

TERMS & CONDITIONS

1. Acceptance of Terms.

1. RiseSmart, Inc. ("RiseSmart") provides its Service (as defined below) to you through its web site located at <http://www.RiseSmart.com> (the "Site"), subject to the terms of this agreement and the Data Privacy and Security Addendum "Addendum"), a copy of which is attached and incorporated into this agreement at Schedule 1. If there is any conflict between this agreement and the Addendum, the Addendum will prevail to the extent of any inconsistency. Together, the agreement and the Addendum comprise the Terms of Service ("TOS"). By accepting this TOS or by accessing or using the Service or Site, you acknowledge that you have read, understood, and agree to be bound by this TOS. If you do not agree with this TOS, you must not accept this TOS and may not use the Service.
2. RiseSmart may change this TOS from time to time without prior notice. The revised terms and conditions will become effective upon receipt of written notice of the revised terms and conditions and if you use the Service after that date, your use will constitute acceptance of the revised terms and conditions. If any change to this TOS is not acceptable to you, your only remedy is to stop accessing and using the Service.

2. Description of Service.

The "Service" includes (a) the Site, (b) RiseSmart's outplacement and career management services, and other related services (including file management and analytics services), and related technologies, and (c) all software (including the Software, as defined below), materials, portals, recommendations, job leads, data, reports, text, images, sounds, video, analytics and other content made available through any of the foregoing (collectively referred to as the "Content"). Any new features added to or augmenting the Service are also subject to this TOS.

3. General Conditions/ Access and Use of the Service.

3.1 Subject to the terms and conditions of this TOS, you may access and use the Service only for lawful purposes. All rights, title and interest in and to the Service and its components will remain with and belong exclusively to RiseSmart. You shall not (a) sublicense, resell, rent, lease, transfer, assign, time share or otherwise commercially exploit or make the Service available to any third party; (b) use the Service in any unlawful manner (including without limitation in violation of any data, privacy or export control laws) or in any manner that interferes with or disrupts the integrity or performance of the Service or its components, (c) modify, adapt or hack the Service to, or otherwise attempt to gain unauthorized access to the Service or its related systems or networks; or (d) use any Content on other web sites or any media (e.g., a networking environment). You shall comply with any codes of conduct, policies or other notices RiseSmart provides you or publishes in connection with the Service, and you shall promptly notify RiseSmart if you learn of a security breach related to the Service. In addition, when using certain services, you will be subject to any additional terms applicable to

such services that may be posted on the Service from time to time, including, without limitation, RiseSmart's Privacy Policy.

3.2 Any software that may be made available by RiseSmart in connection with the Service ("Software") contains proprietary and confidential information that is protected by applicable intellectual property and other laws. Subject to the terms and conditions of this TOS, RiseSmart hereby grants you a personal, non-transferable, non-sublicensable and non-exclusive right and license to use the object code of any Software on a single device solely in connection with the Service, provided that you shall not (and shall not allow any third party to) copy, modify, create a derivative work of, reverse engineer, reverse assemble or otherwise attempt to discover any source code or sell, assign, sublicense or otherwise transfer any right in any Software. You agree not to access the Service by any means other than through the interface that is provided by RiseSmart for use in accessing the Service. Any rights not expressly granted herein are reserved and no license or right to use any trademark of RiseSmart or any third party is granted to you in connection with the Service.

3.3 You are solely responsible for all data, information, feedback, suggestions, text, content and other materials that you upload, post, deliver, provide or otherwise transmit or store (hereafter "transmit(ing)") in connection with or relating to the Service ("Your Content"). You hereby represent and warrant that Your Content transmitted by you with respect to the Service will be accurate, true and complete (including with respect to your resume, biographical data and employment information, if you are using the Service as a job seeker). You are responsible for maintaining the confidentiality of your login, password and account and for all activities that occur under your login or account. RiseSmart reserves the right to access your account in order to respond to your requests for technical support. By transmitting Your Content on or through the Service, You hereby do and shall grant RiseSmart a worldwide, non-exclusive, perpetual, irrevocable, royalty-free, fully paid, sublicensable and transferable license to use, modify, reproduce, distribute, display, publish and perform Your Content in connection with the Service. RiseSmart has the right, but not the obligation, to monitor the Service, Content, or Your Content. RiseSmart does not screen or monitor any of Your Content. You further agree that RiseSmart may remove or disable any Content at any time for any reason (including, but not limited to, upon receipt of claims or allegations from third parties or authorities relating to such Content), or for no reason at all.

3.4 You understand that the operation of the Service, including Your Content, may be unencrypted and involve (a) transmissions over various networks, (b) changes to conform and adapt to technical requirements of connecting networks or devices, (c) transmission to RiseSmart's third party vendors and hosting partners to provide the necessary hardware, software, networking, storage, and related technology required to operate and maintain the Service, and (d) transmission to other third parties in connection with the provision to you of the Service. Accordingly, you acknowledge that you bear sole responsibility for adequate security, protection and backup of Your Content. RiseSmart will have no liability to you for any unauthorized access or use of any of Your Content, or any corruption, deletion, destruction or

loss of any of Your Content.

3.5 If you are a job seeker, you further agree to use your own judgment, caution, and common sense in managing job opportunities and information offered by or obtained through the Service and that you bear the sole risk of any reliance or use of any Content (including any job leads or recommendations) provided through the Service.

