OperationsIP

OIP-LEG-004 · Version 1.0 · Effective 1 December 2026

Acceptable Use Policy

This policy protects every business on OperationsIP, their staff and the public. It applies to everyone with a login.

DOCUMENT	VERSION	EFFECTIVE	OWNER	NEXT REVIEW
OIP-LEG-004	1.0	1 December 2026	Director	December 2027

Policy · Legal and customer policies

Legal and standards basis

- Criminal Code Act 1995 (Cth), Part 10.7 (computer offences)
- Equivalent computer misuse laws in each country

1. Don’t

- Share your login, sign in as someone else or let someone clock in for you
- Try to fake a clock-in time or location, or get around the location check
- Try to access another business's data, test our security without permission, or overload the service
- Upload malware, illegal content, or content that harasses, threatens or discriminates
- Store information you have no right to hold, or use OperationsIP to track people outside work
- Send spam or messages people didn't agree to (see Messaging and SMS Acceptable Use Policy (OIP-PRD-001))
- Resell or white-label OperationsIP without a written agreement with us

2. Security research

If you find a security problem, tell us under Vulnerability Management and Responsible Disclosure (OIP-SEC-005). We won't take action against good-faith research that follows that policy.

3. What happens if this policy is broken

We may remove content, limit features, suspend a user or suspend the business account. Where we can, we will warn the Owner first and explain what needs to change.

Related documents

- Messaging and SMS Acceptable Use Policy (OIP-PRD-001)
- Vulnerability Management and Responsible Disclosure (OIP-SEC-005)

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