

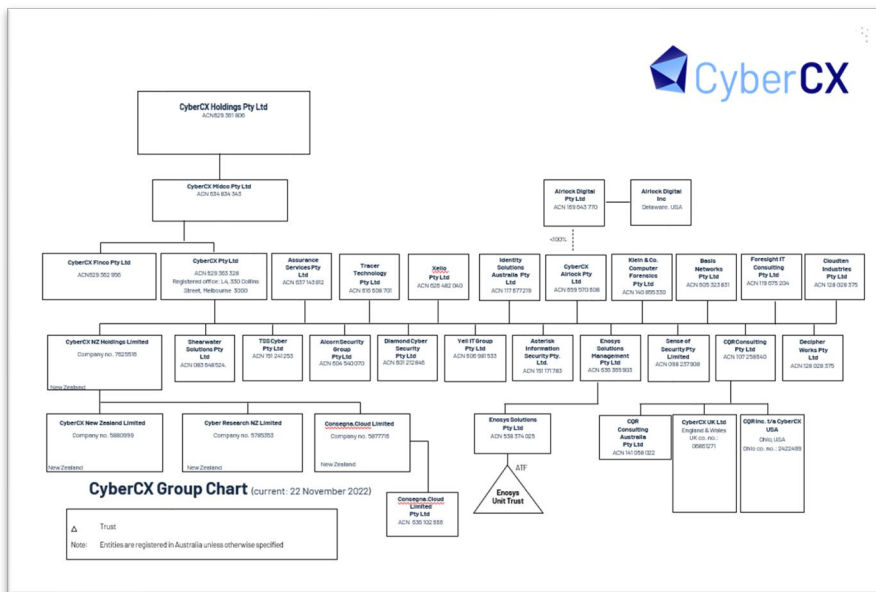
# MODERN SLAVERY STATEMENT

## 1 July 2021 – 30 June 2022

### 1. CONFIRMATION OF REPORTING ENTITY

This Modern Slavery Statement is made by CyberCX Holdings Pty Ltd (**CyberCX**) (ABN 90 629 361 806) for the 2021-22 reporting year in compliance with the Modern Slavery Act 2018 (Cth) (the **Act**).

Headquartered in Melbourne, Australia, the CyberCX group consists of over 20 wholly owned, related bodies corporate across Australia, New Zealand, the United Kingdom and the United States. As none of these related companies is a reporting entity under the Act, this is not a joint statement. CyberCX Pty Ltd is the main trading entity that deals with suppliers and distributors for procurement across the group.



This statement has been prepared covering the financial year ending 30 June 2022 (**FY2022**)

As a good corporate citizen, CyberCX is dedicated to operating in an ethical and legally compliant manner under the Act, and we expect our suppliers to share these values. We are committed to take appropriate steps to minimise the risk of modern slavery occurring in our operations and supply chains.

The purpose of this statement is to outline CyberCX's approach to ensuring our business and supply chains are conducted within a framework that mitigates modern slavery risk. CyberCX is committed to continuous improvement and taking proactive steps to ensure that modern slavery does not occur in our own business and supply chains.

## 2. CYBERCX'S STRUCTURE, OPERATIONS AND SUPPLY CHAINS

### Organisational Structure

CyberCX is Australia's largest, leading independent cyber security services organisation, and is rapidly growing in New Zealand.

Through over 20 acquisitions and a compelling employee proposition, we have unified the most trusted brands in the industry, and the leading cyber security experts from across Australia and New Zealand (and a small number of UK and US staff) who built them.

Our purpose is to help private and public sector organisations of all sizes optimise their cyber security and cyber-risk awareness in an increasingly complex and challenging threat environment. We strive to make the online environment safe and to secure and support the communities in which we live. This purpose is described on our website and embedded in our employee code of conduct and numerous other business policy documents. Consistent with this purpose, we are committed to preventing slavery and human trafficking in our operations and supply chains.



### Operations

CyberCX is principally involved in the delivery of critical, complex cyber security consulting services to government and business customers. We employ more than 1,100 security professionals located across Australia, New Zealand, the United Kingdom, and with employee reach into the United States. We are one team on a single mission, and we are customer obsessed. CyberCX's operations are primarily delivered by our personnel in Australia and New Zealand who are employed directly by our head companies in those countries. It is CyberCX's preference to engage persons as employees rather than contractors where possible.