3.6 The failure of RiseSmart to exercise or enforce any right or provision of this TOS shall not be a waiver of that right. You acknowledge that this TOS is a contract between you and RiseSmart, even though it is electronic and is not physically signed by you and RiseSmart, and it governs your use of the Service and takes the place of any prior agreements between you and RiseSmart.

3.7 You acknowledge that a company client of RiseSmart may engage RiseSmart to assist its current and/or former employees' search for employment through the Service ("Company Client Engagements"). If you are using the Service pursuant to a Company Client Engagement, RiseSmart may make available to the company client progress reports and other information that identify you and indicate the status of your use of the Service, the scope of your use of the Service, your milestone progress and status in job search, your customer satisfaction or other feedback relating to the Service, in each case individually or in an aggregated manner. Please see RiseSmart's Privacy Policy for more information regarding RiseSmart's collection, use and sharing of information provided by you and company clients in connection with Company Client Engagements.

3.8 If you are using the Service pursuant to a Company Client Engagement, you acknowledge that the Service made available to you will in no event exceed the scope, duration or other limits of the Company Client Engagement pursuant to which you are granted access to the Service.

3.9 You agree that RiseSmart (a) may establish general practices and limits concerning use of the Service, including without limitation the maximum period of time that Content will be retained by the Service and the maximum storage space that will be allotted on your behalf, (b) RiseSmart has no responsibility or liability for the deletion or failure to store any Content maintained by or uploaded to the Service, and (c) may preserve Content and may also disclose Content if required to do so by law or in the good faith belief that such preservation or disclosure is reasonably necessary to: (i) comply with legal process, applicable laws or government requests; (ii) enforce this TOS; (iii) respond to claims that any Content violates the rights of third parties; or (iv) protect the rights, property, or personal safety of RiseSmart, its users and the public.

4. Payment.

To the extent the Service or any portion thereof is made available for any fee (and is not otherwise paid by a company client of RiseSmart), you will be required to select a payment plan and provide RiseSmart information regarding your credit card or other payment

instrument. You represent and warrant to RiseSmart that such information is true and that you are authorized to use the payment instrument. You will promptly update your account information with any changes (for example, a change in your billing address or credit card expiration date) that may occur. You agree to pay RiseSmart the amount that is specified in the payment plan in accordance with the terms of such plan and this TOS. You hereby authorize RiseSmart to bill your payment instrument in advance on a periodic basis in accordance with the terms of the applicable payment plan until you terminate your account, and you further agree to pay any charges so incurred. If you dispute any charges you must let RiseSmart know within sixty (60) days after the date that RiseSmart invoices you. We reserve the right to change RiseSmart's prices. If RiseSmart does, RiseSmart will provide notice of the change on the Site or in email to you, at RiseSmart's option, at least 30 days before the change is to take effect. Your continued use of the Service after the price change becomes effective constitutes your agreement to pay the changed amount.

5. Representations and Warranties.

In connection with your use, you agree NOT to: violate any local, state, and federal rules, regulations and statutes, including, but not limited to, U.S. export laws and regulations, anti-discrimination, or equal opportunity employment laws; infringe any intellectual property and privacy rights, including, but not limited to, patent, copyright, trademark, or trade secrets, of any third party; upload, post, transmit, or store any material that: is unlawful, offensive, defamatory, fraudulent, deceptive, misleading, harmful, threatening, harassing, obscene, or objectionable; breaches any of your contractual or confidentiality obligations; disrupts or interferes with the normal operations of the Site, such as posting or transmitting viruses, continuous posting of repetitive materials, or posting abnormally large load; or are not permitted by RiseSmart, including, but not limited to, any unauthorized advertising materials, unsolicited promotional materials, "junk mail," "spam mail," "chain letters," pyramid schemes, franchises, distributorship, club membership, sales arrangement, or otherwise unacceptable materials; violate other's privacy rights or personal rights by abusing the Materials, including, but not limited to, harassing or "stalking" another person, sending unsolicited e-mails, and collecting other's personal information; breach or attempt to breach any security measures of the Site; use any device, process, or mechanism to monitor, retrieve, search, or access, e.g., spider or robot, the Site or any Material without RiseSmart's prior written consent; access or attempt to access any account or login of any third party listed on the Site; copy, modify, reproduce, delete, distribute, download, store, transmit, sell, re-sell, publish, reverse engineer, or create derivative works of any Materials, except for materials that have been submitted and owned by you; post or submit any inaccurate, false, or incomplete information, such as your resume, biographical data, or employment information; impersonate any person or entity; forge any header information in any electronic posting or mail; or misrepresent yourself, your affiliation with any third party, or your entity.

If You are located in Australia, RiseSmart agrees to provide the Service under these TOS in accordance with the terms and conditions of the Australia Data Privacy and Data Security

Addendum attached at Schedule 1 of these TOS.

