Equifax Australasia Workforce Solutions Pty Ltd

ABN 86 080 799 720

SOW for fit2work® (Australia & New Zealand)

Effective 28th May 2021

1. Introduction

1.1 This statement of work ("**SOW**") applies when we, Equifax Australasia Workforce Solutions Pty Limited ABN 86 080 799 720 ("**Equifax**") supply any fit2work® product services ("**fit2work**") to you, our customer, under our terms of supply for information services accessible electronically at www.equifax.com.au/hrsolutions/pdf/terms-of-supply.pdf ("**Terms of Supply**"). Those Terms of Supply and this SOW govern our provision of the fit2work services to you. Additional terms may also apply to various types of fit2work services we supply; if so, those additional terms are set out in an Onboarding Form, Work Order, Fee Schedule or other collateral document (such as a schedule, exhibit or appendix) executed by you and us for purposes of the relevant information service.

1.2 Where other specific contractual arrangements have been executed and are in place between you and us, this SOW applies only to the extent not inconsistent with those contractual arrangements.

1.3 Where this SOW uses terms defined by the Terms of Supply that it does not separately define in schedule 1 to this SOW, those terms have the same meaning in this SOW unless the context otherwise requires. The terms defined in schedule 1 to this SOW have the same meaning where used in this SOW, unless the context otherwise requires.

1.4 fit2work services are provided in accordance with its Collection Statement accessible at www.equifax.com.au/hrsolutions/pdf/fit2work-collection-statement.pdf.

1.5 Our fit2work services comprise both automated or manual methods of providing income and employment verifications in respect of an Applicant nominated by you and include:

(a) national and worldwide identity verification searches;
(b) Australian police and criminal background checks through AFP and ACIC;
(c) NZ criminal conviction checks through the Ministry of Justice;
(d) other international criminal history and identity checks;
(e) professional history qualification & registration checks;
(f) ANZ licencing checks (including ASIC, APRA and directorship records);
(g) employment history and behavioural reference checks;
(h) at the direction of the Applicant, financial history and credit checks accessed through our Affiliate using its independent consumer and commercial credit reporting services;
(i) medical checks through various health service providers;
(j) interface with HR platform management systems for workforce management across the employment cycle;
(k) various other related workforce data search services; and
(l) consolidated reporting.

1.6 Where you are a Consumer, you may have access to a limited number of our fit2work services (including, for example, searches offered by ACIC, the AFP or the MoJ, or purchasing a fit2work Badge). If you are a Consumer, clauses 2 and 5 (other than clause 5.1(e)) of this SOW apply to you. For the avoidance of doubt, where you are a business that is treated as a Consumer, the balance of the provisions in this SOW also apply to you to the extent not inconsistent with clause 2 of this SOW.

2. Supply of fit2work services – Consumer

2.1 When purchased by a Consumer, the fit2work services come with consumer guarantees that cannot be excluded under the relevant Consumer Law. In such case, subject to the relevant Consumer Law and as contemplated by clause 10 of the Terms of Supply, if a guarantee is not satisfied you may be entitled to a resupply of that service or payment of the cost of having that service supplied again, as well as to cancel the service.

2.2 Nothing in this SOW is intended to exclude, restrict or modify any rights that you may have under the relevant Consumer Law or any other applicable legislation which may not be excluded, restricted or modified by agreement.

2.3 For the purposes of section 5D of the FTA (NZ) and section 43 of the CGA (NZ), to the extent permitted by Law, where you are a business (including as a sole trader):

(a) the fit2work services provided to you under or in connection with this SOW are being provided and acquired in trade;
(b) if either or both the FTA (NZ) or the CGA (NZ) applies to the supply of the fit2work services to you then, in respect of all matters under or in connection with this SOW, the parties are contracting out of the CGA (NZ) and sections 9, 12A and 13 of the FTA (NZ); and
(c) it is fair and reasonable for the parties to be bound by this clause 2.3.

2.4 Where you apply for any fit2work service as an Applicant at the request (or otherwise knowingly for the benefit) of an employer who is also our customer, you acknowledge that:

(a) we act as the agent of that employer as contemplated by clause 2.2 of the Terms of Supply; and
(b) to the extent that we may also otherwise act, or be seen as acting, as your agent for purposes of performing an information service (including obtaining search results or providing a report to that employer), you:
  (i) have full knowledge of our role as agent of the employer;
  (ii) have read and understood the Collection Statement accessible at *www.equifax.com.au/hrsolutions/pdf/fit2work-collection-statement.pdf*;
  (iii) are aware of any material facts which might affect you in any dealings with your personal information by us as agent for the employer (for example, if you are a bank employee, disclosure of potential departure to a current employer, through compliance with the *ABA Conduct Background Check Protocol*);
  (iv) freely consent to our involvement for the employer and any transactions contemplated by this SOW for its benefit; and
  (v) waive any conflict of interest or fiduciary duty otherwise owed to you to the extent inconsistent with that consent.