CyberCX provides cyber security services across 9 key 'practices' in the areas of:

- Strategy & Consulting
- Security Testing & Assurance
- Governance, Risk & Compliance
- Security Integration & Engineering
- Identity & Access Management
- Digital Forensics & Incident Response
- Cyber Capability, Education & Training
- Managed Security Services
- Secure Digital Transformation



### Key supply chains areas

CyberCX's supply chain consists of goods and services that support our cyber security consultancy services across Australia, New Zealand, the United Kingdom and the United States. As a professional services focused organisation, that predominantly undertakes desk-based professional IT-based services for customers, within Australia and New Zealand, CyberCX has a limited supply chain when assessing modern slavery risks. Our greatest expenditure is in remuneration of our team members.

A review of our supply chain in FY2022 has confirmed that it is predominantly focused on expenditure that provides the infrastructure, facilities and other support required to enable the delivery of our services in the following key categories:

- Technology and hardware
- Premises and facilities
- Professional services
- Staff costs (which includes staff merchandise and apparel)
- Limited travel and related expenses
- Hospitality and entertainment.

The majority of goods and services by value that we procure come from suppliers based in Australia.

CyberCX also recognises that some of our supply-chain source goods or services from outside Australia, including some jurisdictions that present a higher risk of modern slavery. These include:

- IT hardware for personal use – including laptops, docking stations and peripherals – and IT infrastructure – primarily servers and routers – which are produced in China and Malaysia.
- CyberCX merchandise that is procured from suppliers which source goods from China.

In FY2022, CyberCX had over 626 suppliers that form part of our operational supply chains. Less than 135 suppliers receive an annual FY2022 expenditure from CyberCX of more than \$100,000.

### 3. OUTLINING THE RISKS OF MODERN SLAVERY PRACTICES IN OUR OPERATIONS AND SUPPLY CHAINS

CyberCX is required to identify the ‘risks of modern slavery practices’ in its supply chain, meaning the potential for CyberCX to cause, contribute to, or be directly linked to modern slavery through our operations and supply chains.

The Modern Slavery Act defines ‘modern slavery’ as including eight types of serious exploitation: trafficking in persons, slavery, servitude, forced marriage, forced labour, debt bondage, the worst forms of child labour and deceptive recruiting for labour or services.

#### Operations

As a primarily high-skilled, professional services organisation operating with over 95% of staff in trans-Tasman locations, CyberCX’s operations are generally considered to be low risk for modern slavery.

CyberCX carries on business in Australia, New Zealand, the United Kingdom and the United States. It has no operations, joint ventures or partnerships in countries reported to have a high prevalence of modern slavery practices by the Global Slavery Index.

Additionally, our 1,100+ employee workforce is subject to the requirements of relevant local labour laws and regulations, including the Australian Fair Work Act 2009 (Cth), the New Zealand Employment Relations Act 2000, the United Kingdom’s National Minimum Wage Act 1998 and Employment Rights Act 1996, and the federal and state laws in the United States, along with the various workplace health and safety regimes in the jurisdictions in which we operate.







As a large Australian organization, CyberCX is compliant with other Commonwealth legislative requirements to enable employees to raise any concerns regarding work conditions, modern slavery or otherwise, via its internal reporting lines, as well as under its Whistle Blowing Policy.

Accordingly, as the key operational functions of CyberCX involve the employment or engagement of staff in our offices in Australia, New Zealand, the United Kingdom and the United States to deliver cyber security services, CyberCX has assessed the risk of modern slavery in its operations as relatively low.



#### Supply Chain

CyberCX’s supply chains consist of goods and services which support our corporate operational departments and client facing services lines. We operate in a sector that is generally considered a low risk for modern slavery; however, we recognise we can be indirectly exposed to modern slavery risks through our supply chains. Excluding remuneration, our major categories of procurement are:

AREA	EXPOSURE TO MODERN SLAVERY RISKS
 <p><b>Technology and hardware</b> <i>Data storage, hardware and software supply, including resale to customers</i></p>	<p>Electronics is recognised as a high-risk industry globally. We procure from leading Tier 1 globally recognised suppliers, and Australian based distributors, who have mature measures to reduce modern slavery risks in their supply chains, including independent auditing and public reporting of key measures and KPIs. Our ongoing review of these providers gives us comfort they are taking adequate steps to identify and manage modern slavery risks.</p>
 <p><b>Premises and Facilities</b> <i>Rental, cleaning, energy and related</i></p>	<p>Cleaning services are recognised as high-risk services globally. CyberCX uses the cleaning services provided by the building management (usually large, superannuation-backed infrastructure managers with mature reporting arrangements) at each of our office sites.</p>
 <p><b>Professional Services</b> <i>Insurance, audit, legal, accounting and taxation services</i></p>	<p>All such services are sourced predominantly from Australia and New Zealand firms, and when engaged our close working relationship allows us sufficient oversight to have no concerns about this low-risk sector.</p>
 <p><b>Staff items</b> <i>Staff apparel and merchandise</i></p>	<p>Textiles is considered a high-risk industry globally. We procure staff apparel and merchandise from a number of local suppliers, some of which is made in China, recognised as a country that may present a higher risk of modern slavery practices. We continue to engage with our distributors and suppliers in this regard, noting challenges encountered by the lasting impacts of COVID-19 lockdowns on supply chains and responses to supply chain engagement</p>
 <p><b>Travel and expenses</b></p>	<p>All travel occurs domestically within Australia, New Zealand and the United Kingdom. Our utilization of such services remains limited due to business shifts to online meetings and engagement during the height of the COVID-19 lockdowns.</p>
 <p><b>Hospitality and entertainment</b></p>	<p>CyberCX recognizes that as a client focused organization, our suppliers include those who provide us with entertainment venues and ancillary services such as catering. CyberCX engages with prominent entertainment venues such as large hotels and sporting venues (many of which are reporting entities for Modern Slavery purposes) and we have ascertained there is low to minimal risk of Modern Slavery for procurement in this sector.</p>

## 4. OUR ACTIONS TAKEN TO ADDRESS MODERN SLAVERY RISKS

### Governance controls and training

In FY2021, CyberCX established its Modern Slavery Policy and internal governance controls for engaging with suppliers (and in particular high risk sector suppliers, such as IT Hardware) which we referred to as our governance framework.

In FY2022, CyberCX has:

- continued to improve our engagement with our suppliers to ensure we have a clear understanding of their businesses and modern slavery risks;
- further refined and developed its Supplier Code of Conduct to address new issues, the evolving expectations of our customers and best practice generally;
- continued to refine our internal online training programs and ensure staff undertake annual mandatory refresher training to all employees (this program covers a broad range of governance, risk and training subjects and is expanding to tailored modules for supply chain risks).
- Actively monitored its internal compliance with applicable laws and workplace awards and standards, and such monitoring has not identified any issues or risks
- Revised aspects of our WHS policies and procedures (in particular with respect to risks posed by communicable diseases such as COVID-19) and continue to monitor these to maintain employee safety.

### **Supplier assessments and contractual mechanisms**

CyberCX has continued work undertaken in the previous reporting period to assess the risks in its supply chain, and work towards mitigation of those risks.

Recognising that our greatest risk of modern slavery is in our supply chains, in FY2022 CyberCX has continued implementing specific modern slavery clauses in supplier contracts when achievable, recognising that many of our largest suppliers by expenditure are global, mature technology providers that are not willing to agree to tailored clauses, but are able to demonstrate other processes which mitigate modern slavery risks.

We have commenced planning and implementation of a risk screening for all existing and future material suppliers in relation to modern slavery compliance. Once the risk level has been determined for a supplier, CyberCX is committed to undertaking remedial actions as required (which may involve moving to a new supplier that has a more satisfactory approach to modern slavery risks).

As part of our ISO27001 certification, we have implemented a system-based risk management process. When onboarding new suppliers we undertake a basic form of due diligence (including questions concerning modern slavery risks and practices) and we continue to develop and formalize this process. We have identified challenges during FY2022 for some of our suppliers due to mergers and acquisitions, or transferal of the products we requisition to new entities. This has prompted CyberCX to further consider steps for managing this type of change.

In FY2022, CyberCX conducted its annual review of its significant spend suppliers. These are suppliers to which CyberCX either routinely purchases goods or services, and/or had a spend of over \$100,000 during the financial year. Of these, CyberCX categorised responses into two types of supplier: (i) those that supply CyberCX for its own consumption (**General Suppliers**) (53% of significant spend suppliers); and (ii) those which supply CyberCX for the purposes of resale or servicing its end customers (**ICT Suppliers**) (47% of significant spend suppliers). Due to the nature of the IT industry, CyberCX considers these ICT Suppliers to be potentially higher risk than our General Suppliers.

