readytech

TPES Addendum

BACKGROUND:

This TPES Addendum (**Addendum**) is an addendum to the Proposal, Purchase Order or Commercial Details Schedule to which it is attached.

OPERATIVE PROVISIONS:

1 Definitions, Interpretation and Application

1.1. In this Addendum:

(a) any words starting with a capital letter have the meanings given to them in our Terms of Service at https://www.readytech.com.au/assets/ReadyTech-PDFs/ReadyTech-Terms-of-Service.pdf or as otherwise defined in the Agreement or in this Addendum;

(b) **TPES** means Third-Party Employment and Skills System;

(c) **DEWR** means the Department of Employment and Workplace Relations of the Australian Government (whether or not operating under that name, or any successor of that Department from time to time, as the case may be);

(d) **IRAP** means Infosec Registered Assessor Program.

(e) **RFFR** means Right Fit For Risk.

1.2. The rules of interpretation set out in the Agreement apply to this Addendum.

1.3. This Addendum only applies in respect of the following Software (**TPES Software**):

(a) EsherHouse Cortex;

(b) Job Ready;

(c) Ready Apprentice; and

(d) Ready Recruit.

1.4. Each TPES Software is a TPES that is approved by the DEWR. A copy of the DEWR accreditation report for the TPES Software is available on the DEWR website.

2 Security

2.1. We implement physical and technical security safeguards necessary to protect your End User Data from unauthorised access. As part of these safeguards, we will take all reasonable steps to:

(a) maintain and enforce an information security program including safety and physical and technical security policies and procedures with respect to our processing of your End User Data;

(b) provide technical and organisational safeguards against accidental, unlawful or unauthorised access to or use, destruction, loss, alteration, disclosure, transfer or processing of your End User Data consistent with best practice;

(c) procure penetration testing by a reputable security consultant to identify security vulnerabilities with respect to the Software or End User Data;

(d) implement reasonable safeguards to remedy any vulnerabilities reported by the penetration testing consultant;

(e) monitor the Software for security breaches and where we become aware that any such breach occurs, take all reasonable remedial measures to eliminate such threats;

(f) prevent: (A) you from having access to the data of our other customers or such other customer's users of the Services (except as otherwise agreed by us); (B) your End User Data from being commingled with or contaminated by the data of our other customers; and (C) unauthorised access to your End User Data;

(g) ensure that your End User Data is protected in transit and at rest with encryption;

(h) have a security and data breach response plan in place;

(i) immediately notify a designated point of contact specified by you in writing to us of any breach of security or unauthorised access involving

the instance of the Software made available to you or any of your End User Data (including any such breach or access by any of our personnel) in our possession or control that comes to our attention and use diligent efforts to remedy all such breaches in a timely manner;

(j) provide you with access to relevant access logs related to your End User Data and the Services that we supply to you, but only where and to the extent required by you to investigate any unauthorised disclosure, access to or use of your End User Data;

(k) only use reputable third parties to host End User Data for the purposes of the Agreement;

(l) maintain or cause to be maintained disaster avoidance procedures designed to safeguard your End User Data throughout the Term and at all times in connection with the actual or required performance of the Services under the Agreement;

(m) conduct daily backups of your End User Data held by us; and

(n) maintain a business continuity and disaster recovery plan (**Plan**) in respect of the hosting of the Software under the Agreement, implement such Plan in the event of any unplanned interruption of the hosting of the Software and test such Plan on at least an annual basis in accordance with industry best practices.

2.2. We will:

(a) use our best endeavours to maintain our RFFR accreditation with DEWR in respect of the Software during the Term;;

and

(b) where we use the hosting services of a third party cloud services provider during the Term, also use our best endeavours to ensure that each such provider and the hosting services that it provides that are relevant to the Agreement are also subject to an IRAP security assessment by an IRAP assessor at least once in every 24 months during the Term.

3 Changes to Service Provider Arrangements

3.1. We will provide you with at least once month's notice of any change to our hosting provider or any other significant change to our service provider arrangements.

4 Data Portability

4.1. We will use reasonable endeavours to ensure that your End User Data is stored by us in a portable manner that allows for:

(a) backups of the End User Data by us;

(b) service migration (where we undergo a migration of our hosting facility to a new hosting provider selected by us; and

(c) decommissioning of any instance of the Software upon termination of the Agreement,

without loss of your End User Data.

5 Incident Response Plan

5.1. We will develop, implement and maintain an Incident Response Plan to deal with any unauthorised access or administration of the Software or your End User Data.

5.2. We will ensure that the Incident Response Plan is tested at least annually.