6. Termination.

You have the right to terminate your account at any time in accordance with the procedures set forth on the Site or provided to you separately, where applicable. If you are using the Service pursuant to a Company Client Engagement, you acknowledge that your access to such Service will expire upon the expiration or termination of the Company Client Engagement. RiseSmart reserves the right to (i) modify or discontinue, temporarily or permanently, the Service (or any part thereof) and (ii) refuse any and all current and future use of the Service, suspend or terminate your account (any part thereof) or use of the Service and remove and discard any of Your Content in the Service, for any reason, including if RiseSmart believes that you have violated this TOS. RiseSmart shall not be liable to you or any third party for any modification, suspension or discontinuation of the Service. RiseSmart will use good faith efforts to contact you to warn you prior to suspension or termination of your account by RiseSmart. All of Your Content on the Service (if any) may be permanently deleted by RiseSmart upon any termination of your account in its sole discretion. If RiseSmart terminates your account without cause and you have signed up for a fee-bearing service, RiseSmart will refund the pro-rated, unearned portion of any amount that you have prepaid to RiseSmart for such Service. However, all accrued rights to payment and the terms of Section 4-12 shall survive termination of this TOS.

7. DISCLAIMERS.

THE SERVICE, INCLUDING THE SITE, CONTENT (INCLUDING JOB LEADS, RECOMMENDATIONS AND ANALYTICS) AND ALL SERVER AND NETWORK COMPONENTS ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS WITHOUT ANY WARRANTIES OF ANY KIND, AND RISESMART EXPRESSLY DISCLAIMS ANY AND ALL WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. YOU ACKNOWLEDGE THAT RISESMART DOES NOT WARRANT THAT THE SERVICE WILL BE UNINTERRUPTED, TIMELY, SECURE, ERROR-FREE OR VIRUS-FREE AND NO INFORMATION, ADVICE OR SERVICES OBTAINED BY YOU FROM RISESMART OR THROUGH THE SERVICE SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THIS TOS. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, IF YOU ARE A JOB SEEKER, (A) YOU ACKNOWLEDGE AND AGREE THAT JOB LEADS THAT RISESMART MAY POST TO YOUR ACCOUNT ARE RECEIVED FROM THIRD PARTIES WITH NO VETTING WHATSOEVER AND (B) RISESMART DOES NOT WARRANT OR GUARANTEE THAT ANY JOB LEADS WILL BE ACCURATE OR LEGITIMATE, YOU WILL SUCCESSFULLY OBTAIN EMPLOYMENT THROUGH THE USE OF THE SERVICE OR ANY EMPLOYMENT YOU FIND THROUGH THE USE OF THE SERVICE WILL FIT YOUR NEEDS OR BE APPROPRIATE FOR YOU.

Under no circumstances will RiseSmart be liable in any way for any content or materials of any third parties (including users), including, but not limited to, for any errors or omissions in any content, or for any loss or damage of any kind incurred as a result of the use of any such

content. You acknowledge that RiseSmart does not pre-screen content, but that RiseSmart and its designees will have the right (but not the obligation) in their sole discretion to refuse or remove any content that is available via the Service. You agree that you must evaluate, and bear all risks associated with, the use of any content, including any reliance on the accuracy, completeness, or usefulness of such content.

8. LIMITATION OF LIABILITY.

8.1 UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY (WHETHER IN CONTRACT, TORT, OR OTHERWISE) SHALL EITHER PARTY BE LIABLE TO THE OTHER PARTY OR ANY THIRD PARTY FOR (A) ANY INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, CONSEQUENTIAL OR PUNITIVE DAMAGES, INCLUDING LOST PROFITS, LOST SALES OR BUSINESS, LOST DATA OR BUSINESS INTERRUPTION, OR (B) FOR ANY DIRECT DAMAGES, COSTS, LOSSES OR LIABILITIES IN EXCESS OF THE FEES ACTUALLY PAID BY YOU IN THE SIX (6) MONTHS PRECEDING THE EVENT GIVING RISE TO YOUR CLAIM OR, IF NO FEES APPLY, ONE HUNDRED (\$100) U.S. DOLLARS. THE PROVISIONS OF THIS SECTION ALLOCATE THE RISKS UNDER THIS TOS BETWEEN THE PARTIES, AND THE PARTIES HAVE RELIED ON THESE LIMITATIONS IN DETERMINING WHETHER TO ENTER INTO THIS TOS. THIS LIMITATION APPLIES TO ALL CAUSES OF ACTION IN THE AGGREGATE INCLUDING UNDER ANY INDEMNITY UNDER THESE TOS.

NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED HEREIN, THE EXCLUSIONS AND LIMITATIONS OF LIABILITY CONTAINED IN THIS SECTION SHALL NOT APPLY TO: YOUR FAILURE TO PAY FEES DUE AND OWING UNDER THESE TOS; (II) LOSSES ARISING OUT OF OR RELATING TO A PARTY'S FAILURE TO COMPLY WITH ITS INTELLECTUAL PROPERTY AND CONFIDENTIALITY OBLIGATIONS OR DATA PRIVACY LAWS OR BREACH OF REGULATORY OR SECURITY REQUIREMENTS SUCH AS BREACHES GIVING RISE TO REGULATORY FINES (III) PERSONAL INJURY, INCLUDING DEATH, AND DAMAGE TO TANGIBLE PERSONAL PROPERTY CAUSED BY THE NEGLIGENT, WILFUL OR INTENTIONAL ACTS OF A PARTY OR ITS EMPLOYEES, AGENTS OR SUBCONTRACTORS (V) LOSSES SUFFERED BY A PARTY ARISING OUT OF ACTS OR OMISSIONS OF THE OTHER PARTY THAT ARE COMMITTED OR OMITTED BY THE OTHER PARTY VOLUNTARILY NOTWITHSTANDING THAT THE OTHER PARTY KNOWS OR OUGHT TO HAVE KNOWN THAT SUCH ACTS OR OMISSIONS WILL RESULT IN DAMAGES INCLUDING, IN THE CASE OF RISESMART, CESSATION OF THE SERVICES.

