Information Security Management System (ISMS) Plan

Purpose

The purpose of this Information Security Management System (ISMS) Plan is to establish, implement, maintain, and continually improve the information security practices of MindMend.

This plan aligns with ISO 27001:2022 standards and covers all business processes and activities related to the development, maintenance, and delivery] of MindMend's SaaS platform. It ensures the confidentiality, integrity, and availability of information assets, thereby supporting the company's objectives and legal obligations.

Background and Objectives

Background

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.

Business-Aligned Objectives

- Protect customer and company information from unauthorised access, disclosure, alteration, and destruction.
- Comply with all applicable legal, regulatory, and contractual requirements.
- Establish a framework for setting, monitoring, and achieving information security objectives.
- Promote a culture of security awareness among all employees and stakeholders.
- Continually improve the ISMS to adapt to evolving threats and business needs.

ISMS Framework

The ISMS framework is based on the ISO 27001:2022 standard and incorporates the Plan-Do-Check-Act (PDCA) cycle to ensure continuous improvement. The framework integrates policies, procedures, guidelines, and resources to manage and protect information assets effectively.

4. Context of the Organisation

4.1 Understanding the Organisation and Its Context

MindMend operates in the SaaS space providing customers with AI-powered therapy matching platform integrated with telehealth, analytics, and compliance tools for healthcare providers. To effectively manage information security risks and achieve its objectives, the following internal and external factors must be considered.

Internal Issues & Factors

1. **Organisational Structure and Identity**
    - **Leadership Team**: Comprised of multiple key roles, including CEO (Dr. Nina Hayes), Security Officer (Jordan Lee), Privacy Officer (Jordan Lee), and Risk Manager (Amir Qureshi)
    - **Security Committee**: Responsible for overseeing the security of operations, services, and systems, ensuring a collaborative approach to security management.
    - **Support Functions**: Including IT, Human Resources, finance, and administrative support
    - **Organisation Identity**: Company culture, values, mission, and vision

2. **Technological Infrastructure**
    - **On-premises Infrastructure**: Supporting internal operations and client services
    - **Cloud Services:** Requiring robust cloud security measures and adherence to best practices.
    - **Software Development Practices:** MindMend follows a secure Software Development Life Cycle (SDLC), integrating security reviews, static code analysis, and CI/CD pipeline controls across tools such as GitHub, Jira, Snyk, and AWS. Security is embedded from requirements through to deployment and monitoring.
    - **Data Storage and Processing:** Management of sensitive or confidential data necessitates secure data storage, encryption at rest and in transit, and strict access controls.
    - **Security Operations Centre**: Monitoring and responding to security incidents

3. **Service Delivery Model**
    - **SaaS Platform Delivery:** AI-powered mental health service platform, offered on a subscription basis.
    - **Telehealth Integration:** Virtual care delivery tools for mental health providers and clients.
    - **Data & Compliance Tools:** Real-time analytics and privacy-focused compliance features.
    - **Cloud-Only Operations:** Fully remote, cloud-native infrastructure with no on-premise deployments.
    - **No Consulting/Managed Services:** MindMend does not offer project-based, advisory, or traditional IT services.

4. **Internal Policies**
    - Comprehensive policy framework covering all aspects of operations
    - Regular review and update cycles
    - Compliance monitoring and enforcement

5. **Employee**
    - **Expertise & Training:** Maintain high skill levels through regular training to stay current with threats, technologies, and compliance.
    - **Security Awareness:** Foster a workplace culture where all employees understand and uphold their responsibilities in maintaining security.

External Issues & Factors

1. **Legal and Regulatory Requirements**
    - Privacy Act 1988
    - Notifiable Data Breaches (NDB) Scheme
    - Cyber Security Act 2024
    - Spam Act 2003
    - Crimes Act 1914
    - State-specific Surveillance Act
    - ISO/IEC 27001 Information Security Management Systems (Standard)
    - Cybercrime Act 2001
    - Work Health and Safety Act
    - Fair Work Act 2009
    - Corporations Act 2001
    - Copyright Act 1968
    - State-specific privacy legislation
    - Industry-specific regulations affecting clients
    - ISO 27001: 2022

2. **Market Conditions**
    - Increasing demand for secure cloud solutions
    - Growing cybersecurity threats and awareness
    - Competitive services market in Australia
    - Rapid technological advancement

