healthOS

SECURITY POLICY

Information Security Policy

How HealthOS protects the information it holds, who is accountable, how information is classified and handled, and the suppliers involved.

Edition November 2026 · Public edition · Security: security@healthos.net.au

Contents

Purpose 2

Scope 2

Objectives 3

Roles and accountability 3

Principles 3

Information classification and handling 4

Access control 4

Acceptable use 5

Suppliers 5

The policy set 6

Exceptions 7

Breaches of this policy 7

Purpose

HealthOS holds health information about people on behalf of the organisations that care for them, and connects to government systems that trust it to behave. This policy states how that information is protected, who is accountable, and which documents carry the detail. Every other policy in this directory sits under this one.

Scope

- **Information:** customer data (personal and health information held for a tenant), information obtained from government systems, source code, credentials and keys, and the organisation's own business records.
- **Systems:** every deployed HealthOS stack on Azure, the GitHub repositories and CI, the marketing websites, and the devices and accounts used to build and operate them.
- **People:** everyone covered by Personnel Security.

Customer-hosted installations are in scope for the software and out of scope for the hosting, which is the customer's.

Objectives

1. **Confidentiality.** A person's information is seen only by people with a reason to see it, and one tenant's information never reaches another.
2. **Integrity.** Records are accurate, and every change is attributable.
3. **Availability.** The service and its data can be restored within the times in infra/BACKUP-AND-RECOVERY.md.
4. **Compliance.** The Privacy Act 1988 and the Australian Privacy Principles, the My Health Records Act and Healthcare Identifiers Act, the NDIS Act where NDIA information is held, and the terms of each government and licensor agreement are met.

How well these are being met is measured by these measures, reported to the director quarterly in the ISMS review: open findings by severity; the age of the oldest unapplied critical or high patch; the last restore drill date and result; incidents and near misses; access reviews completed on time; training completion.

Roles and accountability

ROLE	WHO	ACCOUNTABLE FOR
Directors	Aaron Le Saux (sole director)	Approving this policy and the risk appetite; resourcing security
Security owner	Aaron Le Saux	This policy set, the risk register, the incident response, assessor liaison
Privacy officer	Aaron Le Saux (privacy@healthos.net.au)	Privacy Act compliance, data breach assessment and notification
Engineering	Everyone who changes the system	Building to the rules below, and reporting what they see
Everyone	—	Following this policy and reporting suspected incidents at once

Principles

These are how the system is built, and each can be checked in the repository.

- **Tenant isolation in three layers.** Every tenant route requires an organisation context, runs in an organisation-scoped transaction, and reads tables under forced row-level security. The runtime database role cannot bypass it. A check (`verify:tenant-isolation`) fails a deployment where that is not true.
- **Least privilege.** Role-based access with facility and ward scope inside the application; a separate, narrower database role for the patient portal; managed identities instead of stored keys where the platform allows.
- **Secure by default.** Production refuses to start on a missing, short or reused signing secret. Mock and sandbox modes are refused in production unless explicitly allowed. Outbound connections to private networks and plain HTTP are off in production.

- **Defence in depth.** No single control is relied on: a route check and row-level security; platform encryption and field encryption for credentials; a classifier and separate signing secrets per token class.
- **Everything is attributable.** Reads and changes of clinical records are logged in append-only tables kept seven years (Audit Logging).
- **Data stays in Australia.** Stacks are deployed to Azure `australiaeast`. The one qualification is recorded under suppliers below.

Information classification and handling

CLASS	WHAT IT IS	HANDLING
Restricted	Health information and government identifiers (IHI, Medicare, DVA, NDIS numbers); information obtained from government systems, including NDIA Protected Agency Information; credentials, keys and certificates; licensed classification material	Stored only in the production data stores and vaults, encrypted at rest and in transit. Never in a repository, a ticket, an email, a chat, a log or a lower environment. Access is by role and is logged. Licensed classification material has further rules in the repository's `CLAUDE.md`
Confidential	Other personal information; customer configuration and contracts; source code; security assessments, pen test reports and this risk register; unreleased plans	Shared on a need-to-know basis inside the organisation. Sent outside only under a confidentiality agreement and over an encrypted channel
Internal	Working documents, procedures, internal communications	Not published; no special handling beyond that
Public	The website, published guides, published specifications	No restriction

Rules that follow from the table:

- **No production data outside production.** Development and testing use the seeded fictional tenants, never a copy of a customer's data (secure-development.md).
- **Support access to customer data** happens only on a customer's request, through a named account, and is logged like any other access.
- **Retention.** Clinical and audit records are kept for the periods the law and the customer's own obligations set; SaaS workspace retention is in saas-data-retention.md.
- **Disposal.** Data is deleted from the live stores on the retention schedule and ages out of backups within the backup retention (35 days). Equipment that held Confidential or Restricted information is wiped before reuse or disposal.
- **De-identified is not public.** De-identified clinical text sent to an AI service is still handled as Confidential.