2.5 Where, as Applicant, you are resident in the EU at the time we process personal information as part of our information services, we act as a data controller or joint data controller and a data importer. In those circumstances, we comply with our GDPR obligations in respect of your personal data as set out in schedule 4 to our Collection Statement. A supplier of data to us for purposes of those services may function as a data processor under the GDPR, in accordance with that supplier's service contract with us.

2.6 Where, as Applicant, you are under 18 years of age, a parent or guardian may complete application for a fit2work service on your behalf and that person will be taken to have certified that the personal information provided by them regarding you is true, correct and not misleading in any material particular. You acknowledge that your participation, whether directly or through the act of a parent or guardian, in applying for a fit2work service is a civil act which is for the benefit of you as a minor participant and is fair and reasonable as at the time you apply for the services.

2.7 (a) Where, as an Applicant, you purchase a fit2work Badge, you purchase a:
  (i) 'Gold fit2work Badge' (including police, entitlement to work (visa) and primary qualifications checks);
  (ii) 'Silver fit2work Badge' (including police and entitlement to work (visa) checks); or
  (iii) 'Bronze fit2work Badge' (including police check only),
  (each a 'fit2work Badge', as defined in Schedule 1 below).
(b) All fit2work Badges include an ACIC police check and the badge will expire 6 months from the date of purchase, unless your subscription is maintained.
(c) If your police check is clear and once all your applicable fit2work Badge check results have been provided to you, you may share your fit2work Badge securely with an employer.
(d) We make no warranty or guarantee that a fit2work Badge will be accepted by an employer or that your fit2work Badge is sufficient to meet an employer's background screening requirements, policies or processes.

3. Supply of fit2work services – B2B

3.1 Consistent with clause 4.8 of the Terms of Supply, you will appoint a representative who is to be responsible for the business relationship with us for our fit2work services and who is to be the single point of contact for us and, as may be relevant, the AFP and ACIC. In the absence of any notice from you specifying an Authorised Officer, the officer executing your Onboarding Form or otherwise deemed as accepting this agreement (or any successor in that position from time to time) will be your Authorised Officer.

3.2 The Authorised Officer is authorised to accept notices on your behalf in respect of fit2work services and is responsible for:
(a) contract management and compliance;
(b) your performance as that relates to our provision of fit2work services; and
(c) supporting us in developing the capability to provide the reports contemplated by this SOW.

3.3 We will undertake the checks that you request and report on those in the fastest time practicable. We are not liable for any delay or failure to provide information arising from, or caused or contributed to by, your acts or omissions or those of any third party; however, we will employ all reasonable endeavors to complete the checks and will notify you in a timely manner if this cannot be done.

3.4 You and your Personnel must provide us with all information, materials, assistance and decisions required to enable us to provide the fit2work services and otherwise perform our obligations under this SOW. In particular, you acknowledge that we cannot action any check request until we receive the necessary informed consent from the Applicant.

3.5 We will make a maximum of three attempts to verify information or obtain missing information in respect of check before closing that verification or search as "unverified". Our fit2work service is then complete upon reporting to you that the verification or search is "unverified".

3.6 If we request you, or the Applicant, to provide further instructions and we do not receive any adequate response to that request, we reserve the right to close any related search; however, we will not close any such search before the date that is 14 days after we make that request for further instructions.

3.7 You acknowledge that we:
(a) obtain all data supplied as part of the fit2work services from third parties and rely on those suppliers of data to take reasonable steps to ensure that the data provided is accurate; and
(b) do not independently verify the data that we obtain and supply and do not provide any guarantee or

warranty as to the accuracy or completeness of any such data provided to you or an Applicant.

4. Your use of our information services

4.1 You must use the fit2work services, and any information provided to you as a part of those services, for the Approved Purpose only and at all times comply with our agreement (including this SOW) and all applicable Laws in all jurisdictions that relate to your access to and use of those services.

4.2 Without limiting clause 4.1 of this SOW, you must:

(a) in dealing with any personal information, comply with all Privacy Legislation by which you are or have agreed to be bound;

(b) restrict access to any personal information to Personnel who need to access that personal information to fulfil your obligations for the Approved Purpose;

(c) not disclose or permit the disclosure of personal information to any third party including, without limitation, a third party outside the jurisdiction in which the information is initially received by you, unless:

(i) expressly required or permitted under this agreement; or

(ii) otherwise with our prior written consent, which may be conditional;

(d) take all reasonable steps to ensure that the personal information is protected against misuse and loss, or unauthorised dealing, including by:

(i) undertaking any staff training as may be required;

(ii) monitoring staff and third-party use of any personal information;

(iii) procuring compliance with clause 3 of this SOW by any third party or Personnel to which you have disclosed or permitted disclosure of any personal information;

(e) take such steps we reasonably require of you to facilitate our compliance with the Privacy Legislation, including cooperating with us to resolve any complaint alleging a breach of any Privacy Legislation in respect of any actual or alleged dealing with personal information by you or any of your Personnel (as contemplated by clause 10.8 of the Terms of Supply);

(f) not do or omit to do any act that would put us in breach of any Privacy Legislation; and

(g) immediately notify us if you become aware of a breach of the Privacy Legislation in connection with this agreement.