3. **Client Requirements**
    - Diverse industry sectors with varying compliance needs
    - High expectations for service availability and security
    - Growing demand for digital transformation
    - Need for cost-effective solutions

4. **Technology Landscape**
    - Emerging technologies (AI, ML, IoT)
    - Cloud computing trends
    - Cybersecurity threats and solutions
    - Industry standards and best practices

5. **Environmental Impact**
    - Eco-friendly practice
    - Carbon footprint reduction
    - Green technology and reducing e-waste

4.2 Understanding the Needs and Expectations of Interested Parties

Interested Party	**Needs and Expectations**
Clients	- Secure and reliable IT/SaaS services - Compliance with regulatory requirements - Transparent communication - Rapid incident response
Employees	- Clear security policies and procedures - Regular training and development - Safe working environment - Tools and resources to perform securely
Partners/Vendors	- Clear security requirements - Efficient collaboration processes - Fair and transparent relationships
Regulators and Accreditation Bodies	- Compliance with Australian laws, regulations and/or frameworks - Timely reporting and disclosure - Adequate security controls
Shareholders	- Protection of company assets - Sustainable growth - Risk management - Return on investment

4.3 Determining the Scope of the ISMS

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.

Scope overview

Organisational Units:

- Engineering
- Product
- Customer Support
- Legal & Compliance
- Clinical
- Marketing
- Human Resources
- Sales
- Executive Leadership

Systems and Applications:

- **AWS** – Cloud infrastructure (hosting, storage, and compute)
- **GitHub** – Source control and development lifecycle
- **Jira & Confluence** – Task management and documentation
- **Datadog & Snyk** – Security monitoring, logging, and vulnerability management
- **Segment & Twilio** – Customer data and communication infrastructure
- **Google Workspace** – Email, calendars, documents, and internal collaboration
- **Drata** – ISMS and compliance automation
- **Stripe & Xero** – Financial systems
- **KnowBe4** – Security awareness training platform
- **Slack, Mailgun, HubSpot, Canva –** Internal and external communication and marketing tools

Business Processes:

Business Process	Department Head	Brief description of their work
Engineering	Priya Desai	Develops and maintains MindMend’s SaaS platform, infrastructure, and security integrations.
Product	Daniel Kim	Defines platform features, roadmap, and user experience; works closely with Engineering and Clinical.
Customer Support	Lucy Chen	Handles support tickets, technical issues, and user inquiries cross the platform.
Clinical Operations	Dr. Nina Hayes	Oversees clinical governance, safety protocols, therapist onboarding, and service quality assurance.
Legal & Compliance	Olivia Mercer	Manages privacy, regulatory compliance, contracts, and ISO/IEC 27001 implementation.
Finance	Mia Zhang	Oversees financial operations including budgeting, payroll, revenue reporting, and SaaS billing models.
Human Resources	Laura Simmons	Leads recruitment, onboarding, engagement, policy management, and remote workforce support.
Marketing	Jasper Quinn	Drives brand strategy, campaigns, customer engagement, and communications.
Sales & Partnerships	Ethan Rawlins	Manages sales strategy, lead generation, enterprise client onboarding, and partnership development.
Executive Leadership	Dr. Nina Hayes	Provides overall strategic direction, governance, and organisational oversight.

Locations:

Address	Description
22 Elgin Street, Carlton, VIC 3053, Australia	Head Office
N/A	Regional Office

The following are out of scope:

- Third-party systems and environments not owned or managed by MindMend (e.g. client IT systems).
- On-premises systems operated by clients or partners.
- Any physical infrastructure, as MindMend operates in a fully remote capacity.
- Third-party tools and services where MindMend is a consumer and does not manage infrastructure (e.g. hosted SaaS tools like Stripe, HubSpot, Canva).
- Vendors and subcontractors operating independently under their own security and compliance obligations, outside of formal contractual control.