Access control

- Every account belongs to one named person. Shared accounts are not used; where a platform forces a shared administrator credential it is held in Key Vault and its use is logged.

- Multi-factor authentication is required on GitHub, Azure and every application administrator account.
- Passwords are checked against known breaches and stored as bcrypt hashes; the product's own password and session policy is set per organisation.
- Access is granted on request and approval, revalidated every six months, and removed on the day someone leaves or changes role (backup-restoration-and-privileged-access.md).

Acceptable use

People covered by this policy:

- use organisation systems and customer data only for the work they are engaged to do;
- work on devices that have full-disk encryption, a screen lock, a supported and patched operating system, and are not shared;
- keep credentials in a password manager, never in a file, a note or a message, and never reuse one across services;
- do not copy Restricted information to a personal device, personal cloud storage or removable media;
- do not paste Restricted information into any external tool or AI service that is not on the supplier list below for that purpose;
- report a lost device, a suspicious message or a mistake at once. Reporting a mistake quickly is the expected behaviour and is never penalised.

The device standard: full-disk encryption on; screen lock at 5 minutes or less; a supported operating system with automatic updates; built-in anti-malware on; no shared accounts. The owner checks it quarterly and records the check in SharePoint: HealthOS ISMS > Asset and device register.

Suppliers

A supplier that stores or processes Confidential or Restricted information is assessed before use and reviewed every year. The assessment records what the supplier holds, where, under what terms, and what independent assurance it has (a SOC 2 report or ISO 27001 certificate, read, not just noted).

SUPPLIER	WHAT IT DOES	HOLDS	WHERE
Microsoft Azure	Hosting, database, storage, Key Vault, monitoring	Restricted	`australiaeast`
Azure AI Foundry	AI model for coding features	Confidential (de-identified clinical text)	Account in `australiaeast`. No Restricted information is sent to it
GitHub	Source hosting, CI	Confidential (source code)	Outside Australia
AI coding tools	Development assistance	Confidential (source code)	Outside Australia

SUPPLIER	WHAT IT DOES	HOLDS	WHERE
Stripe	Subscription billing	Subscriber billing details	Outside Australia
Microsoft 365	HealthOS's own email (sign-up links, invitations, sign-in codes, support), sent app-only with Mail.Send from no-reply@healthos.net.au in HealthOS's own tenancy. Postmark was used before and is decommissioned	Email addresses, message content	Microsoft's data centres for HealthOS's Microsoft 365 tenancy
Telstra	Telephony and SMS	Phone numbers, message content	Australia
Kelly Partners	Accounting	HealthOS's financial records, subscriber billing details	Australia
Penti	Security scanning of the deployed application	What an unauthenticated or test-account scan can see, and the findings	In Penti's platform in the United States (an overseas disclosure; the results describe vulnerabilities, not personal information)

This table is drawn from the repository and is not complete. The full list, with the contract or terms each supplier is used under and the date its assurance report was last read, is kept in SharePoint: HealthOS ISMS > Supplier register. `[Owner to set: the domain registrar and any support tooling still to be added.]`

No supplier is given Restricted information unless it is hosted in Australia or the customer and, where relevant, the government agency concerned has agreed.

The policy set

SUBJECT	DOCUMENT
Risk	Risk Management Framework
Incidents and data breaches	Security Incident and Data Breach Response
People	Personnel Security
Encryption and keys	Encryption and Key Management, key-rotation.md
Audit logging	Audit Logging
Development and change	secure-development.md
Patching and vulnerabilities	patching-and-vulnerability-management.md
Customer notification	end-of-support-and-vulnerability-notification.md

SUBJECT	DOCUMENT
Backup, restore, privileged access	backup-restoration-and-privileged-access.md, infra/BACKUP-AND-RECOVERY.md
Security testing	pentest/README.md
Vulnerability disclosure	`website/.well-known/security.txt` and the trust page

Exceptions

An exception to any policy in this set is requested in writing with its reason, the risk it creates, what compensates for it, and an end date. It is approved by the security owner, or by a director where the security owner is the requester, and entered in the risk register. An exception without an end date is not an exception; it is a change to the policy and is made as one.

Breaches of this policy

A breach is reported like any other incident. A deliberate or repeated breach may lead to removal of access and to action under the person's agreement.

healthOS

Questions about security

Email **security@healthos.net.au**. To report a vulnerability, see https://healthos.net.au/trust/#disclosure.

© 2026 HealthOS Pty Ltd · ABN 81 697 460 889. This is the public edition. The web edition is at https://healthos.net.au/trust/policy-information-security.html.