4.3 Without limiting clause 3.4 of this SOW, you acknowledge and agree that where, to provide the fit2work services, we need to transfer personal information of an Applicant to a third party, you have (or will obtain within the requisite timeframe) a valid authority of that Applicant to allow us to make that transfer.

4.4 Where you place an order for the provision of nationally coordinated criminal history check information from ACIC in respect of an Applicant as part of our fit2work services, you do so in accordance with the contract set out in schedule 2 to this SOW which governs those services. Notwithstanding any other provision of this SOW, if we are not satisfied as to an Applicant's claimed identity or the legitimacy of the identity documents supplied for purposes of a search application to ACIC, and you cannot otherwise satisfy us as to such matters, we may refuse to lodge that application but still render a fee for the service.

4.5 Where you are placing an order for a fit2work service on behalf of an Authorised Client, you are permitted to use those services and any information provided to you as a part of those services for the sole purpose of providing your recruitment or other employment-related services to your Authorised Client, provided that you do not also use those services for your own benefit, and clause 4.2 of the Terms of Supply and clause 3.1 of this SOW are modified accordingly.

4.6 Where you are placing an order for a fit2work service on behalf of an Authorised Client, you:

(a) warrant that you have authority to act as the agent of the Authorised Client;

(b) will ensure that the Authorised Client complies with this agreement (including clauses 3.1 and 3.2 of this SOW) as if it were a party hereto;

(c) will be responsible for the acts and omissions of your Authorised Client in your own right and as if they were your acts or omissions;

(d) indemnify us in accordance with clause 10.7 of the Terms of Supply in respect of any loss or liability we incur through any acts or omissions of your Authorised Client.

4.7 You undertake that:

(a) you or your Authorised Client (as relevant) will provide the Applicant with a reasonable opportunity to respond to or validate the information contained in any report provided by either the ACIC or the AFP before making any decisions that may adversely affect that Applicant; and

(b) if an Applicant wishes to formally dispute the accuracy of any report provided by either the ACIC or the AFP, you will refer that Applicant to us to enable use of an appropriate 'Disputed Record' form and consideration by that authority, prior to you relying on any of the information contained in that report.

4.8 Where you place an order for the provision of KYC / AML checks, you acknowledge that we are not a reporting entity, nor providing a designated service, as contemplated by an AML/CTF Act, and our services do not relieve you of your obligations under that legislation.

4.9 Where you access our fit2work services through or at the direction of a reseller or other third party, we may pay that third party a commission or provide benefits to it for enabling that use of our information services.

5. Information we collect from and provide to you

5.1 We will:

(a) comply with all applicable Privacy Laws;
(b) only collect, use and disclose personal information required to provide the fit2work services in accordance with the Collection Statement accessible electronically at *www.equifax.com.au/hrsolutions/pdf/fit2work-collection-statement.pdf*, as made available to any Applicant;
(c) be responsible for ensuring that any sub-contractors engaged by us in providing the fit2work services are also compliant with this our obligations under this SOW;
(d) hold data provided by you or an Applicant securely and take all appropriate steps to prevent:
(i) misuse, interference and loss; or
(ii) unauthorised access, modification or disclosure,
of that data, and will advise you:
(iii) if we receive a complaint about the handling of that data;
(iv) the steps taken to resolve any such complaint;
(v) if there is a data breach or incident involving that data; and
(vi) the steps being taken by us to remedy any such breach or incident and to prevent it from re-occurring; and
(e) if you request, permit you undertake annual privacy and security reviews to monitor compliance with this clause 5.1 of the SOW in respect of your data.

5.2 We are not in any way providing advice to you in respect of your obligations under, or your compliance (or otherwise) with, any Law, and we disclaim all responsibility for any use you may choose to make of the fit2work services in assisting you to comply with any Law. For example, if you seek a National Police Check from the AFP, you must be satisfied as to any relevant Commonwealth legislation or other basis supporting that check.

5.3 Without limiting clause 5.1 of this SOW, other than as may be required by Law or for a secondary purpose disclosed to the Applicant (and, if that use involves direct marketing, that Applicant has not 'opted-out'), we hold personal information submitted by an Applicant for a minimum of 3 months but no longer than 15 months after a check is completed. We hold any report generated by us for you for at least 2 years after its provision to you.

5.4 We seek to collect and supply the personal information of an Applicant through upload to our website. Where you or the Applicant choose to provide or receive personal information by e-mail, both you and the Applicant acknowledge that e-mail is not a secure form for transmitting information and that any communications transmitted over it may be intercepted or accessed by unauthorised or unintended parties, may not arrive at the intended destination or may not arrive in the form transmitted. In such circumstances, we take no responsibility for communications transmitted over the internet and give no assurance that such communications will remain confidential or intact. Any such communications shall be at the sole risk of you and the Applicant. Where our information services are accessed or viewed by means or in formats other than as originally intended or provided by us, both you and the Applicant remain responsible for reviewing all pertinent portions of those services, including any relevant disclosures and disclaimers.