The following locations are out of scope:

- **Not applicable – MindMend does not maintain any physical office or on-site infrastructure due to its fully remote operating model.**

5. Leadership

5.1 Leadership and Commitment

The Executive Management demonstrates leadership and commitment to the ISMS by:

- Establishing and maintaining the information security policy and objectives
- Ensuring integration of ISMS requirements into business processes
- Providing necessary resources for effective ISMS implementation
- Communicating the importance of effective information security management
- Supporting continuous improvement initiatives
- Promoting risk-based thinking in all security-related decisions

Information Security Governance Structure

Executive Management Committee

- Reviews and approves ISMS strategy and major initiatives
- Ensures alignment with business objectives
- Provides resources and support for ISMS implementation
- Quarterly review of ISMS performance

Information Security Steering Committee

- Meets regularly to oversee ISMS implementation
- Reviews security metrics and KPIs
- Approves security policies and procedures
- Ensures cross-functional coordination

Roles and Responsibilities

Role	**Primary Responsibilities**
Chief Executive Officer (Dr Nina Hayes)	• Provides strategic direction and approves ISMS scope and resources • Promotes a security-first culture
Chief Compliance Officer (Olivia Mercer)	• Owns the ISMS and ensures regulatory compliance • Manages audits, risks, and performance reporting
Head of Engineering (Priya Desai)	• Implements security controls across code and infrastructure • Leads incident response and patch management
Head of Product (Daniel Kim)	• Embeds security into product development • Participates in change and risk management processes
Clinical Director (Dr. Nina Hayes)	• Oversees PHI/PII safeguards in clinical systems • Provides input into clinical risk assessments
Head of People & Culture (Laura Simmons)	• Manages onboarding/offboarding security practices • Delivers training and enforces acceptable use policies

5.2 Policy Framework

The leadership team has established an Information Security Policy that is available as documented information, managed, and communicated to employees via Drata GRC platform. Management may also make the Information Security Policy available to external parties in certain circumstances as deemed appropriate (e.g., to satisfy due diligence requests from prospects, etc).

Through the establishment and implementation of the Information Security Policy, management is committed to satisfying applicable requirements related to information security and continuously improving the ISMS.

In addition to this plan and the Information Security Policy, management has established and implemented topic-specific policies to support the implementation of information security controls in specific areas of and security areas. These topic-specific policies will be managed and made available to employees via Drata GRC platform:

- Acceptable Use Policy
- Access Control Policy
- Asset Management Policy
- Backup Policy
- Business Continuity Plan
- Change Management Policy
- Code of Conduct
- Data Classification Policy
- Data Protection Policy
- Data Retention Policy
- Disaster Recovery Plan
- Document Control Policy
- Encryption Policy
- Incident Response Plan
- Information Security Policy
- Information Security Risk Management Framework
- Logging and Monitoring Policy
- Network Security Policy
- Password Policy
- Physical Security Policy
- Vendor Management Policy
- Vulnerability Management Policy

These policies provide a framework for setting and reviewing information security objectives and are available to all employees.

5.3 Organisational Roles, Responsibilities, and Authorities

The following roles and responsibilities serve as a summary of the key roles of people that form part of this ISMS.

Role	Assigned Person	Job Title	ISMS Responsibilities	Required Competencies
ISMS Leadership	Dr. Nina Hayes	CEO	Sponsor ISMS, allocate resources, align security with business goals	Leadership, strategy, risk understanding, ISO awareness
	Olivia Mercer	Chief Compliance Officer (CCO)	Oversee ISMS governance, review effectiveness, approve controls	Regulatory knowledge, decision-making, governance
ISMS Manager	Olivia Mercer	CCO	Maintain ISMS framework, report risks, update policies, oversee awareness & incident response	ISO 27001 experience, stakeholder management, policy implementation
Security Risk Committee	Olivia Mercer	CCO	Assess risk, recommend treatment, make decisions on controls	Risk analysis, compliance knowledge, governance judgment
	Priya Desai	Head of Engineering	Identify technical risks, advise on security control implementations	System architecture, vulnerability knowledge, DevSecOps
	Daniel Kim	Head of Product	Participate in product-related risk reviews	Product security, feature risk assessment
HR Manager	Laura Simmons	Head of People & Culture	Handle onboarding, training, background checks, and employee security awareness	HR compliance, training skills, onboarding/offboarding management
Privacy Officer/Legal	Olivia Mercer	CCO	Data protection, privacy compliance, DPIAs, and privacy training	Privacy law, GDPR, communication, assessment skills
IT/DevOps Manager	Priya Desai	Head of Engineering	Manage incident response, maintain security tooling, enforce secure DevOps practices	Secure infrastructure, technical recovery, control integration, system-level security
All Employees	All staff	All roles	Follow information security policies relevant to their role Protect sensitive and personal data Comply with security policies as a condition of employment • Understand that violations may lead to disciplinary action	• Awareness of security policies and role-based controls • Understanding of common threats • Familiarity with data classification • Ability to identify and report incidents effectively

All roles have documented responsibilities in role descriptions and are reviewed annually to ensure alignment with ISMS objectives.

