healthOS

SECURITY POLICY

Risk Management Framework

How risks to information are found, rated, treated or accepted, and how often they are reviewed.

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

Contents

Purpose 2

Roles 2

Risk appetite 2

How a risk is rated 3

Treatment 4

Where risks come from 4

The register 4

Review 5

Purpose

To make sure the risks to the information HealthOS holds are found, written down, rated the same way each time, and either treated or accepted by someone with the authority to accept them. It sits under Information Security Policy.

Roles

ROLE	WHO	DOES
Directors	Aaron Le Saux (sole director)	Set the risk appetite; accept High and Critical risks
Risk owner (security owner)	Aaron Le Saux	Keeps the register, runs the quarterly review, accepts Low and Medium risks
Treatment owner	Named per risk	Carries out the treatment by its date
Everyone	—	Raises a risk when they see one

Risk appetite

The director adopts this statement unchanged, on the date of adoption. It is drafted from how the system is already built.

- **No appetite** for one tenant's information reaching another, for unauthorised disclosure of health information or government-sourced information, or for breaching a government agency's or licensor's terms. A risk of this kind rated Medium or above is treated, not accepted.
- **Low appetite** for loss of integrity or availability of clinical records.
- **Moderate appetite** for risks to delivery speed, cost and convenience, where the information above is not affected.

How a risk is rated

Rate the risk as it stands with current controls (the residual risk).

Likelihood

SCORE	LEVEL	MEANING
1	Rare	Not expected in five years
2	Unlikely	Could happen in the next five years
3	Possible	Could happen in the next year
4	Likely	Expected in the next year
5	Almost certain	Expected within months, or already happening

Impact — take the highest that applies.

SCORE	LEVEL	INFORMATION	SERVICE	LEGAL AND COMMERCIAL
1	Minor	No personal information involved	Under an hour, one customer	None
2	Moderate	Internal or Confidential information, a few records	Hours, one customer	A customer complaint
3	Major	Personal information of a few people, not serious harm	A day, or several customers	A contract breach; a finding by an assessor
4	Severe	An eligible data breach affecting one customer	Days	Notification to the OAIC or an agency; loss of a customer
5	Critical	An eligible data breach across customers, or loss of clinical records	A week or more, or data unrecoverable	Loss of a government connection or licence; the business at risk

Rating = likelihood × impact.

SCORE	RATING	WHO MAY ACCEPT IT	ACTION
1–4	Low	Risk owner	Accept and review yearly
5–9	Medium	Risk owner	Treat within 90 days, or accept with a written reason
10–16	High	A director	Treat within 30 days; a treatment plan within 7

SCORE	RATING	WHO MAY ACCEPT IT	ACTION
20–25	Critical	A director, and only for a stated short period	Treat at once; reported to the directors the same day

Treatment

Each risk gets one of four decisions, recorded with its reason:

- **Reduce** — add or strengthen a control. The usual choice.
- **Avoid** — stop doing the thing that creates the risk.
- **Transfer** — to an insurer or a supplier under contract. This moves cost, not accountability.
- **Accept** — by the person the table above allows, with a reason and a review date. An acceptance without a review date lapses after 12 months.

Where risks come from

A risk is added to the register when any of these produces one:

- a penetration test or scanner finding (pentest/findings-log.md), including each finding dispositioned "risk accepted";
- a threat model for a change that crosses a trust boundary (secure-development.md);
- a security incident or near miss (Security Incident and Data Breach Response);
- a dependency or platform advisory (patching-and-vulnerability-management.md);
- a new supplier, integration, customer type or kind of data;
- a change in law or in an agency's or licensor's terms;
- an exception granted under the information security policy;
- anybody saying so.

The findings log remains the detailed record of test findings. The register holds the risk each one represents, so an accepted finding has an owner and a review date instead of only a line in a log.

The register

Kept in SharePoint: HealthOS ISMS > Risk register. It is Confidential. Each entry has:

FIELD	CONTENT
ID	`R-nnn`
Risk	What could happen, to what, and why
Source	Where it came from, with a link

FIELD	CONTENT
Existing controls	What limits it today
Likelihood, impact, rating	By the tables above
Decision	Reduce, avoid, transfer or accept
Treatment	What will be done
Treatment owner, due date	A person and a date
Accepted by, review date	For an accepted risk
Status	Open, in treatment, accepted, closed

Review

- **Quarterly:** the risk owner reviews every open and accepted entry, closes what is done, re-rates what has changed, and chases overdue treatments.
- **Yearly:** a full assessment — walk the assets and suppliers in the information security policy and ask what is missing from the register — and a report to the directors of the High and Critical risks and the acceptances in force.
- **On the day:** after an incident, a new integration, or a new kind of data.

Each review is recorded with its date and who took part.

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-risk-management.html.