Privacy Notice – Team Members & Applicants

This notice outlines CyberCX's (including its corporate group's) personal information management practices for our **Team Members,** and for **Applicants** who apply to work for us.

This notice provides key information regarding our collection, use and disclosure of Personal Information. It should be read in conjunction with CyberCX's **Global Privacy Policy.** And as applicable, CyberCX's Data Processing Agreement (UK), and Data Transfers Addendum, each located online at **www.cybercx.com.au**.

1 Definitions

Applicant means a person who applies (either themselves or through an agent) to work for CyberCX but have not yet become a Team Member.

CyberCX means the CyberCX group of companies including: CyberCX Pty Ltd (Australia), CyberCX New Zealand Ltd (New Zealand), CyberCX UK Ltd (United Kingdom), and CQR Inc t/a CyberCX USA Inc (USA).

Personal information includes a broad range of information, or an opinion, that could identify an individual. This includes a person's name, home address, email address, telephone number, date of birth, medical records, bank account details and employment details. It may also include a person's employment details, such as work address and contact details, salary, job title and work practices.

Sensitive PI is a sub-set of personal information about an individual's racial or ethnic origin, political opinion, religious beliefs, sexual orientation, criminal record or health information (including biometric data).

Team Member means an employee, intern or registered contractor working for a CyberCX company anywhere in the world.

2 What do we collect and why?

2.1 General Purposes – Applicants

We collect Applicants' details in our job application forms (such as names, contact details, work history, right to work information, and work references). We may also collect this information from your recruiter or other agents acting on your behalf.

During the application process, we may need to conduct background checks about you, and in doing so, collect information about you from third party background check service providers (**Background Providers**). We may initiate these checks through a Background Provider for you to engage with, or we may conduct them independently. We may also collect information about your right to work (e.g. visa entitlement) in a particular country (depending on where the role you are applying for may be offered) so we may assess your legal entitlement to perform the role in that location.

2.2 Specific Purposes – Applicants

For certain roles, we may collect additional information about you to satisfy security related criteria or other inherent requirements to that role (including educational or professional qualifications). We may collect this from you directly or others you nominate, Background Providers, publicly available sources such as social media, or private sources such as educational institutions.

During the recruitment process:

(a) we may ask you to participate in psychometric or similar pre-employment testing or assessments (which may be facilitated via our third party service providers), to assist in our determination of suitability for the relevant role; and
(b) where relevant, you may choose to disclose to us if you have any health conditions that may require reasonable adjustments as part of your application process. In addition to this information you disclose, we may need to collect from you further details and evidence supporting your condition and reasonable adjustments.

We may need to collect information about you from third parties, such as any criminal history, academic misconduct, health information, or your involvement with former employers (for example in the defence sector, or a foreign government due to legislative requirements).

2.3 General Purposes – Team Members

We collect your Personal Information so that we may administer your employment relationship with CyberCX from start to finish. This includes information we need to fulfil our obligations under law such as payment of wages and workplace entitlements, investigate work health and safety matters, as well as so we may provision you with goods or services to enable you to perform your work for us.

This information will be collected directly from you, save where we need to validate details you have provided, including references and prior work experience, in which case we will collect information about you from the most relevant source (such as the referee themselves, or your previous employers).

2.4 Specific Purposes – Team Members

We may collect and validate your Personal Information for annual background checks and, security clearances. For work required to be undertaken in secure areas, we may also collect certain biometric information from you (such as your retinal data or fingerprints) to identify you and authenticate your access to those areas.

If your role requires you to hold or maintain specific qualifications or clearances, we will continue to collect and re-validate information about you to confirm you meet such requirements throughout your employment (or otherwise while you remain in that role).

In certain situations, we may:

(a) collect sensitive information such as health information from you or third parties for workplace health and safety issues, implementing agreed reasonable adjustments, medical emergencies, sick leave and for public health order compliance. For further information relating to Personal Information collected to manage workplace health and safety please visit CCX Connect;
(b) use your Personal Information as part of a submission to a public or private tender for the purpose of outlining the experience, qualifications and basic details of a person that we intend to perform the work if we are chosen to deliver the work under the tender; and
(c) use your personal details when discussing resource availability and suitability with our customers.

From time to time, you may be invited to participate in psychometric testing activities. This testing is intended to be for self reflection and introspection and the results of such are not used by us for any reason other than to facilitate your use/receipt of this testing and results.

2.5 Change of purpose

If we use your personal information for another purpose (that would not be reasonably expected) we will notify and seek the consent from you. For Sensitive PI we will obtain your consent for any other purpose.

A secondary purpose for Personal Information (excluding Sensitive PI) may include, but are not limited to, fraud prevention, audits, investigations, dispute resolution or insurance purposes, litigation and defence of claims or general company research.

We may also use your personal information (including Sensitive PI) without notifying you or seeking your consent as and when permitted by law.

2.6 When else does CyberCX collect personal information about Team Members?

While you perform work for us, we may indirectly or discreetly collect information about you through monitoring practices. For example, the logging and monitoring of your use of IT systems and networks so that we can identify and respond to any suspicious activity (whether caused by you, or affecting the systems you are interacting with).

We may also use, as permitted by law, CCTV to monitor access to, or areas within, our sites for security purposes. We may collect and aggregate information about you to determine your identity or whether your activities in such spaces are authorised or appropriate.

You can obtain further information about our security approach and use of Personal Information in our IT Systems Security Policy (via CCX Connect).