6. Planning

6.1 Actions to Address Risks and Opportunities

6.1.1 General

Information security risks and opportunities are identified through regular assessments to ensure the ISMS remains effective and is continually improved.

6.1.2 and 8.2 Information Security Risk Assessment

For this purpose, a methodology for risk assessment was established which will include the following:

- Process for identifying risks that could cause the loss of confidentiality, integrity, and/or availability of information
- Identification of risk owners
- Assessment of consequences and the likelihood of risks

Risk assessment process is conducted as outlined in the Information Security Risk Management Framework. A risk assessment is conducted at least annually to identify threats to information assets.

6.1.3 and 8.3 Information Security Risk Treatment

Risk treatment involves selecting appropriate controls to mitigate identified risks, documented in the Risk Treatment Plan. Controls are selected from ISO 27001 Annex A and implemented following the Risk Management Framework.

The following documents and activities are managed as part of risk treatment:

- **Risk Treatment Plan.** The Risk Treatment Plan is a crucial part of the ISMS implementation. A treatment plan will be documented for every identified risk, which will include the necessary controls to modify risk, responsible party, and as deemed necessary, timing and intervals, and allocated resources/budgets.
- **Evaluation of Effectiveness.** MindMend will measure and evaluate the fulfilment and effectiveness of the controls in place and other ISMS objectives in place.
- **Statement of Applicability.** The Statement of Applicability (SOA) links risk assessment and treatment with the implementation of the ISMS. The SOA will list all controls identified by MindMend to be necessary to implement the risk treatment plan based on the results of the risk assessment. This may include ISO 27001 Annex A controls, controls from other frameworks, custom controls deemed necessary by the organisation, etc. The SOA will indicate any controls that are not deemed necessary to treat an identified risk as justification for exclusion. Each control in the SOA will have implementation status and implementation details. Refer to **Appendix 1** for the Statement of Applicability.

6.2 Information Security Objectives and Planning to Achieve Them

MindMend has established the following SMART (Specific, Measurable, Achievable, Relevant, Time-bound) information security objectives:

Summary	Description	Metric	Metric Owner
Ensure Business Continuity	Develop, maintain, and test business continuity plans, including information security continuity, to safeguard systems and services.	● Annual Incident Response Plan completed ● Annual BCP, DR Tests completed	**Olivia Mercer** (CCO) **Priya Desai** (Engineering)
Strengthen Incident Response	Ensure all information security breaches and weaknesses are promptly reported, investigated, and resolved to mitigate risks.	● No major information security incidents ● All incidents resolved within response times ● PIRs completed for all incidents	Olivia Mercer (CCO)

Summary	Description	Metric	Metric Owner
Safeguard Information Assets	Protect organisational information from unauthorised access, accidental disclosure, or compromise, maintaining confidentiality, integrity, and availability.	• 100% critical CVEs resolved within SLA • 95% high-priority issues remediated within 14 days	**Priya Desai** (Engineering)
Enhance Compliance and Risk Management	Meet regulatory and legislative requirements while providing frameworks for assessing and mitigating security risks.	• ISO 27001 audit with <2 major NCs and <5 minor NCs • All findings tracked and closed in Drata	**Olivia Mercer** (CCO)
Promote Security Awareness and Trust	Foster a culture of security awareness and build customer trust by delivering secure services and transparent security practices.	• 100% completion of annual security training • <10% phishing failure rate • Customer trust score (survey) • Timely response to security questionnaires	**Laura Simmons** (HR) **Jasper Quinn** (Marketing) **Olivia Mercer** (CCO)

6.3 Planning of Changes

All changes to the ISMS or related processes are planned and documented according to the **Change Management Policy**. This includes impact assessments, resource allocation, and communication plans.