5.5 Without limiting clause 3.7 of this SOW or clause 5.2 of the Terms of Supply, you acknowledge that:
(a) the results of a check may be constrained by data fields that are collected by a data provider (such as bankruptcy checks under an Insolvency Register) and an exact match to an Applicant may not be possible, in which case we will report a 'possible match';
(b) if an Applicant refuses permission to contact a specific prior employer or contractor, we may rely on secondary evidence (such as a payslip provided by the Applicant) to complete a check; and
(c) we can provide no assurance as to the legitimacy of any prior employer, educational institution, professional membership body or like entity as identified by an Applicant,
and we do not provide any guarantee or warranty as to the accuracy or completeness of any data returned to you or to third parties.

6. Fees

6.1 Unless otherwise covered by a Fee Schedule, you must pay us the fees for our fit2work services as displayed and accessible electronically at **https://www.equifax.com.au/fit2work/** when you access the relevant service.

6.2 In addition to the fees identified by clause 6.1 of this SOW (and unless otherwise provided by a Fee Schedule), we will:
(a) charge additional fees for searches we conduct outside of Australia and New Zealand: those additional fees will be based on the country and type of verification requested and we will notify you of any such additional fees and seek your consent before proceeding with the relevant search; and
(b) pass through any disbursements levied by third party information providers such as academic institutions, agencies, professional bodies and like entities, but capped at $250 per Applicant search.

6.3 The Fee Schedule may specify a 'Term' as the duration for our information services. Where that period expires, and no further duration is identified, the information services can continue or repeat indefinitely.

6.4 We may charge you a fee when you order one or more fit2work checks on an applicant (excluding medical checks) and the check(s) are cancelled before completed, or if an incomplete ordered check remains open for more than ninety (90) days from the date of order. The fee is reflected in the Fee Schedule or in our communications with you. This fee is not intended to exclude, limit or modify a Consumer's rights described in clauses 2.1 and 2.2 above.

7. Privacy

7.1 Notwithstanding that, in providing our information services to you:
(a) we act as your agent under a limited agency in accordance with the Terms of Supply; and

(b) you may have notified us of a privacy policy or any other privacy statement that you operate under,

the fit2work services are supplied in accordance with our Privacy Statement, accessible electronically at *www.equifax.com.au/hrsolutions/pdf/privacy.pdf*, and this SOW. You warrant that our delivery of the fit2work services is compatible with the privacy policy or any other privacy statement or requirement that you operate under.

8. Onboarding Form

8.1 Where you are a new customer, you establish and accept your contractual arrangements with us by completing an Onboarding Form and submitting that to us. Upon approval of that request we will create an account in your name. You represent and warrant that all information provided to us in that Onboarding Form, including the information identifying and relating to any Authorised Officer you specify from time to time, is true, correct, accurate and not misleading and sufficient to allow us to properly assess both your business eligibility and the appropriateness of that Authorised Officer.

8.2 Notwithstanding clause 8.1 and any absence of a completed Onboarding Form, by ordering and accepting our fit2work services (and in the absence of any other specific contractual arrangements between us) you agree those are delivered on the terms in this SOW and the Terms of Supply.

8.3 You acknowledge that ACIC, other governmental departments or supplier entities may require us to satisfy ourselves:

(a) as to the identity of an Authorised Officer; and

(b) that any Authorised Officer is a 'fit and proper' person, or otherwise appropriate, for purposes of that role,

and agree that we may obtain a nationally coordinated criminal history check information from ACIC in respect of an Authorised Officer (together with any other check or checks we may determine as appropriate, acting reasonably) as part of our fit2work services for you, at such times and from time to time as we may determine prudent to satisfy our obligations to that data supplier.

8.4 Without limiting clause 9 of the Terms of Supply, where your Authorised Officer acts in that capacity for purposes of any nationally coordinated criminal history check sourced through ACIC, you will ensure that they deal with such information only as permitted by the terms of schedule 2 (NPCS Services) to this SOW (including clause 10 of that schedule). You acknowledge that the obligations under this clause 8.4 survive the expiry or termination of our agreement and exist in perpetuity, unless otherwise notified by us or ACIC.

8.5 Further guidance on the obligations of an Authorised Officer in connection with any nationally coordinated criminal history check sourced through ACIC is accessible electronically (after logging in) in our toolbox at fit2work.com.au. To the extent that there may be any inconsistency between that guidance and schedule 2 (NPCS Services) to this SOW, the latter prevails.

9. Document verification – Gateway Service User

9.1 Where you wish to access a Gateway Service enabling you to direct information match requests to and from a document issuer or Official Record Holder, we may facilitate provision of those services through a related body corporate.

9.2 Where a Gateway Service is provided to you, you acknowledge and agree that:

(a) we have no responsibility for your use of that Gateway Service;

(b) you access the Gateway Service under a separate contract with our related body corporate, including through complying with any further terms and conditions of use as may be imposed by the Gateway Service hub; and

(c) you will create or modify your business processes and ICT security in a manner reasonably acceptable to that company to establish and maintain functional connection to the hub.

