Koala Freight Pty Ltd: Information Security Policy

Document ID	KF-POL-001
Version	1.0
Effective date	5 November 2026
Policy owner	Darvin Patel, Information Security Lead
Approved by	Board (portfolio exercise)
Next review	November 2027
Classification	Internal

Portfolio exercise: Koala Freight Pty Ltd is a fictional company. This policy is educational and is not legal or compliance advice.

1. Purpose

This policy sets out how Koala Freight Pty Ltd ("Koala Freight") protects the confidentiality, integrity and availability of its information and systems, including customer consignment data, the customer portal and the cloud platforms that run it. It defines the responsibilities of everyone who handles company information and supports Koala Freight's obligations under customer contracts, the Privacy Act 1988 (Cth) and the Notifiable Data Breaches scheme.

2. Scope

This policy applies to:

- all employees, contractors, interns and temporary staff;
- third parties, including subcontracted carriers, software vendors and managed service providers, who access Koala Freight systems, data or networks;
- all information Koala Freight creates, receives or stores, in any format;
- all company systems, including the customer portal, dispatch and billing platform, AWS and Azure environments, Microsoft 365, company-managed laptops and mobile devices, and any personal device used to access company email or applications;

whether work is performed in the Sydney office, at a customer or depot site, or remotely.

3. Roles and responsibilities

- **Board:** approves this policy, sets Koala Freight's risk appetite and receives a security and risk report at least quarterly.
- **Chief Executive Officer:** accountable for information security across the business and for providing the resources needed to meet this policy.
- **Information Security Lead (Policy Owner, Darvin Patel):** owns and maintains this policy, reviews it at least annually, maintains the risk register, coordinates incident response and reports security posture to the CEO and Board.
- **Head of Engineering:** ensures the customer portal, cloud platforms and backups are designed, configured and operated in line with this policy.
- **IT and Security Lead:** manages identities, endpoints, patching and access reviews.
- **Managers:** ensure their teams understand and follow this policy, approve access requests for their staff and notify IT promptly when people join, move or leave.

- **All personnel:** comply with this policy, complete security awareness training at induction and annually, and report suspected security issues promptly.

4. Policy statements

4.1 Access control

Access to systems and data is granted on a least-privilege, need-to-know basis and must be approved by the person's manager. Access rights are reviewed at least quarterly for privileged and production accounts and at least every six months for all other accounts. Access is removed promptly when no longer required, and in all cases within one business day of a person leaving Koala Freight. Shared accounts are not permitted unless approved by the Information Security Lead and recorded in the access register.

4.2 Privileged access

Administrative access to cloud consoles, production systems and endpoints is limited to staff who need it for their role. Privileged users use a separate administrator account that is not used for email or web browsing. Privileged access is reviewed every quarter, and the AWS root account and Entra ID global administrator accounts are used only for break-glass purposes.

4.3 Acceptable use

Company systems are provided for legitimate business purposes, with limited personal use permitted where it does not interfere with work or create risk. Users must not misuse systems, install unapproved software, share credentials, or attempt to bypass security controls. Company data must not be stored in personal cloud storage or personal email accounts.

4.4 Authentication

Strong, unique credentials are required for every account. Passwords or passphrases must be at least 14 characters and must not be reused across systems; staff use the company-approved password manager. Multi-factor authentication is required for all remote access, all cloud and SaaS administrator accounts, Microsoft 365 and the customer portal's internal administration functions, and is used wherever else it is supported. Phishing-resistant methods are preferred for privileged accounts.

4.5 Data classification and handling

Information is classified as Public, Internal, Confidential or Restricted and handled according to its classification:

- **Public:** approved for release, such as marketing material.
- **Internal:** day-to-day business information not intended for outside parties.
- **Confidential:** customer contracts, pricing, consignment records and personal information about consignees, staff and drivers.
- **Restricted:** credentials, encryption keys, security assessments and payroll or banking data.

Confidential and Restricted information must be encrypted in transit and at rest, shared only with people who need it, and never sent to external parties without an approved business reason and, for third parties, a signed agreement covering data protection.

4.6 Remote and hybrid work

Staff may work remotely on company-managed devices that have disk encryption, endpoint protection, automatic screen lock and current security updates. Remote access to internal systems is through the company's single sign-on with multi-factor authentication. Staff must take reasonable care in public places to prevent others viewing their screen, must not leave devices unattended or unlocked, and must report lost or stolen devices to IT immediately so they can be wiped remotely.

4.7 Endpoint and patch management

Company laptops are centrally managed and enrolled in device management before use. Security patches for operating systems and internet-facing applications are applied within two weeks of release, or within 48 hours where a vulnerability is rated critical or an exploit exists. These timeframes meet or exceed the ACSC Essential Eight Maturity Level One requirements. Operating systems and applications no longer supported by their vendor are removed or replaced. Microsoft Office macros from the internet are blocked, and only approved applications may run on company endpoints.

4.8 Cloud and network security

Cloud resources are deployed through approved accounts and subscriptions only. Storage buckets and blobs are private by default, and public access requires written approval from the Head of Engineering. Network security groups and firewall rules must not allow inbound administrative access (such as SSH or RDP) from the internet. Cloud audit logging is enabled in every account and subscription, and configuration is checked against the CIS Benchmarks on a regular schedule.

4.9 Third-party and vendor security

Before a new vendor, SaaS product or subcontracted carrier is given access to Confidential or Restricted data, the business owner must complete a vendor security assessment proportionate to the risk, approved by the Information Security Lead. Contracts with such third parties must include confidentiality, data protection, breach notification within 72 hours of discovery, the right to request security evidence (for example an ISO/IEC 27001 certificate or SOC 2 report), and return or deletion of data at the end of the relationship. Critical vendors are reviewed at least annually, and third-party access is removed when the engagement ends.

4.10 Backup and recovery

Business-critical data, including the customer portal database and dispatch records, is backed up daily. Backups are encrypted, stored separately from production and protected from modification or deletion by normal user and administrator accounts. Restores are tested at least every six months, and the result is recorded.

4.11 Logging and monitoring

Security-relevant events from cloud platforms, identity systems and the customer portal are logged and retained for at least 12 months. Alerts for high-risk events, such as administrator sign-ins from unusual locations or changes to logging settings, are reviewed promptly.

4.12 Data retention and disposal

Information is kept only as long as needed for business, legal and contractual purposes. Unless a longer period is required by law or contract, consignment and proof-of-delivery records are retained for seven years to meet tax and financial record-keeping obligations, security logs for at least 12 months, and personal information about former staff and drivers only as long as required by employment and tax law. When no longer required, information is securely deleted or destroyed, and devices are wiped or physically destroyed using an approved method before disposal or reuse.

4.13 Incident reporting

All suspected security incidents, including phishing, lost devices, suspicious account activity and accidental disclosure of data, must be reported without delay to the IT service desk at security@koalafreight.example or through the #security-incidents channel in Microsoft Teams. The Information Security Lead coordinates the response under the Incident Response Plan, and assesses whether an incident is an eligible data breach that must be notified to the Office of the Australian Information Commissioner and affected individuals, and whether customers must be notified under their contracts.

5. Enforcement

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract, and where relevant, legal action. Exceptions to this policy must be requested in writing, approved by the Information Security Lead, recorded in the risk register with an expiry date and reviewed before they expire.

6. Review

This policy is reviewed at least annually, or after any significant change to the business, its systems, its legal obligations or its risk environment, including after a major security incident.

7. Approval and version history

Version	Date	Author	Approved by	Changes
1.0	5 November 2026	Darvin Patel	Board (portfolio exercise)	First issue