7. Support

7.1 Resources

MindMend allocates necessary resources for the establishment, implementation, maintenance, and continual improvement of the ISMS, including:

- Personnel with defined roles and responsibilities.
- Technological tools for security monitoring and management.
- Financial resources for training and system upgrades.

7.2 Competence

Employees are assessed for competency in information security relevant to their roles. Training and professional development opportunities are provided to fill any gaps.

Specific to the ISMS, the required competencies are defined in the section ‘5.3 Organisational Roles, Responsibilities, and Authorities’.

7.3 Awareness

All employees are made aware of:

- The ISMS policies and their responsibilities.
- The importance of information security.

- The potential impact of non-compliance.

This is reinforced through regular training sessions. Refer to the **Code of Conduct** and **Acceptable Use Policy**.

7.4 Communication

Internal and external communications relevant to the ISMS are determined by:

- **What**: Information to be communicated.
- **When**: Frequency and timing.
- **With Whom**: Stakeholders and interested parties.
- **How**: Methods and channels of communication.

Communication plans are documented in the **Communication Plan (Appendix 2)**.

7.5 Documented Information

7.5.1 General

The following table includes the documents determined by MindMend as being necessary for the effectiveness of the ISMS.

MANDATORY RECORDS & DOCUMENTS

Document	**Reference**	**Location**
Scope of the Information Security Management System (ISMS)	Clause 4.3	ISMS Plan
Information Security Policy	Clause 5.2	Drata GRC Platform
Information Security Objectives	Clause 6.2	ISMS Plan
Risk Assessment Process	Clause 6.1.2	Risk Management Framework
Risk Assessment Results	Clause 8.2	In Drata GRC Platform
Risk Treatment Process	Clause 6.1.3	Risk Management Framework
Risk Treatment Plan	Clause 6.1.3e	In Drata GRC Platform
Statement of Applicability	Clause 6.1.3d	ISMS Plan
Competence (e.g., Skills Matrix & Associated Proof of Skills)	Clause 7.2	ISMS Plan / In Drata GRC Platform
Monitoring & Measurement Results	Clause 9.1	Drata GRC Platform
Internal Audit Plan & Reports	Clause 9.2	Drata GRC Platform
Results of Management Reviews of ISMS	Clause 9.3	Drata GRC Platform

Document	Reference	Location
Nonconformities, Corrective Actions & Improvement Suggestions	Clause 10.1; 10.2	Drata GRC Platform

7.5.2 and 7.5.3 Creation and Control of Documented Information

Document control across the ISMS, including version control, approval, access permissions, retention, and disposal, is managed through the organisation's Document Control Policy. This policy outlines how documented information is created, updated, reviewed, published, and retired. It applies to all ISMS-related documents, including policies, procedures, risk assessments, audit records, and other supporting information. The Document Control Policy is owned and maintained by the GRC function and is accessible to all staff via the corporate policy portal.

9. Performance Evaluation

9.1 Monitoring, Measurement, Analysis, and Evaluation

MindMend will evaluate its security objectives by monitoring and measuring the implemented controls. Monitoring provides awareness of the status and state of assets and processes that have been selected to be watched and can provide basic and immediate alerts if something is not performing as expected. These evaluations are meant to allow MindMend to:

- Ensure control objectives are being satisfied and validate the decisions made.
- Establish a roadmap to meet set targets and expectations.
- Produce evidence and justification for implemented measures; and/or,
- Discover and identify security gaps that would require change, corrective actions, or intervention.

Systems, Processes, and Activities Monitored/Measured:

- ISMS Implementation
- Incident Management (measured)
- Vulnerability Management (measured)
- Configuration Management
- Resource Management
- Security Awareness and Training (measured)
- Access Control, Firewall, and other Event Logging
- Audits (measured)
- Policy Management
- Risk Assessment Process
- Risk Treatment Process
- Third Party Risk Management
- Business Continuity Management (measured)
- Physical and Environmental Security Management
- System Monitoring
- Management Review

9.2 Internal Audit

Internal audits are conducted annually to assess the ISMS's conformity to ISO 27001 and effectiveness. The **ISMS Internal Audit Program and Procedure (Appendix 3)** outlines the audit process, criteria, scope, and responsibilities.

