CyberCX Supplier Code of Conduct

Supplying to CyberCX

This Supplier Code of Conduct ('**Code'**) sets out the minimum standards of behaviour that CyberCX expects of suppliers who provide us goods and services. As a leader in cyber security we have a social and legal role to play in ensuring the needs and values of our customers are met with respect to our supply chains.

When supplying goods or services to CyberCX, Supplier must abide by this Code and ensure that it and its personnel, and their supply chains, will meet or exceed these minimum standards. Suppliers must communicate this Code to their related entities, their own suppliers and subcontractors who support them in supplying to CyberCX, so that they are aware of, understand and comply with this Code.

Regardless of whether this Code has been formally agreed to into a contract between CyberCX and a Supplier, this Code will be deemed to apply by virtue of a Supplier's conduct of supplying CyberCX with Goods and/or Services, having been made aware of this Code.

Where a Supplier is not compliant with this Code, CyberCX will seek to work with the Supplier to remedy such noncompliance, and failing this, CyberCX may immediately terminate an agreement or relationship for that Supplier's continued or repeated noncompliance with this Code.

By supplying CyberCX with goods or services, the Supplier agrees and acknowledges this termination right shall apply to such transactions notwithstanding any provision to the contrary.

In this Code:

- "**Supplier**" means any individual or entity (including businesses, employees, consultants, distributors and channel partners) that supplies goods or services to the CyberCX group of companies in Australia, New Zealand, and anywhere else in the world where CyberCX operates; and
- "**Workers**" refers to employees, contractors, agencies, or any other individual who represents or provides goods or services on behalf of the Supplier and of the Supplier's related entities.

Laws & Trade Controls

Suppliers must comply with all applicable:

- laws of the countries in which they operate, and
- laws and regulations relating to sanctions, export, re-export, deemed exports, import and trade controls including but not limited to the laws enacted by Australia, the UN, the US, the EU and the UK.

Human Rights and Workers

CyberCX respects and supports human rights and the UN's Guiding Principles on Business and Human Rights. CyberCX has high ethical and professional standards driven by our desire to provide customers with the best experience.

To allow us to meet these standards, our Suppliers are expected to, and must:

- respect and support the protection of human rights of Workers and their communities, and to monitor their work environments and supply chains for any instances of Modern Slavery (as that term is used in Australia's Modern Slavery Act 2018 (Cth)), and to prevent such instances occurring.
- Notify CyberCX on becoming aware of any instances of Modern Slavery in its workplaces or supply chain;
- Not engage in any form of discrimination (whether or not prohibited by law) as it relates to its hiring or employment practices (including discrimination on the basis of race, gender (or gender identification or sexual orientation), disability, religion, or age);
- Prevent bullying, harassment, or other forms of coercion, threats or violence (whether physical, verbal or psychological) in its business and in its dealings with CyberCX;
- Respect Worker's rights, and any rights to assembly, association or collective bargaining under applicable law;
- Respect and comply with any maximum work hours set by local law for their Workers, and ensure Workers receive appropriate renumeration, leave and other entitlements (including minimum wages and overtime pay) as required by local law;

- Ensure employment contracts with their Workers are clear and easily understood by their Workers, and any temporary or foreign workers must receive their legal entitlements as and when they are due.

Forced Labour

A Supplier must not:

- use any form of forced, bonded or compulsory labour, or engage in any form of slavery or human trafficking.
- require a Worker to surrender any government issued identification document (including passports or work permits) as part of their employment.
- require a Worker to pay any form of recruitment fee for their employment;
- use children or any underaged labour, and must have robust measures to verify the age of its Workers. CyberCX considers the minimum age for a Worker's employment to be 15 years of age or as otherwise permitted by law in which the Supplier provides goods and services to CyberCX.
- use any children under the age of 18 in any hazardous work. Such children must be paid at least the same wage rate as other entry level workers performing similar tasks.

Suppliers must notify CyberCX on identifying any child labour and ensure use such is stopped immediately. Suppliers must also develop a plan to prevent further infringements and respect the development of the child until they are no longer a child.

Health and Safety

Suppliers must comply (and ensure their Workers comply) with relevant work health and safety (**WHS**) laws applicable to their workplaces.