10. Medical checks

10.1 Our medical check information service fees are based on use of Jobfit, our primary medical service provider, in accordance with clause 10.2 of this SOW. Those fees may change in accordance with clause 7.5 of our Terms of Supply. If we determine to use, or you request that we use, another medical check service provider, additional or different fees may apply. For example, we may determine to use another provider if Jobfit does not have capacity, where the Applicant is in a remote regional location or to meet a specific timeframe. We will notify you through our platform when making a booking with another provider and, where practicable, will advise you of any additional or different fees that may apply.

10.2 You will request any medical assessment for an Applicant as a fit2work service through our platform. When using Jobfit, this will permit the flow of relevant information to populate the Jobfit MediManager system and Jobfit will contact the Applicant to co-ordinate any appointment for the medical assessment. Status updates will be available to you through our fit2work platform.

10.3 Irrespective of the service provider, certain circumstances may require an additional medical assessment appointment to be made or additional costs to be incurred in respect of an Applicant. These circumstances include:

(a) multiple health practitioners are required to complete all requested check assessments;

(b) an Applicant is not able to attend the initial appointment and so needs rebooking;

(c) an Applicant cancels their appointment with less than **one clear working days' notice** through the Jobfit MediManager system (or otherwise to us), fails to attend their appointment at the

scheduled time, or requires extra services to be performed to achieve the assessment sought;

(d) certain aspects of the medical assessment not being able to be conducted at the initial appointment or needing to be undertaken at a different clinic; for example, if an instant drug screen result is non-negative, an additional GCMS test may be required to confirm the result – in which case an additional fee will apply, dependant on the pathology clinic used.

10.4 Where clause 10.3 of this SOW applies, further fees apply for the additional administrative work undertaken, as well as any additional clinic or similar fees incurred. If an Applicant cancels their appointment with less than one clear working days' notice, a cancellation fee equalling 100% of the fee for that medical assessment will apply. Any such additional fees may be rendered by a second invoice, credit or adjustment note from us. We will provide an appropriate explanation of those costs at the time of rendering for such additional fees and costs.

10.5 If a practitioner requires further information (whether from an Applicant's GP or otherwise) to perform the required medical assessment on an Applicant, the Applicant must provide that directly to the doctor. In such circumstances:

(a) we will not receive that further information and, if it is misdirected to us, we will treat it as unsolicited personal information and destroy it as soon as practicable; and

(b) any associated costs in obtaining that information are to be paid by the Applicant – it is then at your discretion as to whether to reimburse the Applicant for those costs.

Where an Applicant does not provided information requested by a practitioner within 2 weeks of the initial appointment, the Applicant's check will be closed as "incomplete" and our fees will apply.

11. Bankruptcy checks

11.1 You acknowledge and agree that prior to requesting for a bankruptcy check, you agree to provide any notification to individuals or obtain any consents that are required under the Privacy Law to request for the bankruptcy check.

11.2 The bankruptcy check will be conducted on the information, being the full primary name and date of birth, that is declared in the fit2work platform provided by the Applicant. Accordingly, you acknowledge and agree that by not providing the Applicant's full primary name (including middle name where applicable) or providing false or incorrect information, may result in a bankruptcy check that is incomplete or incorrect.

11.3 Further to clause 11.2, the Applicant will ultimately be responsible for providing the information that will be used to conduct the bankruptcy check. In any event:

(a) we do not independently verify the information that has been declared in the fit2work platform by the Applicant or you;

(b) we take no liability for any incorrect or incomplete bankruptcy check caused by you or the Applicant providing incomplete or incorrect information; and

(c) we do not provide any guarantee or warranty as to the accuracy or completeness of any information provided to you or the Applicant.

12. Confidential Information

Where you are aware of any suspected or actual breach of clause 9 of the Terms of Supply, you must notify us immediately and take all reasonable steps to prevent or stop the suspected or actual breach.

13. Intellectual Property

12.1 In order for us to provide you with the fit2work services under this SOW, we may incorporate data obtained from third-party sources including (but not limited to) AHPRA Data into the fit2work services.

12.2 In addition to clause 8 of the Terms of Supply, you acknowledge and agree that the Intellectual Property Rights in the data outlined in clause 12.1 of this SOW will remain the sole property of the party that provided the data.

12.3 Nothing in this SOW assigns, grants or transfers any right, title or interest in the data outlined in clause 12.1 of this SOW, to you.

Schedule 1 – Dictionary

In this fit2work SOW:

(a) "ACC Act" means the *Australian Crime Commission Act 2002* (Cth);

(b) "Account Representative" means an officer appointed by us and notified to you as our primary point of contact for your dealings with us;

(c) "ACIC" means the Australian Criminal Intelligence Commission;

(d) "Accredited Body" means an accredited body under section 46A(5) of the ACC Act having an agreement with ACIC permitting it to access the National Police Checking Service;

(e) "AFP" means the Australian Federal Police;

(f) **AHPRA Data** means health practitioner registration data obtained from the Australian Health Practitioner Regulation Agency and incorporated or uploaded into the eCredential platform and provided as part of the eCredential Services.

