

CUSTOMER & COMMERCIAL

Confidentiality & Non-Disclosure Statement

Statement | SAL-STD-003 | Version 1.0

Document number	SAL-STD-003
Version	1.0
Document owner	Rhiannon Frankas, Director
Approver	Daniel Frankas, Managing Director
Issue date	19 July 2026
Effective date	On management approval
Review date	19 July 2028 or earlier following material change
Status	For approval and website publication

MISCO uses confidential information only for authorised business purposes, limits access to people who need it, and applies reasonable protection throughout receipt, use, storage, transmission, return and disposal.

1. Purpose

State how MISCO protects confidential information received or created in business relationships.

2. Scope

Technical, commercial, customer, supplier, employee, security and business information in oral, visual, physical or electronic form.

3. Policy statement and commitment

MISCO uses confidential information only for authorised business purposes, limits access to people who need it, and applies reasonable protection throughout receipt, use, storage, transmission, return and disposal.

4. Mandatory requirements

- Confidential information includes non-public drawings, specifications, pricing, forecasts, processes, customer lists, security information and personal information.
- Information is not treated as confidential to the extent it is lawfully public, already known without restriction, independently developed or lawfully received from another source.
- Access is limited to personnel and approved providers with a legitimate need and suitable obligations.
- Do not copy, disclose, reverse engineer, publish or use information outside the authorised purpose.
- Apply secure transfer, storage, access, clean-desk and disposal controls proportionate to sensitivity.
- Lawfully compelled disclosure must be limited and, where permitted, notified to the owner in advance.
- Return or securely destroy information when required, subject to legal retention, backups and evidentiary needs.

- A specific signed NDA prevails where it imposes different or stronger obligations.

5. Implementation and operational controls

- Mark and communicate sensitivity where practical.
- Use project or customer access restrictions.
- Include confidentiality duties in employment and supplier arrangements.
- Investigate and contain suspected unauthorised disclosure.

6. Roles and responsibilities

Role	Responsibility
Directors	Approve the document, provide resources, set the expected standard and review material breaches or exceptions.
Managers and supervisors	Apply the requirements in daily work, communicate expectations, retain required records and escalate concerns.
Employees and contractors	Follow the document, complete required training, protect MISCO interests and promptly report suspected breaches.
Suppliers and business partners	Meet applicable contractual, ethical, safety, quality, security and legal requirements when acting for or supplying MISCO.
Customers and website users	Provide accurate information, use technical content within its stated limits and promptly report errors, incidents or product concerns.

7. Reporting, complaints and escalation

Report lost documents, misdirected emails, unauthorised access or suspected disclosure immediately to a Director.

MISCO will assess concerns proportionately, preserve confidentiality as far as lawful and practicable, prevent retaliation, and refer matters to regulators, emergency services, insurers, professional advisers or law enforcement where required.

8. Monitoring and assurance

- The Document Owner will monitor relevant complaints, incidents, nonconformities, legal or standards changes, website accuracy and overdue actions.
- Material findings will be considered through management review, internal review or corrective action as appropriate.
- Public claims and linked downloads will be checked when evidence, certification, licensing, supplier, product, website technology or business practice changes.

9. Records and retention

Approvals, declarations, registers, reports, investigations, training, complaints, correspondence and other records created under this document must be accurate, protected, accessible to authorised personnel and retained under IT-POL-003 and applicable legal, contractual and evidentiary requirements.

10. Related MISCO documents

- IT-POL-001 Information Security Policy

- IT-POL-005 Privacy Policy
- SAL-STD-001 Terms & Conditions of Sale

11. External references

- [Privacy Act 1988 \(Cth\), Australian Privacy Principles and OAIC guidance](#)
- [OAIC Data breach preparation and response guidance](#)
- [Copyright Act 1968 \(Cth\), Trade Marks Act 1995 \(Cth\) and IP Australia guidance](#)

References were verified from primary or authoritative sources on 19 July 2026. Standards are identified but not reproduced; current licensed editions and legal advice should be consulted where exact requirements determine a decision.

12. Approval and review

Role	Name	Approval / signature	Date
Document owner	Rhiannon Frankas		
Approver	Daniel Frankas		

Review due 19 July 2028, or earlier following material legislative, regulatory, standards, certification, system, operational or organisational change.

Revision history

Version	Date	Change
1.0	19 July 2026	Initial controlled issue prepared for management approval and website publication.