Our Suppliers are expected to maintain minimum health and safety standards including:

- identifying workplace hazards and minimising the risk of injuries (including illness and disease);
- supply appropriate equipment, resources and information for Workers to undertake their duties;
- ensure any goods and services supplied to CyberCX meet safety and other standards and legislative requirements which apply to such goods or services;
- providing appropriate break rooms and or cleaning facilities for Workers, as well as adequate ventilation, heating or cooling, and reasonable personal space;
- monitor the health of workers and workplace conditions, and support workers in raising any health or safety issues or concerns without fear of reprisal; and
- promptly responding to any workplace incidents, injuries or emergencies, and have appropriate systems and training programs in place to deal with such events.

Ethical behavior & Anti Bribery

Our Suppliers must:

- behave in an ethical and honest manner;
- avoid any actual or potential conflicts of interest between it and CyberCX's employees. This includes providing favours or gratuity in exchange for favourable treatment outside of the norms of transparent business hospitality;
- disclose any actual or potential conflicts of interest to CyberCX;
- comply with applicable anti-bribery and anti-corruption laws (including but not limited to the US Foreign Corrupt Practices Act 1977 and the UK Bribery Act of 2010);
- not offer or give any bribes, or 'facilitation payments', secret or inflated commissions, kickbacks or any similar kinds of payments or improper benefits (and this includes any payments to or from any person (including foreign officials or politicians or candidates) irrespective of whether this is a common or accepted practice in an applicable country; and
- not engage or seek to engage in any form of anti-competitive conduct.

Cyber Security and Privacy

As a security services organisation, the goods and services supplied to us must meet our technical and other security requirements. This is important to both our business and that of our customers.

Our Suppliers must ensure:

- where applicable, any goods or services are secure (and any security is up to date in line with best practice) and do not expose CyberCX's or our customers' data and/or systems to any security breaches or unauthorised access;
- any data or information CyberCX shares with a Supplier is kept in confidence and handled in an appropriate manner given the nature of such data or information;
- where required, any specific security or industry standards or requirements are met;
- they immediately notify CyberCX upon becoming aware of any data or network breach of their systems, or any subsisting security issue with their supplied goods or services;
- any Personal Information (as that term is used in Australia's Privacy Act 1988 (Cth)) provided by CyberCX (or its customers) is protected from misuse, unauthorised access, interference, loss, modification or disclosure, and must only be used or disclosed for the purposes for which CyberCX (or its customer) provided it to the supplier. Such Personal Information must be deleted immediately on the earlier of: the end of the last contractual relationship with CyberCX, or once the specific purpose for its use has concluded;
- where they operate across jurisdictions, they comply with the highest standard of protection and management for Personal Information applicable in those jurisdictions;
- they do not do anything which would create a perception that CyberCX is acting inconsistently with its Privacy Policy; and
- where CyberCX communicates to a Supplier that its goods or services are intended to be resupplied to a customer in the Government/Public sector, the Supplier will agree to any security or privacy flow-downs required by that customer.

Code reporting

From time to time and on request by CyberCX, our Suppliers will provide information or answer questionnaires in relation to their compliance with this Code (including with respect to their compliance with Modern Slavery laws, monitoring and management of their supply chains, and security and privacy).

CyberCX expects its Suppliers to fully cooperate with any inquiries it may make, including by promptly responding and providing access to documents or personnel, to verify compliance with this Code.

Notifications

All notifications to CyberCX in connection with this Code are to be sent to:

Attn: Strategic Alliances & Partnerships
Email: vendors@cybercx.com.au
Mail: Level 4, 330 Collins Street, Melbourne VIC 3000

Effective Date & Changes

This Code is effective as of 1 January 2023. For Suppliers with an agreement with CyberCX prior to the above date, this Code is to take effect 30 days after the date on which it is first notified to that Supplier.

This Code may be updated or replaced from time to time by posting a new version on our website. CyberCX will endeavour to notify Suppliers of changes but expects Suppliers to inform themselves of any changes.

Document History Details

Version number	Effective date	Owner	Reviewed by (date)	Approved by (date)	Review date
1	1 January 2023	General Counsel	General Counsel (November 2022)	CyberCX Board (November 2022)	November 2024
1.01	1 May 2025	General Counsel	General Counsel	General Counsel	December 2028