

GOVERNANCE & CERTIFICATION

Defence Industry Security Program (DISP) Commitment

Commitment | COR-POL-008 | Version 1.0

Document number	COR-POL-008
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 supports the objectives of the Defence Industry Security Program and will assess and uplift security controls according to contractual and membership needs. This document does not state that MISCO is a DISP member or authorised to handle classified information; such status will be claimed only when confirmed by Defence.

1. Purpose

State MISCO's commitment to building security governance suitable for Defence supply-chain participation and potential DISP requirements.

2. Scope

Governance, personnel, physical and cyber security for Defence-related opportunities, contracts, information, systems, facilities and supply-chain relationships.

3. Policy statement and commitment

MISCO supports the objectives of the Defence Industry Security Program and will assess and uplift security controls according to contractual and membership needs. This document does not state that MISCO is a DISP member or authorised to handle classified information; such status will be claimed only when confirmed by Defence.

4. Mandatory requirements

- Determine whether DISP membership and the required domain levels are mandated or appropriate before accepting relevant work.
- Protect OFFICIAL, sensitive, export-controlled and security-classified information according to applicable contract and government requirements.

- Assign accountable security roles and screen personnel where required.
- Control physical access, visitors, assets, documents, incidents and changes in circumstance.
- Maintain cyber controls appropriate to the required DISP level, noting current Defence expectations for Essential Eight maturity.
- Flow relevant security requirements to suppliers and contractors.
- Report security incidents and changes through required channels and preserve evidence.

5. Implementation and operational controls

- Conduct a gap assessment before application or controlled work.
- Maintain a security plan, registers and training proportionate to scope.
- Use Defence resources and competent advisers for membership preparation.
- Review public statements to prevent unsupported membership or clearance claims.

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

Defence security enquiries and incidents must be escalated directly to a Director and handled on a need-to-know basis.

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
- COR-POL-007 Import/Export Control & Trade Compliance Policy

11. External references

- [Australian Government Department of Defence - Defence Industry Security Program](#)
- [Australian Signals Directorate, Essential Eight](#)
- [Defence Trade Controls Act 2012 \(Cth\) and Defence Export Controls 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.