9. Indemnification.

You shall defend, indemnify, and hold harmless RiseSmart from and against any claims, actions or demands, including without limitation reasonable legal and accounting fees, arising or resulting from your breach of this TOS, any of Your Content, or your other access, contribution to, use or misuse of the Service. RiseSmart shall provide notice to you of any such claim, suit or demand. RiseSmart reserves the right to assume the exclusive defense and control of any matter which is subject to indemnification under this section. In such case, you agree to cooperate with any reasonable requests assisting RiseSmart's defense of such matter. Notwithstanding the foregoing, you will have no obligation to indemnify, defend or

hold harmless any RiseSmart from or against any claims, actions or demands resulting from any action or inaction of RiseSmart.

10. Assignment.

You may not assign this TOS without the prior written consent of RiseSmart, but RiseSmart may assign or transfer this TOS, in whole or in part, without restriction.

11. Governing Law.

This TOS shall be governed by the laws of the State of California without regard to the principles of conflicts of law. Unless otherwise elected by RiseSmart in a particular instance, you hereby expressly agree to submit to the exclusive personal jurisdiction of the federal and state courts of the State of California for the purpose of resolving any dispute relating to your access to or use of the Service.

12. DMCA

The Digital Millennium Copyright Act of 1998 (the "DMCA") provides recourse for copyright owners who believe that material appearing on the Internet infringes their rights under U.S. copyright law. RiseSmart will promptly process and investigate notices of alleged infringement and will take appropriate actions under the DMCA and other applicable intellectual property laws with respect to any alleged or actual infringement. A notification of claimed copyright infringement should be emailed to RiseSmart's Copyright Agent at ddavenport@risesmart.com (subject line: "DMCA" Takedown Request"). You may also contact us by mail or facsimile at:

Attention: Copyright Agent RiseSmart, Inc.

55 Almaden Boulevard, Suite 800 San Jose, CA 95113

Facsimile: [\(408\) 886-3155](tel:4088863155)

Notice: To be effective, the notification must be in writing and contain the following information:

- an electronic or physical signature of the person authorized to act on behalf of the owner of the copyright or other intellectual property interest;
- a description of the copyrighted work or other intellectual property that you claim has been infringed;
- a description of where the material that you claim is infringing is located on the Site, with enough detail that we may find it on the Site;
- your address, telephone number, and email address;
- a statement by you, made under penalty of perjury, that the above information in your Notice is accurate and that you are the copyright or intellectual property owner or authorized to act on the copyright or intellectual property owner's behalf. a statement by

you that you have a good faith belief that the disputed use is not authorized by the copyright or intellectual property owner, its agent, or the law;

13. Apple-Enabled Software Applications

RiseSmart offers Software applications that are intended to be operated in connection with products made commercially available by Apple Inc. ("Apple"), among other platforms. With respect to Software that is made available for your use in connection with an Apple-branded product (such Software, "Apple-Enabled Software"), in addition to the other terms and conditions set forth in this TOS, the following terms and conditions apply:

- RiseSmart and you acknowledge that this TOS are concluded between RiseSmart and you only, and not with Apple, and that as between RiseSmart and Apple, RiseSmart, not Apple, is solely responsible for the Apple-Enabled Software and the content thereof.
- You may not use the Apple-Enabled Software in any manner that is in violation of or inconsistent with the Usage Rules set forth for Apple-Enabled Software in, or otherwise be in conflict with, the App Store Terms of Service.
- Your license to use the Apple-Enabled Software is limited to a non-transferable license to use the Apple-Enabled Software on an iOS Product that you own or control, as permitted by the Usage Rules set forth in the App Store Terms of Service.
- Apple has no obligation whatsoever to provide any maintenance or support services with respect to the Apple-Enabled Software.
- Apple is not responsible for any product warranties, whether express or implied by law. In the event of any failure of the Apple-Enabled Software to conform to any applicable warranty, you may notify Apple, and Apple will refund the purchase price for the Apple-Enabled Software to you, if any; and, to the maximum extent permitted by applicable law, Apple will have no other warranty obligation whatsoever with respect to the Apple-Enabled Software, or any other claims, losses, liabilities, damages, costs or expenses attributable to any failure to conform to any warranty, which will be RiseSmart's sole responsibility, to the extent it cannot be disclaimed under applicable law.
- RiseSmart and you acknowledge that RiseSmart, not Apple, is responsible for addressing any claims of you or any third party relating to the Apple-Enabled Software or your possession and/or use of that Apple-Enabled Software, including, but not limited to: (i) product liability claims; (ii) any claim that the Apple-Enabled Software fails to conform to any applicable legal or regulatory requirement; and (iii) claims arising under consumer protection or similar legislation
- In the event of any third party claim that the Apple-Enabled Software or the end-user's possession and use of that Apple-Enabled Software infringes that third party's intellectual property rights, as between RiseSmart and Apple, RiseSmart, not Apple, will be solely responsible for the investigation, defense, settlement and discharge of any

such intellectual property infringement claim.

