healthOS

SECURITY POLICY

# Personnel Security

Screening before someone starts, confidentiality, training, access while engaged, and what happens when someone leaves.

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

# Contents


Why this one is almost entirely the organisation's 2

Who this covers 2

Before someone starts 2

Confidentiality 3

Where people work from 3

Access while someone is engaged 3

Training 4

When someone leaves 4

Contractors, third parties and source code 4


# Why this one is almost entirely the organisation's

The other policies in this directory describe a system, and much of what they say can be checked in the repository. This one describes how an organisation hires, manages and farewells people, and nothing in a repository can show that. So this document sets the rule and marks, more often than the others, what only the organisation can supply. The NDIA's evidence list for this requirement is four items, and each is named where it is answered.

# Who this covers

Everyone who can reach HealthOS source code, a production system, or customer data: employees, directors, contractors, and the staff of any third party given access. "Access" below means any of those three.

# Before someone starts

Nobody is given access until all of the following are done and recorded.

1. **Identity is verified** against government-issued photo identification.
2. **Right to work in Australia is confirmed.**

3. **A national police check** is obtained, issued within the last 12 months. A disclosable outcome is assessed by the owner against the role; the assessment is recorded.
4. **References or employment history are checked** for the last 5 years.
5. **The agreement is signed.** It carries the confidentiality terms in the next section.

The screening record (what was checked, when, by whom, the outcome, not the documents themselves beyond what the law requires keeping) is held in SharePoint: HealthOS ISMS > Screening register.

*NDIA evidence: "process descriptions detailing pre-employment screening".*

# Confidentiality

Every employment and contractor agreement includes terms under which the person:

- keeps confidential all customer data, personal and health information, source code, credentials and security information, during the engagement and after it ends;
- uses access only for the work it was granted for;
- acknowledges that information obtained from government systems has its own legal protection. For the NDIA APIs this is Protected Agency Information under the NDIS Act, and unauthorised collection, use or disclosure of it is a criminal offence;
- reports a suspected security incident at once (Security Incident and Data Breach Response);
- returns or destroys all organisation information and equipment on leaving.

The standard agreements containing these terms are the HealthOS employment contract and contractor agreement templates, kept in SharePoint: HealthOS ISMS > Agreements.

*NDIA evidence: "internal policy document detailing how employees maintain confidentiality of enterprise information" (this section) and "sample contracts detailing conditions of employment" (the agreements).*

# Where people work from

All development and support of HealthOS is carried out from within Australia. No employee, contractor or support provider works on HealthOS, or reaches its production data, from another country. A proposal to change this is a change to this policy and to the answers given to the NDIA, which must be told before it happens (NDIA API Terms cl. 2.9).

# Access while someone is engaged

- **Named accounts only**, with multi-factor authentication, on GitHub, Azure and the application's administrator roles.
- **Least privilege.** Access is granted for the role, not for convenience, and through the request-and-approve process in backup-restoration-and-privileged-access.md, which also sets the six-monthly revalidation.

- **Role changes** are treated as a leaving and a starting: access the new role does not need is removed on the day.

# Training

- **On starting:** security and privacy induction before access is granted, covering this directory's policies, the Privacy Act obligations, how to report an incident, and phishing.
- **Every year:** a refresher for everyone, recorded with the date.
- **Developers, every year:** secure coding against the OWASP Top 10 and the system's own rules (tenancy, parameterised queries, secrets handling).

The training register is SharePoint: HealthOS ISMS > Training register.

# When someone leaves

On the last day, or at once if the departure is not amicable:

1. Remove the person from the GitHub organisation and revoke their tokens and SSH keys.
2. Remove their Azure role assignments and directory account.
3. Disable their HealthOS application accounts on every stack.
4. Remove them from the security alert recipients, shared mailboxes and any third-party console (Stripe, Microsoft 365 admin, the domain registrar, the assessor and scanner portals).
5. **Rotate every shared secret they could read**, following key-rotation.md. That document already names "when someone with access leaves" as a rotation trigger.
6. Recover equipment, and confirm in writing that no organisation information remains on personal devices.
7. Remind them, in writing, that the confidentiality terms continue.

Each step is ticked and dated on a separation checklist kept with the screening record.

*NDIA evidence: "process descriptions detailing … separation procedures".*

# Contractors, third parties and source code

The NDIA asks for written confirmation that no contractor or non-employee has access to the source code, and applies personnel security provisions to any that do.

**What can be stated from the system:** the source is in a private GitHub repository (`alesaux83/HealthOS`), and the licensed classification material is held in a separate private repository limited to named people.

**What the organisation must state:**

- Whether any person who is not an employee has repository access. The repository's collaborator list is the evidence, reviewed on the cycle in secure-development.md. As at 21 Nov 2026 nobody but Aaron Le Saux

has access: the `healthos` repository has one collaborator (`alesaux83`, admin). The collaborator list is reviewed quarterly.
- Any non-employee who does have access goes through everything in this policy first (screening, agreement, training, separation), has access that is time-limited and recorded with its end date, and is disclosed to the NDIA.

**Services that process source code.** The code is hosted by GitHub, built by GitHub Actions and Azure Container Registry, and worked on with AI coding tools. These are services under contract, not people with access, but they do process the source outside the organisation's own staff. They are listed in the answer to the NDIA questionnaire's question on third parties relied on to develop or support the software, and the written confirmation above should say so plainly instead of leaving it to be discovered. Ask the Digital Partnership Office how it treats them before signing the confirmation.

*NDIA evidence: "written confirmation … that no contractors or non-employees have access to the source code".*

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-personnel-security.html.