

DATA PROTECTION & INFORMATION MANAGEMENT

Information Security Policy

Policy | IT-POL-001 | Version 1.0

Document number	IT-POL-001
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 will use proportionate governance, people, process and technical controls to prevent unauthorised access, loss, alteration, disclosure and interruption.

1. Purpose

Protect MISCO information according to its confidentiality, integrity, availability and legal or contractual sensitivity.

2. Scope

Paper and electronic records, email, MYOB and other business systems, devices, networks, cloud services, drawings, customer and supplier information, backups and third-party access.

3. Policy statement and commitment

MISCO will use proportionate governance, people, process and technical controls to prevent unauthorised access, loss, alteration, disclosure and interruption.

4. Mandatory requirements

- Classify information as public, internal, confidential or restricted where sensitivity warrants, and apply handling controls accordingly.
- Grant access on least-privilege and need-to-know principles; use individual accounts and promptly remove access when roles end or change.
- Use approved systems, secure authentication, supported software, backups and protective controls suitable for the risk.
- Encrypt or otherwise securely transfer sensitive information and verify recipients before sending.
- Protect drawings, customer specifications, pricing, payroll, banking, personal and security-sensitive records from unauthorised access.
- Assess service providers before entrusting information and include confidentiality, security, access and incident obligations in material arrangements.

- Report suspected loss, phishing, malware, misdirected email, unauthorised access or disclosure immediately.

5. Implementation and operational controls

- Maintain access, asset, backup and incident records.
- Review privileged and shared access at planned intervals.
- Provide security awareness and phishing education.
- Test recovery and update controls after incidents, system changes or emerging threats.

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.

7. Reporting, complaints and escalation

Immediately notify a Director of a suspected information-security incident. Do not investigate by altering evidence, contacting an attacker or concealing the incident.

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-002 Cybersecurity Policy
- IT-POL-003 Data Retention & Disposal Policy

- IT-POL-004 Electronic Communications & Email Policy
- IT-POL-005 Privacy Policy

11. External references

- [Privacy Act 1988 \(Cth\), Australian Privacy Principles and OAIC guidance](#)
- [OAIC Data breach preparation and response guidance](#)
- [Australian Signals Directorate, Essential Eight](#)

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.