- You represent and warrant that (i) you are not located in a country that is subject to a U.S. Government embargo, or that has been designated by the U.S. Government as a “terrorist supporting” country; and (ii) you are not listed on any U.S. Government list of prohibited or restricted parties.
- If you have any questions, complaints or claims with respect to the Apple-Enabled Software, they should be directed to RiseSmart as follows:

user.support@risesmart.com RiseSmart, Inc.

55 Almaden Boulevard, Suite 800

San Jose, CA 95113

RiseSmart and you acknowledge and agree that Apple, and Apple’s subsidiaries, are third party beneficiaries of this TOS with respect to the Apple-Enabled Software, and that, upon your acceptance of the terms and conditions of this TOS, Apple will have the right (and will be deemed to have accepted the right) to enforce this TOS against you with respect to the Apple-Enabled Software as a third party beneficiary thereof.

SCHEDULE 1

DATA PRIVACY AND SECURITY ADDENDUM

This Addendum by and between Randstad Pty Limited (“Randstad”) and RiseSmart Inc (“the Service Provider”), amends the terms and conditions of service between the parties dated _____ 2016 (the “Agreement”), under which the Service Provider is providing Randstad and/or Randstad Stakeholders with certain services (the “Services”).

The parties agree as follows:

2. Definitions

“END USER” MEANS THE INDIVIDUALS AUTHORISED BY RANDSTAD TO ACCESS AND USE THE SERVICES PROVIDED BY THE SERVICE PROVIDER UNDER THE AGREEMENT.

“PERSONAL DATA” MEANS THE DATA CONCERNING AN IDENTIFIED OR IDENTIFIABLE NATURAL PERSON PROCESSED OR TO BE PROCESSED BY THE SERVICE PROVIDER IN THE CONTEXT OF THIS ADDENDUM/THE AGREEMENT

“SECURELY DESTROY” MEANS TAKING ACTIONS THAT RENDER DATA WRITTEN ON PHYSICAL (E.G., HARDCOPY, MICROFICHE, ETC.) OR ELECTRONIC MEDIA UNRECOVERABLE BY BOTH ORDINARY AND EXTRAORDINARY MEANS. THESE ACTIONS MUST MEET OR EXCEED THOSE SECTIONS OF APPLICABLE

AUSTRALIAN LEGISLATION AND/OR GUIDELINES RELEVANT TO DATA CATEGORISED AS PERSONAL DATA.

“SECURITY BREACH” MEANS A SECURITY-RELEVANT EVENT IN WHICH THE SECURITY OF A SYSTEM OR PROCEDURE USED TO CREATE, OBTAIN, TRANSMIT, MAINTAIN, USE, PROCESS, STORE OR DISPOSE OF DATA IS BREACHED, AND IN WHICH RANDSTAD DATA IS EXPOSED TO UNAUTHORISED DISCLOSURE, ACCESS, ALTERATION, OR USE.

“SERVICES” MEANS ANY GOODS OR SERVICES ACQUIRED BY RANDSTAD FROM THE SERVICE PROVIDER.

“RANDSTAD DATA” MEANS DATA PROVIDED TO THE SERVICE PROVIDER BY RANDSTAD WHICH INCLUDES ALL PERSONALLY IDENTIFIABLE INFORMATION OF ANY RANDSTAD STAKEHOLDER AND OTHER INFORMATION THAT IS NOT INTENTIONALLY MADE GENERALLY AVAILABLE BY RANDSTAD ON PUBLIC WEBSITES OR PUBLICATIONS, INCLUDING BUT NOT LIMITED TO BUSINESS, ADMINISTRATIVE AND FINANCIAL DATA, INTELLECTUAL PROPERTY, AND PERSONAL DATA OF ANY RANDSTAD STAKEHOLDER.

“RANDSTAD STAKEHOLDERS” MEANS THE PERSON OR PERSONS WHOSE PERSONAL DATA WILL BE PROCESSED IN CONNECTION WITH THE PROVISION OF THE SERVICES INCLUDING BUT NOT LIMITED TO RANDSTAD’S CANDIDATES, EMPLOYEES, CONTRACTORS AND CUSTOMERS OR PROSPECTIVE CUSTOMERS.

“Registered User” means an individual who creates a profile on and/or otherwise becomes a registered user of the Service Provider’s platform, system or services.

“Territory” means Australia.

2. Rights and license in and to Randstad Data

2.1 The parties agree that as between them, all rights including all intellectual property rights in and to Randstad Data shall remain the exclusive property of Randstad, and the Service Provider has a limited, nonexclusive license to use these data as provided in the Agreement solely for the purpose of performing its obligations hereunder. This agreement does not give a party any rights, implied or otherwise, to the other’s data, content, or intellectual property, except as expressly stated in the agreement.

2.2 The parties acknowledge and agree that once a Randstad Stakeholder or any other individual becomes a Registered User:

- a) the Registered User is subject to the Service Provider’s standard user terms and conditions and privacy policy as applicable from time to time; and
- b) the Service Provider will be responsible for that individual’s Personal Data in accordance with its own terms and conditions and privacy policy.

3. Intellectual property disclosure/rights

3.1 Unless expressly agreed to the contrary in writing, all goods, products, materials, documents, reports, writings, video images, photographs or papers of any nature including software or computer images prepared by the Service Provider (or its subcontractors) exclusively for Randstad under the Agreement will not be disclosed to any other person or entity without the written permission of Randstad.

