infotrust

SECURE YOUR FUTURE.

MODERN SLAVERY STATEMENT

Infotrust Ltd (ACN 089 224 402)

ABOUT THIS STATEMENT

This Modern Slavery Statement (**Statement**) is made by Infotrust Ltd (ABN 73 089 224 402) (ASX: ITS) (**Infotrust** or **Company**) for the financial year 1 July 2024 to 30 June 2025 (**FY25**), in accordance with the *Modern Slavery Act 2018* (Cth). It covers Infotrust and its controlled entities (**Group**).

The Board of Directors (**Board**) is responsible for overseeing modern slavery risk across the Group. The Board has delegated day-to-day implementation to management, but retains ultimate accountability for the Group's approach.

Infotrust is committed to conducting business with integrity, respecting human rights, and avoiding any involvement in modern slavery practices in its operations and supply chains.

This Statement was approved by the Board on 25 December 2025 and will be published on the Company's website.

MESSAGE FROM THE MANAGING DIRECTOR AND CEO

At Infotrust, we are committed to conducting our business with integrity, transparency and respect for human rights, and we take seriously our responsibility to identify and address modern slavery in all its forms. Modern slavery remains a pervasive global issue, and as a provider of secure digital workplace and cyber solutions, we recognise our obligation to manage these risks across complex supply chains.

Throughout FY25, we strengthened our controls by conducting targeted supplier due diligence, expanding fourth-party visibility, embedding our Supplier Code of Conduct and delivering training to relevant teams. We did not identify any instances of modern slavery during the reporting period; however, we remain vigilant and committed to continually maturing our approach as the risk landscape evolves.

This Statement reflects our dedication to ethical leadership, accountability and meaningful action in preventing modern slavery.

Julian Challingsworth
Managing Director and CEO
Infotrust Ltd

1. OUR STRUCTURE, OPERATIONS AND SUPPLY CHAINS

Structure

Infotrust Ltd is an ASX-listed Australian technology and cyber security services provider headquartered in Melbourne. Through wholly owned subsidiaries, the Group operates across three segments:

- Cyber Security;
- Secure Managed Technology; and
- Cloud & Communications.

We support more than 1,000 mid-market and enterprise customers nationally across sectors such as financial services, education, mining, healthcare and government.

Operations

Infotrust's direct workforce is based predominantly in Australia in professional, technical and engineering roles.

We also utilise selected offshore business process outsourcing (**BPO**) partners for customer support, technical services and back-office functions where scale is required. Oversight of labour practices remains a priority in these arrangements.

Supply Chain

Our supply chain is multi-tiered and services-driven, with spend across:

- ICT hardware and equipment;
- Software, cloud and data centre providers;
- Telecommunications carriers;
- Professional services;
- Outsourced business services, including BPO partners; and
- Corporate and facilities services.

While many suppliers are headquartered in low-risk jurisdictions, Information and Communications Technology (**ICT**) hardware manufacturing, logistics and offshore labour present higher inherent modern slavery risks.

2. MODERN SLAVERY RISKS

Low inherent risk in direct operations

Infotrust's modern slavery risks stem primarily from offshore labour arrangements, ICT hardware supply chains and the multi-tier nature of global technology ecosystems. Our Australian operations present low inherent risk, as our workforce is predominantly professional and technical, operating under strong labour protections, mature HR processes and established safety and whistleblowing frameworks.

Higher inherent risks in offshore labour and ICT supply chains

Higher inherent risks arise within offshore business process outsourcing arrangements, where varying labour law enforcement, subcontracting beyond first-tier visibility, shift-based work and broader economic pressures can create vulnerabilities. These arrangements require enhanced due diligence, contractual controls and continued monitoring.

Our technology supply chains also carry elevated risk, particularly in ICT hardware manufacturing and logistics, where complex global production processes and base-skilled labour may be involved. While many major vendors maintain human rights programs, residual risk can persist deeper in multi-tier supply chains.

Risks arising from business growth and acquisitions

Recent acquisitions expanded Infotrust's supplier base and operational footprint, highlighting variations in supplier governance maturity and inherited subcontracting arrangements. These integration-related risks were assessed and incorporated into our Group-wide supplier risk processes to ensure consistent controls across the consolidated business.

Risk assessment methodology

Infotrust applies a structured assessment methodology that considers sector and service type, geographic risk, supplier maturity, spend and criticality, operational reliance and the visibility of subcontractors and fourth parties. This enables us to identify material risks, prioritise supplier engagement and focus controls where the likelihood of harm is greatest.

3. FY25 ACTIONS TAKEN

FY24 Commitments	FY25 Action Taken	Status
Strengthen supplier due diligence and risk assessment	Reviewed key suppliers above spend threshold; assessed suppliers acquired through M&A in FY25; increased visibility of subcontracting and offshore labour arrangements.	**Done.**
Improve supplier engagement through refreshed questionnaires	Reissued questionnaires to existing key suppliers; issued to new material suppliers; undertook follow-ups where gaps identified.	**Done.**
Embed Supplier Code of Conduct across new contracts	Supplier code of conduct reflected with new contractors.	**Done.**
Enhance contractual protections for modern slavery	Ensured contracts include investigation cooperation, subcontracting transparency, corrective action rights	**Done.**

	and termination clauses. New MSA template strengthened protections across new engagements.	
Increase internal awareness through training	Introduced supplier onboarding practices within the Cyber and Managed Technology divisions that include consideration of modern slavery risks.	**Done.**
Improve tools and systems for supply chain oversight	Identified options to enhance supplier and and fourth-party risk oversight.	**Done.**
Improve reporting to the Audit & Risk Committee (ARC)	ARC endorsed a risk management framework, which addresses a range of enterprise risks, including modern slavery.	**Done.**
Strengthen oversight of offshore BPO partners	Enhanced engagement and review of offshore BPO partners' recruitment and employment practices as part of third-party oversight.	**Done.**
Expand visibility into fourth-party risks	Commenced consideration of fourth-party risk visibility across key suppliers, including identification of tools to support future capture and oversight.	**Done.**
Support continuous improvement in supplier maturity	Follow-ups conducted where questionnaire responses indicated gaps and corrective actions monitored.	**Done.**

FY25 Outcome

Infotrust did not identify any confirmed instances of modern slavery within its operations or supply chains during FY25.