9.3 Management Review

The leadership team conducts a review of the ISMS to ensure its continuing suitability, adequacy, and effectiveness. The review includes assessing opportunities for improvement and the need for changes to the ISMS.

Management Reviews will be conducted using the guidelines specified in ISO 27001:2022 and follow a set standard. Management Reviews will be conducted at least annually.

10. Improvement

10.1 Continual Improvement

MindMend is committed to the continual improvement of the ISMS by:

- Monitoring performance and feedback.
- Implementing corrective actions.
- Keeping abreast of new threats and technologies.

10.2 Nonconformity and Corrective Action

Nonconformities are managed according to the **Nonconformity and Corrective Action Procedure (Appendix 5)**, which includes:

- Identifying and documenting the nonconformity.
- Determining the cause.
- Implementing corrective actions.
- Reviewing the effectiveness of the actions taken.

Change History

Version	**Date**	**Author**	**Approver**	**Changes**
1.0				Initial release

Appendix 1

Statement of Applicability

Our Statement of Applicability is dynamically in our Drata GRC platform and annually reviewed and added as a spreadsheet into our Drata GRC platform.

Appendix 2

ISMS Communication Plan

This communication plan outlines the lines of communication within the organisation, and with outside entities, to include appropriate government agencies (e.g., law enforcement) and non-governmental organisations. It also defines times and intervals, events and situations, and personnel responsible for the communication

Document	Frequency	Sender	Audience	Delivery Type	Delivery Evidence
Internal Audit Report	Annually	Internal Auditor, Member of Security Team	The Leadership Team, ISMS Implementation	Email, Presentations, Reports & Docs	Email, Committee Meeting Minutes, Drata GRC Tool
External Audit Report	Annually	External Auditor, Member of Security Team	Information Security Officer, Security Committee, Board of Directors	Email, Presentations	Security Committee and/or Board of Directors Closing Meeting Minutes
ISO 27001 Certificate	As necessary	Information Security Officer	Customers, Prospects	Email, Drata GRC Tool	Email, Drata GRC Tool report
ISMS Security Objectives	Annually	Member Responsible for Developing Objectives	Business Unit Leadership for Security Objectives	Email, Meetings	Meeting Minutes
Risk Assessment Report	Annually	Risk Assessment Manager, Information Security Officer	Leadership Team, Security Committee	Email, Reports	In Drata GRC Tool, Review Minutes
Incident Response Reports	Per Incident	Incident Response Manager, Information Security Manager	Leadership, Security Team, Affected Parties, Law Enforcement (if applicable), Authorities (if applicable), other stakeholders (if applicable)	Email, Meetings	Incident Logs, Post-Incident Review
Security Awareness Training Plan	Annually	Training Coordinator, Information Security Officer	Applicable Employees, Contractors and other stakeholders	Email, LMS	Training Completion Records
Policy Updates	As necessary	Policy Owner	Applicable Employees, Contractors and other stakeholders	Email, Intranet	Acknowledgement Receipts

Appendix 3

ISMS Internal Audit Program and Procedures

The ISMS Internal Audit Program is designed to ensure that:

- Systematic coverage of all ISMS elements
- Clear responsibilities and expectations
- Consistent documentation and reporting
- Measurable outcomes and improvements
- Alignment with MindMend's objectives

1. Program Overview

Element	**Description**
Frequency	Annual comprehensive ISMS audit with rolling control audits throughout the year
Coverage	Full ISO 27001:2022 requirements and controls over a 3-year certification cycle
Responsibility	ISMS Owner
Documentation	Maintained in MindMend's ISMS documentation system

2. eAnnual Audit Schedule

Period	**Focus Area**	**Scope**
Year 1	ISMS Foundation (Clauses 4-7)	Context, Leadership, Planning, Support
	Operations (Clause 8)	Operational planning, risk treatment, controls
	Performance (Clauses 9-10)	Monitoring, measurement, improvement
	Annex A Controls	A.5.7, A.5.23, A.5.30, A.7.4, A.8.9, A.8.10, A.8.11, A.8.12, A.8.16, A.8.23, A.8.28
Year 2	Operations (Clause 8)	Operational planning, risk treatment, controls
	Performance (Clauses 9-10)	Monitoring, measurement, improvement
	Annex A Controls	A.5.x and A.8.x
Year 3	ISMS Clauses and Annex A Controls	Complete ISO 27001 standard