(g) "AML/CTF Act" means, as relevant, the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) or *Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (*NZ);

(h) "Approved Purpose" means:

(i) the use of our fit2work information services for pre-employment and employment screening in accordance with the consent given to you by the relevant Applicant; or

(ii) such other purpose as we may expressly agree with you in writing;

(i) "Authorised Client" means, where you act as an agent or service provider to provide recruitment or other employment-related services or real estate services to a third party who is your customer or to whom you otherwise provide a service, that person;

(j) "Authorised Officer" means the officer appointed, or deemed to be appointed, by you under clause 3.1 of this SOW and as specified in an Onboarding Form or any updated advice to us;

(k) "Commencement Date" means the date you establish account arrangements with us to use our fit2work services;

(l) "Consumer" has the same meaning as given by the Consumer Law;

(m) "deal" includes collecting, recording, holding, organising, storing, adapting, altering, retrieving, consulting, using, disclosing, transferring, providing access, combining, blocking, erasing or destroying and "dealing" has a corresponding meaning;

(n) "employer" means the entity that employs or otherwise retains you, or may employ or otherwise retain you, where that entity has obtained your consent to the collection of your personal information for purposes of a relevant information service, and includes:
(i) any entity retaining or seeking to retain your services under contract or other similar service arrangement;
(ii) an entity in which you are, or are seeking to become, enrolled or a member (including any educational, social or charitable institution): and
(iii) where relevant, an Authorised Client;

(o) "EU" means that organisation of European countries known as the 'European Union' having joint policies on matters such as trade, agriculture and finance;

(p) "fit2work Badge" means that fit2work service providing a profile badging system to a Consumer Applicant, allowing them to share their verified credentials with employers through allocation of a unique ID number that can be verified independently via the fit2work website;

(q) "fit2work services" means our supply of any of the information services described in clause 1.5 of this SOW;

(r) "Gateway Service" means a service that enables authorised users to connect to and interact with document issuers or Official Record Holders through an intermediary hub;

(s) "GDPR" means the General Data Protection Regulation as created by the European Commission;

(t) "Home Affairs" means the Commonwealth of Australia represented by the Department of Home Affairs ABN 33 380 054 835;

(u) "Insolvency Register" means, as relevant, the *National Personal Insolvency Index* maintained by the Australian Financial Service Authority or the *Insolvency Register* maintained by Records NZ;

(v) "Jobfit" means Jobfit Health Group Pty Ltd ABN 40 083 014 340 and includes any Affiliates or contractors working on its behalf;

(w) "MoJ" means the Ministry of Justice (Tāhū o te Ture) in New Zealand;

(x) "Official Record Holder" means, in respect of a supported document, the entity against whose official record data the information submitted is requested to be matched (or attempted to be matched);

(y) "Onboarding Form" means an application to us, completed by you in the form we provide to you; and

(z) "Privacy Legislation" means the Privacy Act, any regulations, directives or other subordinate legislation made under a Privacy Act, and any other legislation applying in Australia (including of the Commonwealth of Australia or any State or Territory of Australia) or in New Zealand from time to time affecting privacy, personal information or the collection, handling, storage, processing, use or disclosure of personal information (including health information), data and other types of information and includes the *Spam Act 2006* (Cth), *Do Not Call Register Act 2006* (Cth), *Commonwealth Electoral Act 1918* (Cth), the *Telecommunications Act 1997* (Cth) and the *Unsolicited Electronic Messages Act 2007* (NZ), regardless of whether those Laws would apply to you but for this agreement.

SCHEDULE - NATIONAL POLICE CHECKING SERVICES TERMS AND CONDITIONS

LEGAL ENTITY CUSTOMER CONTRACT

IN RELATION TO THE PROVISION OF NATIONALLY COORDINATED CRIMINAL HISTORY CHECK INFORMATION

NOTE: This schedule incorporates the model Legal Entity Customer Contract as proposed by ACIC to assist Accredited Bodies (such as Equifax) in complying with obligations under the Agreement with the ACIC to access nationally coordinated criminal history checks on behalf of a Legal Entity Customer or Related Government Entity (whichever applies) as Client.

CONTENTS

LEGAL ENTITY CUSTOMER CONTRACT

Date

This Contract is dated as of the Commencement Date.

Parties

This Contract is made between you as the Legal Entity Customer and us as the Accredited Body.

Recitals

A. The Australian Criminal Intelligence Commission (**ACIC**) administers access to nationally coordinated criminal history checks under the *Australian Crime Commission Act 2002* (Cth) (**ACC Act**). The National Police Checking Service (**ACIC Service**) facilitates access to Police Information and nationally coordinated criminal history checks in partnership with the Australian police agencies in accordance with relevant Australian legislation.

B. The ACIC Service provides bodies accredited in accordance with the ACC Act with Police Information to support the assessment of the suitability of people in positions of trust, specified fields of endeavour and as required to meet legislative requirements.