We may also collect personal information when we monitor appropriate uses of social media platforms which include, but are not limited to:

- social networks, such as Facebook, LinkedIn, Twitter (or “X”) or Slack;
- media sharing networks such as Instagram;
- corporate networks and apps (including Teams, Salesforce or Microsoft’s suite of apps); and
- discussion forums.

Appropriate use is detailed in our Media & Social Media Policy and End User Security Policy (via CCX Connect).

3 Consequences of non-collection

If we are unable to collect any of the Personal Information described above:

(a) **For Applicants** – we may be unable to consider your application any further, you may be deemed to be unsuitable for a role, or otherwise we may simply reject your application without further notice;

(b) **For Team Members** – if we are unable to collect details about you for general purposes, we may be unable to sustain your employment relationship with us, or this may lead to (depending on the circumstances) our inability to uphold our obligations to you (such as payment of your wages or benefits).

If we are unable to collect details about you for specific purposes, your access to systems, facilities or ability to work on some engagements may be curtailed or prohibited. We may also be unable to action any requests you have made that require such information to be

processed (for example, health information to process a work health and safety claim or a reasonable adjustment).

The consequences for us not being able to collect your personal information will vary depending on our purpose for collection. At its most extreme, we may be unable to continue your employment if essential details required by law are not provided and validated.

4 Disclosure of personal information

Personal Information of Team Members and Applicants may be disclosed to third parties for the purposes outlined above, such as validating information they have provided us, or otherwise for the purposes that are directly related to our functions or activities.

Where necessary and appropriate, we may disclose your personal information to:

- government entities such as regulatory authorities
- law enforcement;
- CyberCX's corporate group of companies;
- Authorised service providers, external auditors and/or subcontractors of advisors and or contractors.

CyberCX will not disclose Sensitive PI to third parties unless we have your express written consent to do so.

4.1 Disclosure of personal information Overseas – Applicants

Generally, CyberCX does not disclose or transfer an Applicant's personal information outside the region in which the relevant CyberCX company operates (for example, our Australian company does not transfer personal information outside Australia).

However, CyberCX may do so to:

(a) validate any part of your job application or experience that has taken place overseas, by contacting its agents in those places; or
(b) Inform relevant decision makers of our staff who hold global roles but are situated in a particular region.

We may also disclose your personal information to other members of our group of companies to determine if you have previously worked for, or applied to, those companies.

4.2 Disclosure of personal information Overseas – Team Members

We may disclose our Team Member's personal information to members of CyberCX's corporate group of companies located outside the region in which the relevant CyberCX company operates.

We do this where:

(a) the delivery of a service has a cross-jurisdictional element (such as requiring persons in different time zones, or with different experience);
(b) your information is required to be handled by our head office in Australia (for example: for any legal purposes, such as tax, investigations, work health and safety, or other employment maters);
(c) your management line is located in a different region (for example: you report to a global executive director situated in a different country to where you are located);
(d) you wish to (and where permitted by our policies) transfer your employment, or simply your place of work, to a different geographic region.

From time to time, our customers may also require our services to be provided to their entities located in different geographical regions. In such a case we may need to disclose your personal information to the customer's relevant entities, our overseas health or travel insurers, our local travel agents and other third parties working on our behalf. The details of these geographical regions will be provided or made apparent to you on or prior to the commencement of the relevant service delivery.

Sensitive PI will not leave the CyberCX region you are employed within unless you expressly agree in writing it may do so.

5 Securing personal information

We secure personal information as described in our Privacy Policy.

Team Members can obtain further information about our security approach (which includes the security of their Personal Information) by reading our:

(a) IT Systems Security Policy
(b) Information Classification & Asset Management Policy,

each available to Team Members via CCX Connect.

6 Quality of personal information

In the event an Applicant's personal information changes, we ask that they provide such updates to their relevant contact point (such as a nominated person at CyberCX, or your recruitment agent) as soon as possible.

For Team Members, you may update your details via CyberCX's HR portal.

7 Contact and complaints

Team Members and Applicants can contact the persons noted in the CyberCX privacy policy (see above) to raise any concerns in relation to their Personal Information.

8 Index of laws

In this notice we have referred to various laws which permit our collection, use and disclosure of personal information in certain circumstances. Not all of these laws will apply to every situation (for example, the Privacy Act will apply within Australia, but the GDPR will apply to EU/UK based persons in respect of Personal Information handling). A non-exhaustive list of these laws includes:

(1) Privacy Act 1988 (Cth) (**Privacy Act**);
(2) Work Health and Safety Act 2011 (Cth) and its Australian State equivalents;
(3) Fair Work Act 2009 (Cth);
(4) Workplace Surveillance Act 2005 (NSW) and Surveillance Devices Act 2007 (NSW) and its equivalents in other Australian States, and similar operative legislation in New Zealand, UK and USA;
(5) Tax Laws, including: Income Tax Assessment Act 1936 (Cth)), the Income Tax Assessment Act 1997 (Cth), and the Fringe Benefits Tax Assessment Act 1986 (Cth)
(6) Defence Act 1903 (Cth) (in particular Part IXAA being the Safeguarding Australia's Military Secrets legislation).
(7) Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (**GDPR**)

(8) UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, and once in force, the UK Data Use and Access Act 2025

CyberCX notes that in the event any of this notice is inconsistent or not permitted with or by an applicable law, this notice is to be read down to enable this notice and consent to function to the greatest extent possible.