

DATA PROTECTION & INFORMATION MANAGEMENT

Electronic Communications & Email Policy

Policy | IT-POL-004 | Version 1.0

Document number	IT-POL-004
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

Electronic communications are business records and must be accurate, respectful, secure and used in a manner that protects MISCO and other people.

1. Purpose

Ensure MISCO email, messaging, internet and electronic communications are lawful, secure, professional and appropriately recorded.

2. Scope

Company accounts, devices and systems and any personal system used to conduct MISCO business.

3. Policy statement and commitment

Electronic communications are business records and must be accurate, respectful, secure and used in a manner that protects MISCO and other people.

4. Mandatory requirements

- Use company channels for business wherever practicable and do not share passwords or allow unauthorised account access.
- Verify recipient addresses, attachments, sensitivity and authority before sending; use secure transfer for restricted material.
- Do not send discriminatory, harassing, defamatory, obscene, deceptive or unlawful material.
- Do not click unexpected links, enable macros, open suspicious attachments or comply with urgent payment instructions without verification.
- Marketing messages require consent or another lawful basis, accurate sender identification and a functional unsubscribe mechanism.
- Do not make unauthorised commitments, legal admissions, public statements or product-compliance claims by email or social media.

- Retain communications that evidence approvals, orders, specifications, complaints, decisions or other required business records.
- MISCO may lawfully monitor and access company systems for security, continuity, legal and policy purposes, with reasonable notice and proportionality.

5. Implementation and operational controls

- Use approved signatures and disclaimers.
- Apply spam, malware, access and retention controls.
- Train users in phishing, privacy and professional communication.
- Remove access promptly on separation and preserve required business records.

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 report misdirected messages, suspected compromise, fraudulent instructions or inappropriate communications 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-002 Cybersecurity Policy
- IT-POL-003 Data Retention & Disposal Policy

11. External references

- [Spam Act 2003 \(Cth\) and ACMA guidance](#)
- [Privacy Act 1988 \(Cth\), Australian Privacy Principles and OAIC guidance](#)
- [OAIC Data breach preparation and response 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.