3.2 The Service Provider warrants to Randstad that Randstad will own all rights, title and interest in any intellectual property created by Randstad in connection with the Randstad Data as part of the performance of the Agreement and will have full ownership and beneficial use thereof, free and clear of claims of any nature by any third party including, without limitation, copyright or patent infringement claims. The Service Provider agrees to assign and hereby assigns all rights, title, and interest in any and all intellectual property created by Randstad as part of the performance of the Agreement to Randstad, and will execute any future assignments or other documents needed for Randstad to document, register, or otherwise perfect such rights. Nothing in this section is, however, intended to or shall be construed to apply to existing intellectual property created or owned by the Service Provider that Randstad is licensing under the Agreement or that the Service Provider creates or develops independently of its obligations under the Agreement. For avoidance of doubt, Randstad asserts no intellectual property ownership under this clause to any pre-existing intellectual property of the Service Provider, and seeks ownership rights only to the extent the Service Provider is being engaged to develop certain intellectual property exclusively for Randstad as part of its services for Randstad.

4. Data privacy

4.1 The Service Provider will only use or process the Randstad Data for the purpose of fulfilling its duties under the Agreement and in accordance with the specific processing instructions contained in Annex 1 or as otherwise instructed by Randstad in writing and is not entitled to perform operations in relation to the Randstad Data for which no instruction has been given. The Service Provider will in no event process Randstad Data for any purpose other than that determined by Randstad.

4.2 The Service Provider will not share Randstad Data or disclose it to any third party without the prior written consent of Randstad, except as required by the Agreement or as otherwise required by law and in that event pursuant to Clause 9.1 below.

4.3 The Service Provider will provide access to Randstad Data only to its employees and subcontractors who need to access the data to fulfill the Service Provider's obligations under the Agreement. The Service Provider will ensure that employees who perform work under the Agreement have read, understood, and received appropriate instruction as to how to comply with the data protection provisions of this Addendum.

4.4 Randstad Data will not be stored outside the Territory without prior written consent from Randstad. The Service Provider's processing of Personal Data will comply with the local laws and regulations applicable in the Territory. Where applicable local law provides for a lower level of

protection of Personal Data than that described in this Addendum, the requirements of this Addendum shall apply. Randstad acknowledges that the Service Provider uses third party service providers and that for some (eg Email delivery) this may involve Randstad Data being transmitted through networks and servers located outside of the Territory.

5. Data security

5.1 The Service Provider will store and process Randstad Data in accordance with commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorised access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure the Service Provider's own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved.

5.2 Without limiting the foregoing, the Service Provider warrants that in respect of the delivery of the Services under the Agreement, it has implemented the following with respect to its software platform and will guarantee these during the term of the Addendum/Agreement:

- a) an information security management system that uses external service providers who are certified compliant with ISO27001/2:2013; or
- b) all the security measures contained in annex II.

6. Employee background checks and qualifications

6.1 The Service Provider shall ensure that its employees who will have potential access to Randstad Data have passed appropriate, industry standard, background screening and possess the qualifications and training to comply with the terms of the Agreement.

7. Data authenticity and integrity

7.1 The Service Provider will take reasonable measures, including audit trails, to protect Randstad Data stored with the Service Provider against deterioration or degradation of data quality and authenticity but will have no responsibility for any actions of any Randstad employee or end user or any firm as may be appointed by Randstad to migrate any Randstad Data which cause any such deterioration or degradation. Any such selected firm selected by Randstad must be notified to the Service Provider in writing and be acceptable to the Services Provider acting reasonably, and will be responsible during the term of the Agreement, unless otherwise specified elsewhere in this Addendum, for converting and migrating electronic data as often as necessary so that information is not lost due to hardware, software, or media obsolescence or deterioration.

8. Security breach

8.1 Upon becoming aware of a security breach with respect to the Service Provider's system or services which has or would be reasonably likely to have a material adverse effect on Randstad, or of circumstances that are reasonably understood to suggest such a security breach is likely, the Service Provider will timely notify Randstad consistent with applicable local law, fully investigate the incident, and cooperate fully with Randstad's reasonable investigation of and response to the

incident. Except as otherwise required by law, the Service Provider will not provide notice of the incident directly to individuals whose personally identifiable information was involved, regulatory agencies, or other entities, without prior written permission from Randstad.

8.2 If the Service Provider must under the Agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of Randstad Data known as Personal Data then in addition to any other remedies available to Randstad under law or equity the Service Provider will:

- a) reimburse Randstad in full for all reasonable costs incurred by Randstad in investigation and remediation of any security breach caused by the Service Provider with respect to such Personal Data, including but not limited to providing notification to individuals whose Personal Data was compromised and to regulatory agencies or other entities as required by law or contract;
- b) the payment of reasonable legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the security breach.

8.3 If the Service Provider will under the Agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of Randstad Data known as Personal Data, then in addition to any other remedies available to Randstad under law or equity, the Service Provider will reimburse Randstad in full for all costs reasonably incurred by Randstad in investigation and remediation of any security breach caused by the Service Provider.]