C. The Accredited Body is an accredited body under section 46A(5) of the ACC Act and has an agreement with the ACIC (**ACIC Agreement**) before it is permitted to access the ACIC Service.

D. In order for the Accredited Body to access the ACIC Service on behalf of the Legal Entity Customer to provide the Legal Entity Customer with services relating to national policing information, the Accredited body must have a commercial proposal to have Legal Entity Customers approved by the ACIC and enter into a Legal Entity Customer contract.

E. The Parties acknowledge that the ACIC has approved the Accredited Body to provide services relating to national policing information to Legal Entity Customers and agree to enter into this Contract.

1. Interpretation

1.1. Definitions

1.1.1. Unless otherwise indicated, terms defined below have the followingmeanings:

Accredited Body means Equifax Australasia Workforce Solutions Pty Ltd ABN 86 080 799 720.
Applicant means a person in relation to whom the Legal Entity Customer seeks a nationally coordinated criminal history check.
Australian Privacy Principle Entity (or **APP Entity**) has the same meaning given to the term 'APP entity' in the *Privacy Act 1988* (Cth).
Commencement Date has the same meaning as in the fit2work SOW.
Commencement of Identity Document means the documents identified as 'Commencement of Identity Documents' in clause 1(b) of Annexure A (Identity Proofing Documents and Processes).
Commonwealth means the Commonwealth of Australia and includes the ACIC. **Commonwealth Confidential Information** means information that:
(a) is Police Information;
(b) is provided by, or originates from, the Commonwealth and is by its nature confidential, including the name or contact details of any staff member or security information relating to the provision of the Service; or
(c) the ACIC and the Accredited Body have agreed in writing is confidential (whether through the ACIC Agreement or otherwise).
Contract means the contract contained in this Schedule and includes all schedules and attachments to it;
Disclaimer means the disclaimer set out in Schedule 2 to this Contract.
Expiry Date means the date on which the agreement between the Accredited Body and the Legal Entity Customer is terminated under clause 3.2 of the Terms of Supply, provided that such date is not later than the expiry date of the Accredited Body's Agreement with ACIC (in which case, it is that expiry date).
GST means any tax imposed by the GST Act.
GST Act means *A New Tax System (Goods and Services Tax) Act 1999* (Cth).
Informed Consent has the meaning as given in clause 3.8.2 of this Contract.
Item means an item in schedule 1 to this Contract.
Law means any applicable statute, regulation, by-law, ordinance or subordinate legislation in force from time to time in Australia, whether made by the Commonwealth, a State, Territory or a local government, and includes the common law and rules of equity as applicable from time to time.
Legal Entity Customer means you.
Legal Entity Customer Contract Schedule means schedule 1 to this Contract.
Nationally Coordinated Criminal History Check means a criminal history check conducted, in relation to an Applicant, by the ACIC as part of the ACIC Service and carried out in accordance with the ACIC Agreement between the ACIC and the Accredited Body in relation to the ACIC Service, and the Police Information about an Applicant provided by the Accredited Body to the Legal Entity Customer in a physical or electronic format as a result of the submission of the nationally coordinated criminal history check Application.
Nationally coordinated criminal history check Application (**Application**) means a form (in physical or electronic format) completed by the Applicant, or on behalf of the Applicant, submitted to the Accredited Body requesting the ACIC to conduct a nationally coordinated criminal history check in relation to an Applicant.
Nationally coordinated criminal history check category means one or more categories listed in Item 1 of Schedule 1 to this Contract, being the categories and purpose for which the Legal Entity Customer is permitted to collect, use or disclose Personal Information and Police Information under clause 6.1.3(a) of this Contract.
National Policing Information has the meaning given in the *Australian Crime Commission Act 2002* (Cth).
Permitted Offshore Transfer means the permitted transfer of Personal Information or Police Information to a location outside Australia, where the transfer is:

(a) to provide an Applicant with access to the result of a nationally coordinated criminal history check in relation to the Applicant, where:

(i) the Applicant is located outside Australia; and

(ii) the Applicant has consented to the transfer or supply of Personal Information or Police Information to a location outside Australia; and/or

(b) for the purpose of routing Personal Information or Police Information through servers located outside Australia, where:

(i) the end recipient of that Personal Information or Police Information is located within Australia; and

(ii) the Personal Information or Police Information is retained or stored only on databases, servers or systems located within Australia; and/or

(c) for the purposes of retaining or storing Personal Information or Police Information on databases, services or systems located outside Australia where:

(i) the Applicant has consented to the retention or storage; and

(ii) the ACIC has approved, in writing, the Accredited Body's ICT environment for the retention or storage of Personal Information or Police Information on databases, services or systems located outside Australia; and/or

(d) for any other purpose for which the Applicant has consented to the transfer or supply of Personal Information or Police Information to a location outside Australia.

Personal Information has the meaning given in the *Privacy Act 1988* (Cth).

