OperationsIP

OIP-SEC-009 · Version 1.0 · Effective 1 December 2026

Staff Security and Acceptable Use (OperationsIP team)

This policy applies to OperationsIP's own directors, staff and contractors.

DOCUMENT	VERSION	EFFECTIVE	OWNER	NEXT REVIEW
OIP-SEC-009	1.0	1 December 2026	Director	December 2027

Policy · Security

Legal and standards basis

- Privacy Act 1988 (Cth)
- ASD Essential Eight guidance
- ISO/IEC 27001:2022 Annex A 6 and 8.1

1. Devices and accounts

- Keep work devices locked, encrypted and updated
- Use two-factor sign-in on every work account
- Use a password manager. Never reuse or share passwords
- Report a lost device straight away so access can be revoked

2. Customer data

- Only access customer data for a real support or security reason
- Never copy customer data to personal devices, email or chat tools
- Use demo businesses for training, testing and sales

3. Scams and incidents

Be wary of unexpected requests for passwords, payments or bank changes. Report anything suspicious to the Security lead under Data Breach and Security Incident Response Plan (OIP-SEC-004).

4. Onboarding and leaving

New team members sign confidentiality and IP agreements and complete security training. Access is removed on their last day.

Related documents

- Data Breach and Security Incident Response Plan (OIP-SEC-004)

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