No instances of Modern Slavery were identified or suspected of our General Suppliers (in this case, the majority were Australian based enterprises such as airlines, hotels, building managers and leases, and merchandise).

For our ICT Suppliers, we issued questionnaires and follow up inquiries to 43 entities. Of these ICT Suppliers, most provided information that they were unaware of any instances of Modern Slavery in their business. A number did not respond, and a small percentage refused to provide information citing that they were not subject to such legal requirements under the laws of their country and would not participate. For the

entities that refused to respond or did not participate, CyberCX has noted these entities in its risk matrix and will seek to work with these suppliers over the next financial year to improve these information outcomes.

### **Our focus areas for FY2023**

In FY2023, our focus areas for continuous improvement are:

- Continued organisational awareness and engagement on modern slavery requirements, including via face to face and LMS-based training.
- Ongoing refinement and implementation of CyberCX's Supplier Code of Conduct.
- Further development and enhancement of our supplier onboarding processes and questionnaires to assess modern slavery and other risks for new suppliers.
- Continued implementation of appropriate modern slavery contractual requirements as able.
- Continued work to identify "high risk" suppliers in our supply chain (including those that fail to respond to our reasonable inquiries), and an action plan to either work with the supplier to mitigate these risks or change suppliers to a lower-risk provider.

## **5. ASSESSMENT OF THE EFFECTIVENESS OF OUR ACTIONS**

As a result of the work completed in FY2022, CyberCX has improved its information and oversight of its supply chains and activities and risks associated with particular suppliers. While further work is planned to further centralise and administer all supply contracts, our organizational understanding and knowledge of modern slavery risks has improved on FY2021.

We acknowledge there are areas of our oversight which we plan to improve as some suppliers have proven difficult to obtain information from (due to their size, scale, or ongoing disruptions caused by COVID-19 where IT hardware is procured). However, CyberCX is confident that we have made further progress in meeting the goals and aspirations of Australia's legislative framework for Modern Slavery.

## **6. OUR CONSULTATION APPROACH**

Given all the various wholly owned subsidiaries in the CyberCX group are integrally connected to CyberCX, with shared management, governance, risk and other corporate functions, we have conducted an internal consultation process across key stakeholders of our executive leadership team, relevant supply chain managers and our Governance, Risk and Compliance team in producing this statement.

## **7. FURTHER RELEVANT INFORMATION**

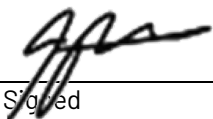
We note the ongoing effects and impact of the COVID-19 pandemic on both CyberCX (as infection rates have waxed and waned in FY2022 across Australian jurisdictions) and our supply chains. We have also been required to devote, often on short notice, considerable time and resources to our people and customers due to the increase demand for cyber security services following the fallout of high-profile data breaches (and this necessity remains ongoing as of the date of this report).

Despite these disruptions which have remained present since FY2021, we continue to make progress regarding our training, our supplier management, and compliance framework.

## 8. APPROVAL

This Modern Slavery Statement was approved by the Board of CyberCX Holdings Pty Ltd on 28 November 2022.

The Board is the principal governing body of CyberCX for the purposes of approving this Statement. This Board has authorised John Paitaridis, Chief Executive Officer, to sign this Statement.



---

Signed

29 November 2022

---

Date

**John Paitaridis**  
**Chief Executive Officer**  
**CyberCX**



Contact us

 [www.cybercx.com.au](http://www.cybercx.com.au)

 **1300 031 274**

### **Australian Headquarters**

Level 4, 330 Collins Street  
**Melbourne, VIC 3000**

### **ACT Head Office**

Level 7, 68 Northbourne Ave,  
Canberra, ACT 2601

### **QLD Head Office**

Level 20, 100 Creek Street  
Brisbane, QLD 4000

### **NZ Head Office**

Level 5, 125 Queen Street  
Wellington, New Zealand 6011

### **NSW Head Office**

Level 23, 2 Market Street  
Sydney, NSW 2000

### **SA Head Office**

Level 11, 95 Grenfell Street  
Adelaide, SA 5000

### **UK Head Office**

Home Park, Grove Road  
Bladon, Oxfordshire OX20 1FX

### **NT Head Office**

19 Smith Street Mall,  
Darwin NT 0800

### **WA Head Office**

Level 13, 28 The Esplanade  
Perth, WA 6000

### **US Head Office**

250 Park Avenue, 7th Floor  
Manhattan, NY 10177