OperationsIP

OIP-SEC-001 · Version 1.0 · Effective 1 December 2026

Information Security Policy

This policy sets out how OperationsIP protects the information customers trust us with. It also serves as the technical and organisational measures annex to the Data Processing Agreement (OIP-LEG-003).

DOCUMENT	VERSION	EFFECTIVE	OWNER	NEXT REVIEW
OIP-SEC-001	1.0	1 December 2026	Director	December 2027

Policy · Security

Legal and standards basis

- Privacy Act 1988 (Cth), APP 11
- GDPR Article 32
- ISO/IEC 27001:2022 (target certification)
- SOC 2 Trust Services Criteria (target report)
- ASD Essential Eight
- OWASP Application Security Verification Standard

1. Purpose and scope

It covers the OperationsIP platform, everyone who works on it (including contractors), every system that stores or processes customer data, and our service providers through written agreements.

2. Roles

Role	Responsibility
Director	Owns this policy, approves risks and changes

Role	Responsibility
Security lead	Runs the controls, reviews logs and leads incident response
Everyone	Follows Staff Security and Acceptable Use (OperationsIP team) (OIP-SEC-009) and reports concerns straight away

3. Key controls

Control	How we do it
Data separation	Every row of data belongs to one business. Database row-level security stops any business seeing another's data, even if the app has a fault
Access	Least privilege by role. Owner, Admin and Staff roles in each business. OperationsIP staff use two-factor sign-in
Sign-in	Passwords are hashed by our sign-in provider. One device per login (Owners and Admins: one phone and one computer). See Access Control and Sign-in Policy (OIP-SEC-002)
Encryption	TLS 1.2 or higher in transit. Data encrypted at rest by our database provider
Locked records	Clock-in times come from our servers and can't be edited. Corrections are added with a reason, and the original stays
Secrets	Payment and integration keys are stored on the server only, never in the app
Logging	Important actions, including support sessions and billing changes, are written to an audit log that can't be edited from the app
Backups	Daily backups and point-in-time recovery. See Backup, Business Continuity and Disaster Recovery Plan (OIP-SEC-007)
Change control	Code changes are reviewed and tested before release. See Secure Development and Change Management (OIP-SEC-006)
Suppliers	Providers are assessed before use and reviewed yearly. See Supplier and Third-Party Risk Policy (OIP-SEC-008)

4. Risk management

We keep a risk register, review it every quarter and after any incident, and treat risks by priority. New features get a privacy and security review before release.

5. Testing and assurance

- Automated security checks on the database after each change
- An independent penetration test before launch and every year after
- Working towards ISO 27001 certification and a SOC 2 report as the business grows

6. Breaches of this policy

Breaches are investigated and may lead to removal of access and disciplinary action. Security incidents follow Data Breach and Security Incident Response Plan (OIP-SEC-004).

Related documents

- Staff Security and Acceptable Use (OperationsIP team) (OIP-SEC-009)
- Access Control and Sign-in Policy (OIP-SEC-002)
- Backup, Business Continuity and Disaster Recovery Plan (OIP-SEC-007)
- Secure Development and Change Management (OIP-SEC-006)
- Supplier and Third-Party Risk Policy (OIP-SEC-008)
- Data Breach and Security Incident Response Plan (OIP-SEC-004)
- Data Processing Agreement (OIP-LEG-003)

OperationsIP by Filo Cleano Services Pty Ltd · operationsip.com · Printed copies are uncontrolled. The current version is always online.