9. Response to legal orders, demands or requests for data

9.1 Except as otherwise expressly prohibited by law, the Service Provider will:

- a) promptly notify Randstad of any subpoenas, warrants, or other legal orders, demands or requests received by the Service Provider seeking Randstad Data;
- b) reasonably consult with Randstad regarding its response;
- c) cooperate with Randstad's reasonable requests in connection with efforts by Randstad to intervene and quash or modify the legal order, demand or request; and
- d) upon Randstad's request, provide Randstad with a copy of its response.

9.2 If Randstad receives a subpoena, warrant, or other legal order, demand (including request pursuant to applicable laws) or request seeking Randstad Data maintained by the Service Provider, Randstad will promptly provide a copy to the Service Provider. The Service Provider will promptly supply Randstad with copies of data required for Randstad to respond, and will cooperate with Randstad's reasonable requests in connection with its response.

10. Data transfer upon termination or expiration

10.1 Upon termination or expiration of the Agreement, the Service Provider will ensure that all Randstad Data is securely returned or destroyed as directed by Randstad in its sole discretion. Transfer to Randstad or a third party designated by Randstad shall occur within a reasonable period of time, and without significant interruption in service. the Service Provider shall use

reasonable efforts to facilitate that such transfer/migration adopts a standard format that as is reasonably agreed between the parties and compatible with the relevant systems of Randstad or its transferee, and to the extent technologically feasible, that Randstad will have reasonable access to Randstad Data during the transition. In the event that Randstad requests destruction of its data, the Service Provider agrees to securely destroy all data in its possession and in the possession of any subcontractors or agents to which the Service Provider might have transferred Randstad Data. The Service Provider agrees to provide reasonable documentation of data destruction to Randstad.

10.2 So far as is reasonably practicable, the Service Provider will notify Randstad of impending cessation of its business and any contingency plans, and will use all reasonable endeavours if necessary to provide Randstad with reasonable access to the Service Provider's system to remove and destroy exclusively Randstad-owned assets and data. Where applicable, the Service Provider shall use all reasonable endeavours to implement its exit plan and take all reasonable actions to ensure a smooth transition of service with minimal disruption to Randstad. Where applicable, the Service Provider will work closely with its successor to ensure a successful transition to the system (where reasonably practicable), with minimal downtime and effect on Randstad, and where reasonably practicable all such work to be coordinated and performed in advance of the formal, final transition date.

11. Audits

11.1 The Randstad reserves the right in its sole discretion to perform audits of the Service Provider at reasonable times and on providing reasonable prior notice at Randstad's expense to ensure compliance with the terms of the Agreement. The Service Provider shall reasonably cooperate in the performance of such audits, provided that no such audit will disrupt the business carried on by the Service Provider or any services provided by the Service Provider to any of its customers. This provision 11.1 applies to all agreements under which the Service Provider must create, obtain, transmit, use, maintain, process, or dispose of Randstad Data.

11.2 If the Service Provider must under the Agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of Randstad Data which contains Personal Data or financial or business data which has been identified to the Service Provider prior to the date of this Addendum as having the potential to affect the accuracy of Randstad's financial statements, the Service Provider will at its expense conduct or have conducted no more than once annually:

- a) security audit with reasonable audit objectives deemed sufficient by Randstad, which attests the Service Provider's security policies, procedures and controls;
- b) vulnerability scan of the Service Provider's electronic systems and facilities that are used in any way to deliver electronic services under the Agreement; and
- c) formal penetration test of the Service Provider's electronic systems and facilities that are used in any way to deliver electronic services under the Agreement.

11.3 Additionally, the Service Provider will provide Randstad upon reasonable request the results of the above audits, scans and tests, and where a reasonable request is made by Randstad will modify

its security measures as needed based on those results in order to meet its obligations under the Agreement. Randstad may require, at Randstad's expense, the Service Provider to perform additional reasonable audits and tests, the results of which will be provided promptly to Randstad following payment by Randstad to the Service Provider of the Service Provider's costs or expense in performing any such audit or test.

12. No Surreptitious Code

12.1 The Service Provider warrants that, to the best of its knowledge, the software platform licenced to Randstad by the Service Provider under the Agreement is free of and does not contain any code or mechanism that collects information or asserts control of any system operated or owned by Randstad without Randstad's consent, or which may restrict Randstad's access to or use of Randstad Data as held by Randstad independently outside of that software platform. The Service Provider further warrants that it will not knowingly introduce, via any means, spyware, adware, ransomware, rootkit, keylogger, virus, trojan, worm, or other code or mechanism designed to permit unauthorised access to Randstad Data, or which may restrict Randstad's access to or use of Randstad Data as held by Randstad outside of any software platform or system operated by the Service Provider.

13. Compliance

13.1 Each of the Service Provider and Randstad will comply with all applicable laws and industry standards in performing their obligations under the Agreement. Any of the Service Provider's or Randstad's personnel visiting the other party's facilities will comply with all applicable policies regarding access to, use of, and conduct within such facilities. Each such party will provide copies of such policies to the other party upon request.

13.2 The Service Provider warrants that the Services are fully compliant with relevant laws, regulations, and guidance that may be applicable to the service in the Territory.

14. Survival; Order of Precedence, Governing Law

14.1 This Addendum shall survive the expiration or earlier termination of the Agreement. In the event the provisions of this Agreement conflict with any provision of the Agreement, or the Service Providers' warranties, support contract, or service level agreement, the provisions of this Addendum shall prevail to the extent of the conflict or inconsistency.

