Employment Hero.
  + Onboarding includes background checks and role-based access privileges.
  + Security training is delivered via KnowBe4 with automated assignments.
* Assets: Asset inventory tracked in:
  + Kandji
  + AWS tagging
  + Endpoints and cloud workloads are monitored via:
    - CrowdStrike
    - Datadog.
* Policies all published and tracked in the policy library. Versioning and quarterly reviews are configured:
  + Remote Work
  + Vendor Management
  + Data Retention
* Controls:
  + Mapped in Drata to ISO 27001.
  + Evidence collected via automated API key integrations (AWS, Okta, GitHub) and monthly manual uploads.

3.2 Integrations

* HR System: Employment Hero [Active]
* SSO: Okta [Active - SCIM sync in use]
* Cloud Services: AWS, Google Workspace [Active]
* Monitoring Tools: Datadog, CrowdStrike Falcon [Active]

**4. Custom Configurations**

4.1 Custom Controls

* Vendor Risk Assessments mapped to ISO 27001 A.15
* Automated evidence collection tied to AWS CloudTrail, S3 bucket access logs

4.2 Custom Policies

* Vendor Management Policy
* Remote Work Policy
* Data Retention Policy
* All policies follow quarterly review cycles and version control

4.3 Custom Workflows

* Automated vendor onboarding and assessment flow
* Risk register auto-linking flagged vendors
* Policy acknowledgement tracking

**5. Access Management**

* Super Admins: Jordan Lee (Security Lead)
* Admin Users: Priya Desai (Technical Lead), Olivia Mercer (GRC Lead)
* Regular Users: Managed via Okta Cross-Domain Identity Management (SCIM) groups
* Role Configurations: Align to department leads (Engineering, Clinical, Compliance)

**6. Evidence Collection**

* Automated: AWS, Kandji, Okta, CrowdStrike, Datadog integrations
* Manual: Uploaded by the Risk Manager monthly (Amir Qureshi)

**7. Monitoring & Alerts**

Alerts Configured for:

* IAM changes
* Critical file access events
* Suspicious login and geographic anomalies

**8. Training & Documentation**

* KnowBe4 active
* Policy library walkthrough conducted 09/05/25
* Teams notifications are enabled for control failures and review reminders

**9. Outstanding Items**

| **Item** | **Status** | **Next Steps** | **Owner** |
| --- | --- | --- | --- |
| Quarterly Internal Audit | Scheduled | Assign Audit Tasks | Olivia Mercer (GRC Lead) |
| Final Vendor List Review | In Progress | Confirm Vendor Tiers | Amir Qureshi (Risk Manager) |

**10. Maintenance Schedule**

* ISMS Review: Quarterly
* Policy Update Review: Quarterly
* Access Review: Monthly
* Drata Sync and Control Check: Weekly

Version Control

Version: 1.0

Date: 08/05/25

Author: Jason King

Changes: Initial Draft