4. GRIEVANCE, ESCALATION & REMEDIATION

Infotrust maintains multiple channels for employees, suppliers, contractors and external stakeholders to raise concerns relating to modern slavery or broader human rights risks:

Reporting channels

- Line managers and People & Culture;
- Legal and the General Counsel;
- Procurement and vendor management;
- Whistleblower channels under the Group Whistleblower Policy (such as, anonymous reporting to the Whistleblower Protection Officer and other Eligible Recipients); and
- Customer or partner escalation pathways.

These channels align with best practice and our Group Whistleblower Policy.

Escalation Pathway

All allegations or red flags relating to modern slavery are escalated immediately to:

- the General Counsel; and
- the Chief Financial Officer or executive sponsor,

with significant matters escalated to:

- the Managing Director and CEO, and
- the Audit & Risk Committee Chair.

The Audit & Risk Committee oversees investigations and outcomes, with material issues being reported to the Board.

Investigation and Remediation

Where a concern is raised, the Group will:

1. Assess immediacy of risk to any potentially affected individuals.
2. Conduct a fact-finding process, including document review, supplier interviews and site engagement where appropriate.
3. Seek specialist external expertise (legal, forensic, human rights).
4. Develop and monitor corrective action with the relevant supplier.
5. Support remediation of adverse impacts, including engagement with affected individuals where feasible.
6. Exercise contractual rights (restrictions, suspension, or termination).
7. Consider notifications to regulators, insurers or customers, where required.

This approach applies to internal and external allegations.

5. ASSESSING EFFECTIVENESS

Infotrust measures the effectiveness of its modern slavery actions through quantitative and qualitative indicators, aligned to the Attorney General Department’s requirements and industry benchmarks:

- Proportion of key suppliers undergoing modern slavery assessment.
- Questionnaire response rates and completeness.
- Supplier remediation actions and timeliness of closure.
- Quality of data within our risk management tool across third and fourth parties.
- Number, nature and outcome of grievances or whistleblower reports.
- Training completion rates for procurement and risk-facing teams.
- Improvements in supplier maturity year-on-year.

No substantiated modern slavery concerns were raised through internal reporting channels or supplier reviews in FY25. While this indicates that controls operated as intended during the period, the Group recognises that ongoing monitoring and capability uplift remain essential.

6. FY26 FOCUS AREAS

Focus Area	Planned Actions for FY26
Supply Chain Assurance	• Continue to review supplier screening approaches, with regard to sector and geographic risk factors. • Maintain engagement with BPO partners on recruitment and employment practices. • Progress work to better understand subcontracting and fourth-party arrangements.
Technology and Data	• Explore opportunities to improve the quality and consistency of supplier data. • Consider options to better connect procurement processes with existing risk information.
Modern Slavery and Enterprise Risk	• Keep modern slavery considerations under review as part of broader third-party risk frameworks. • Continue uplifting Audit & Risk Committee and Board reporting.
Supplier Engagement	• Review the Supplier Code of Conduct to reflect current position. • Refine onboarding materials to reinforce human rights obligations.
Internal Awareness	• Extend training coverage across cyber, SOC, managed technology and business development teams. • Strengthen awareness of escalation pathways and remediation responsibilities. • Continue embedding modern slavery considerations into contract negotiation templates.

7. APPROVAL

This Statement was prepared in consultation with all Infotrust controlled entities. Functional leaders across business units provided input into the content, risk assessment and actions referenced in this Statement.

This Statement is made in accordance with the *Modern Slavery Act 2018* (Cth) and constitutes Infotrust Ltd's Modern Slavery Statement for FY25.

Approved by the Board of Infotrust Ltd on 25 December 2025.

Signed for and on behalf of the Board

Julian Challingsworth
Managing Director and CEO
Infotrust Ltd

infotrust

SECURE YOUR FUTURE.

About Infotrust

Infotrust is Australia's leading ASX-listed technology and cyber security services provider and the largest member of the Infotrust Group (ASX:ITS). With over 250 professionals nationwide, including 140+ cyber specialists, Infotrust delivers end-to end cyber security, managed IT, and advisory services for public and private sectors. Its Australian-based Security Operations Centre operates 24/7, ensuring real-time threat detection and rapid response. Infotrust empowers organisations to manage risk, protect digital assets, and strengthen Australia's cyber resilience.

Brisbane

Lvl 14, 120 Edward St,
Brisbane QLD 4000

Melbourne

Lvl 13, 90 Collins St,
Melbourne VIC 3000

Sydney

Lvl 6, 321 Kent St,
Sydney NSW 2000

Parramatta

Lvl 2, 460 Church St,
Parramatta NSW 2150

For any concerns, please email Infotrust at info@infotrust.com.au or visit Infotrust.com.au.