3. Auditor Requirements

Requirement Type	Criteria
Independence	Must not audit their own work/department
Qualifications	ISO 27001 Lead Auditor certification or equivalent experience
Experience	Minimum 2 years in IT/Security roles
Training	Annual refresher on audit techniques and ISO requirements

4. Audit Process Flow

Phase	Activities	Outputs
Planning	- Review previous findings - Define scope - Select auditor - Prepare schedule	Audit Plan
Preparation	- Document review - Prepare checklists - Notify participants	Audit Checklist
Execution	- Opening meeting - Evidence collection - Interviews - Documentation review	Audit Notes
Reporting	- Draft findings - Closing meeting - Final report	Audit Report
Follow-up	- Track actions - Verify closure - Update ISMS	Action Register

5. Documentation Requirements

Document	Content	Retention
Audit Plan	Scope, schedule, resources	3 years
Audit Reports	Findings, recommendations, evidence	3 years

Document	Content	Retention
Action Plans	Corrective actions, timelines, owners	3 years
Competency Records	Auditor qualifications and training	Duration of employment

6. Reporting Template

Section	Required Information
Executive Summary	Overall assessment and key findings
Scope	Areas/processes covered
Methodology	Approach and techniques used
Findings	Categorised as Major/Minor/Observation
Recommendations	Specific actions for improvement
Action Plan	Timeline and responsibilities

7. Performance Metrics

Metric	Target	Measurement
Audit Completion	100% of planned audits	Quarterly
Finding Closure	90% within agreed timeframes	Monthly
Audit Quality	95% acceptance of findings	Per audit
Control Coverage	100% over 3 years	Annual

8. Special Considerations

- Integration with ISO 27001:2022 transition requirements
- Focus on MindMend's core services (Cloud, MSP, Infrastructure)
- Consideration of client data protection requirements
- Alignment with Australian regulatory requirements
- Exclusion of cloud service controls not managed by MindMend.

Appendix 4

Nonconformity and Corrective Action Procedure

This procedure establishes a systematic process for identifying, documenting, and addressing nonconformities within the ISMS to ensure continuous improvement. It applies to all nonconformities identified within the ISMS through audits, reviews, or daily operations.

A nonconformity is the non-fulfilment of an ISMS or ISO 27001:2022 requirement A corrective action is a set of actions to eliminate the cause and prevent recurrence of the nonconformity.

Once a nonconformity is identified, the Dr. Nina Hayes (CEO) & Olivia Mercer (GRC Lead [Legal & Compliance]) or an appointed delegate will oversee the process and verify effectiveness. The management team will review significant issues and allocate resources

Procedure

Identification and Recording

1. Nonconformities can be identified through:
    - o Internal/external audits
    - o Management reviews
    - o Employee observations
    - o Monitoring activities
    - o Customer feedback
2. All nonconformities must be logged in Drata GRC platform

Initial Response

1. Implement immediate containment actions if required
2. Document actions taken in Drata GRC platform

Root Cause Analysis

1. Process Owner conducts root cause analysis
2. Use appropriate technique (e.g., “5 Whys”)
3. Document findings in Drata GRC platform

Corrective Actions

1. Develop actions to address root cause
2. Assign responsibilities and timelines

3. Update Drata GRC platform with action plan
4. Jordan Lee (Security Lead) / Olivia Mercer (Legal and Compliance) reviews and approves plan

Implementation

1. Execute approved corrective actions
2. Update progress in Drata GRC Platform
3. Document evidence of implementation

Verification

1. Jordan Lee (Security Lead) / Olivia Mercer (Legal and Compliance) verifies effectiveness
2. Document verification results in Drata GRC Platform
3. Close if effective, or develop new actions if needed

Monitoring and Review

1. Jordan Lee (Security Lead) / Olivia Mercer (Legal and Compliance) reviews nonconformity trends quarterly
2. Include analysis in Management Review
3. Review procedure annually

Records

1. All records maintained in Drata GRC Platform
2. Access restricted to authorised personnel

Version	Date	Description	Author
v1.0	28-May-2025	Finalised ISMS Plan for ISO/IEC 27001 audit readiness	Olivia Mercer