14.2 This Addendum is governed by the laws of the State of NSW. Disputes will be submitted to the competent court in in that place.

	Signed for and on behalf of:	Signed for and on behalf of Randstad Pty	
		Limited:	
	Authorised Signatory:	Authorised Signatory:	

	Name:	Name:	
	Title:	Title:	
13		©2016 RiseSmart, Inc.	

Annex 1: Specific Processing Instructions

Annex 2: Security measures

The parties acknowledge and agree that for the purpose of this Annex 2, 'Personal Data' refers to Personal Data of any Randstad Stakeholder provided to the Service Provider by Randstad which Randstad Stakeholder has not yet become a Registered User.

1. Access control to data center premises and facilities (physical)

1.1 Service Provider will maintain commercially reasonable physical security systems at all Service Provider sites which are used to Process Personal Data;

1.2 Physical access control will be implemented for all data centers. Unauthorized access is prohibited by onsite staff, biometric scanning or security camera monitoring at all times (24 hours per day, seven days per week);

1.3 Service Provider will maintain procedures for issuing identification markers or badges to authorized staff and controlling physical access to data centers under its control which process Personal Data;

1.4 Turnstiles will be integrated with access control readers to control physical access at all data center sites at all times by requiring staff to present a photo identity card prior to entering such an Service Provider site;

1.5 Visitors must be pre-approved before coming to such Service Provider sites which are used for to Process Personal Data and will be required to present identification, sign a visitor log, and be escorted at all times while on the sites.

2. Access control to systems (virtual)

2.1 Service Provider will establish and maintain all commercially reasonable safeguards against

accidental or unauthorized access to, destruction of, loss of, or alteration of the Personal Data on its systems which are used to Process Personal Data:

2.1.1 access will be granted to personnel through documented access request procedures. The employees' managers or other responsible individuals must authorize or validate access before it is given;

2.1.2 access controls are enabled at the operating system, database, or application level;

2.1.3 administrative access will be restricted to prevent changes to systems or applications;

2.1.4 users will be assigned a single account and prohibited from sharing accounts.

3. Access control to devices and laptops

3.1 Service Provider will implement and maintain commercially reasonable security measures with respect mobile devices and laptops that are used to Process Personal Data.

4. Access control to Personal Data

4.1 Access will be granted only after Processing an approved "access control form", i.e. LAN Logon ID, application access ID, or other similar identification.

4.2 Unique User IDs and passwords will be issued to the users.

4.3 Users, once authenticated, will be authorized for access levels based on their job functions.

5. Transmission and disclosure control

5.1 Service Provider will implement and maintain measures to prevent that Personal Data can be read, copied, modified or removed without authorization during electronic transmission or transport, and to enable to check and establish to which bodies the transfer of Personal Data by means of data transmission facilities is envisaged.

5.2 Service Provider will maintain reasonable technology and processes designed to minimize access for illegitimate Processing, including technology for the encryption of Personal Data.

6. Input control

6.1 Service Provider will maintain system and database logs for access to all Personal Data under its control;

6.2 All Service Provider systems relevant to the security of Personal Data must be configured to provide event logging to identify a system compromise, unauthorized access, or any other security violation. Logs must be protected from unauthorized access or modification;

6.3 Service Provider will maintain input controls on its systems as relevant to the security of Personal Data.

7. Job control

7.1 Service Provider will implement reasonable procedures to ensure the reliability of its employees and any other person acting under its supervision that may come into contact with, or otherwise have access to and Process, those Personal Data, such as requiring a Certificate of Good Conduct ("VOG") prior to commencement of employment.

7.2 Service Provider will implement reasonable procedures to ensure that its personnel is aware of its responsibilities under the Agreement. Service Provider shall instruct and train all any persons it authorizes to have access to the Personal Data on the Data Protection Legislation as well as on all relevant security standards and shall commit them in written form to comply with the data secrecy, the Data Protection Legislation and other relevant security standards.

7.3 Service Provider will promptly act to revoke access to Personal Data of relevant employees or contractors of Service Provider due to termination, a change in job function, or in observance of user inactivity or extended absence.

7.4 Service Provider shall have in place a data protection policy and a document retention policy, with which its personnel must comply.

8. Incident management

8.1 Service Provider will implement, maintain an incident management procedure that allows Service Provider to inform the Controller within the required time frame of any security breach.

8.2 May a security breach (potentially) affect personal data, Service Provider must notify Randstad as per provision 4 in the Addendum.

8.3 The incident management procedure include periodic evaluation of recurring issues that might indicate a security breach.

9. Availability control

9.1 Service Provider will use all commercially reasonable endeavours to protect Personal Data against accidental destruction or loss by ensuring:

9.1.1 Workstations that are used to Process Personal Data will be protected by commercial anti-virus and malware prevention software receiving regular definition updates;

9.1.2 Upon detection of a virus or malware, Service Provider will take immediate reasonable steps to arrest the spread and damage of the virus or malware and to eradicate the virus or malware.

10. Business continuity management

10.1 Service Provider will implement, maintain a business continuity plan.

10.2 Service Provider will regularly evaluate this plan.

11. Change management

11.1 Service Provider will implement, maintain a change management procedure.

11.2 As part of the change management procedure Service Provider will evaluate the impact on the security and adapt the measures where needed to maintain the agreed security level.