

SUPPLY CHAIN & PROCUREMENT

Import/Export Control & Trade Compliance Policy

Policy | COR-POL-007 | Version 1.0

Document number	COR-POL-007
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 comply with Australian customs, sanctions, export-control and defence trade-control requirements. A transaction will not proceed until material classification, destination, end user, end use and required permits are sufficiently understood.

1. Purpose

Prevent prohibited or unauthorised import, export, supply, brokering and dealings involving controlled goods, technology, destinations or parties.

2. Scope

Physical goods, samples, drawings, CAD files, technical data, software, emails, cloud access, demonstrations, services, brokering, transshipment and international payments.

3. Policy statement and commitment

MISCO will comply with Australian customs, sanctions, export-control and defence trade-control requirements. A transaction will not proceed until material classification, destination, end user, end use and required permits are sufficiently understood.

4. Mandatory requirements

- Screen customers, suppliers, intermediaries, destinations and beneficial owners against applicable sanctions and red-flag information.
- Assess whether goods, technology or services may be controlled under the Defence and Strategic Goods List or another regime before export, supply or publication to a foreign person.
- Obtain permits, licences and declarations before the controlled activity, and comply with all conditions and record-keeping obligations.

- Do not split, reroute, misdescribe or undervalue shipments to evade controls, duties, permits or screening.
- Verify end use and end user where risk warrants and stop when information is inconsistent, incomplete or suspicious.
- Protect export-controlled or security-sensitive technical data from unauthorised access, including through cloud and email systems.
- Use competent customs, freight and legal advisers where classification or obligations are uncertain.

5. Implementation and operational controls

- Use a documented trade-compliance review for higher-risk transactions.
- Retain classification, screening, permits, commercial, shipping and end-use evidence.
- Train sales, purchasing, dispatch and personnel handling technical data.
- Monitor sanctions and control changes relevant to markets and products.

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

Stop and escalate suspected matches, diversion, unusual routing, military or dual-use end-use concerns, incomplete end-user information or requests to misstate documents.

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
- COR-POL-008 Defence Industry Security Program Commitment
- PUR-POL-002 Procurement & Responsible Sourcing Policy

11. External references

- [Australian sanctions laws and Australian Sanctions Office guidance](#)
- [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.