

DATA PROTECTION & INFORMATION MANAGEMENT

Cybersecurity Policy

Policy | IT-POL-002 | Version 1.0

Document number	IT-POL-002
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 applies risk-based cyber controls informed by Australian Government guidance, including the Essential Eight, while scaling implementation to the company's systems and threat exposure.

1. Purpose

Reduce cyber risk to MISCO systems, information, operations and connected parties.

2. Scope

Users, devices, applications, networks, remote access, cloud services, email, backups, websites, suppliers and operational technology connected to MISCO systems.

3. Policy statement and commitment

MISCO applies risk-based cyber controls informed by Australian Government guidance, including the Essential Eight, while scaling implementation to the company's systems and threat exposure.

4. Mandatory requirements

- Use multi-factor authentication for internet-facing, cloud, remote and privileged access wherever supported.
- Patch operating systems, applications, browsers, network devices and firmware according to risk and vendor support.
- Restrict administrative privileges and use separate privileged accounts where practicable.
- Use reputable endpoint protection, email filtering, application controls and secure configuration.
- Maintain protected, tested backups with at least one copy isolated from ordinary user access.
- Permit only authorised devices, software, remote access and storage services.
- Verify payment or bank-detail changes through a known independent channel and treat urgent secrecy requests as fraud indicators.
- Maintain an incident process covering containment, evidence, recovery, notification and lessons learned.

5. Implementation and operational controls

- Keep a current technology and account inventory.
- Provide ongoing awareness on phishing, passwords, invoices and data handling.
- Review supplier cyber dependencies and access.
- Test backups and incident contacts at planned intervals.

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

Disconnect an affected device from the network where safe, preserve it, and immediately contact a Director. Do not pay ransom, delete evidence or communicate with an attacker without authorised specialist advice.

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-004 Electronic Communications & Email Policy
- COR-POL-008 Defence Industry Security Program Commitment

11. External references

- [Australian Signals Directorate, Essential Eight](#)
- [OAIC Data breach preparation and response guidance](#)
- [Australian Government Department of Defence - Defence Industry Security Program](#)

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.