Personnel means:

(a) in relation to the Legal Entity Customer, the Legal Entity Customer's each employee, each Subcontractor and any officer, contractor, partner, volunteer, agent, director, board member of the Legal Entity Customer or a Subcontractor;

(b) in relation to the Accredited Body, the Accredited Body's authorised officer, each Subcontractor and any officer, employee, contractor, partner, volunteer, agent, director, board member of the Accredited Body or a Subcontractor; and

(c) in relation to the Commonwealth, officers, employees, volunteers, agents or contractors of the ACIC or any entity that is contracted by the ACIC other than the persons and entities referred to in paragraph (a) of this definition.

Police Information means any of the following information:

(a) information collected for the purposes of providing the Service;

(b) information collected for the purposes of a nationally coordinated criminal history check; and

(c) information released as part of a nationally coordinated criminal history check including information contained in a nationally coordinated criminal history check.

Primary Use in Community Document means a document named as such in Annexure A (Identity Proofing Documents and Processes).

Privacy Act means the *Privacy Act 1988* (Cth).

Safeguards means practices that a professional organisation handling Personal Information would implement to appropriately protect that information and include the Protection of Personal Information and Police Information Safeguards set out at Annexure B.

Secondary Use in the Community Document means a document named as such in Annexure A (Identity Proofing Documents Processes).

Service means the provision of information relating to the result of a nationally coordinated criminal history check in relation to an Applicant.

Vulnerable Group means:

(a) a child; or

(b) an adult who is:

(i) disadvantaged or in need of special care, support, or protection because of age, disability, or risk of abuse or neglect; or

(ii) accessing a service provided to disadvantaged people.

1.1.2. In this Contract:

a. the singular includes the plural;

b. a reference to one gender includes a reference to all other genders; and

c. any reference to any statute or regulation includes all amendments and revisions made from time to time to that statute or regulation.

1.1.3. Headings in this Contract have been inserted for convenience and reference only.

1.1.4. No rule of construction shall apply to the disadvantage of any party on the basis that it put forward this document.

1.1.5. Any variation to this Contract must be in writing and signed on behalf of each party. The variation will take effect from the date specified in the variation document. This may be done by exchange of letters or counter signing of a letter sent by one party to the other.

1.1.6. Any rights conferred under this Contract upon the ACIC or the Commonwealth are held on trust by the Legal Entity Customer for the benefit of the ACIC.

2. Duration of this Contract

2.1.1. This Contract commences on the Commencement Date and ends on the Expiry Date unless it is extended for a further period by both parties in writing or terminated earlier by either party in writing.

3. Services

3.1. General obligations

3.1.1. The Legal Entity Customer must:

a. not provide use of the Service or access to nationally coordinated criminal history checks to other parties;
b. not send any Police Information or Personal Information about an Applicant to an overseas recipient unless the Legal Entity Customer has the prior approval of the Applicant;
c. act in accordance with the Privacy Act, as if it were an APP Entity;
d. grant the Accredited Body or its authorised officer a right of access to the Legal Entity Customer's premises (and to data, records and other material relevant to the use of the Service and the handing of Police Information, including the right to copy), which the Accredited Body must exercise reasonably and subject to the Legal Entity Customer's reasonable safety and security requirements;
e. only request nationally coordinated criminal history checks for the nationally coordinated criminal history check category set out in Schedule 1 to this Contract; and
f. only use the Service in accordance with this Contract.

3.2. Process for requesting a nationally coordinated criminal history check

3.2.1. Before submitting a request for a nationally coordinated criminal history check, the Legal Entity Customer must provide the Accredited Body with:

a. the Applicant's Application completed in accordance with clause 3.3; and
b. the Applicant's Informed Consent,

for the purpose of the nationally coordinated criminal history check.

3.2.2. The Accredited Body will not submit to the ACIC any request for a nationally coordinated criminal history check unless it has collected the Applicant's Application and Informed Consent in accordance with the requirements set out in this Contract.

3.3. Nationally coordinated criminal history check Application requirements

3.3.1. A nationally coordinated criminal history check Application (Application) must include the following information:

a. the Applicant's surname and given name(s), and all names under which the Applicant was, is or has been known;
b. the Applicant's date and place of birth;
c. the Applicant's gender;
d. the Applicant's residential address(es) for the past five (5) years;
e. if available, the Applicant's driver licence details;
f. if available, the Applicant's firearms licence details;
g. the position title, occupation or entitlement being sought by the Applicant;
h. the proposed place of work and whether the applicant will have contact with Vulnerable Groups;
i. the nationally coordinated criminal history check category to which the nationally coordinated criminal history check relates;
j. a statement or endorsement confirming the Legal Entity Customer is satisfied as to the correctness of the Applicant's identity and has verified the Applicant's identity documents in accordance with clauses 3.4 and 3.5.

3.3.2. The Applicant's Application must:
a. be completed by the Applicant and include the Applicant's signature (in physical or electronic format) and date of signature; or
b. if the Applicant is under 18 years of age — be completed by a parent or legal guardian of the Applicant and include the signature (in physical or electronic format) of the parent or legal guardian and date of signature.

3.4. Confirmation of Applicant's identity

3.4.1. When reviewing an Applicant's Application and Informed Consent, the Legal Entity Customer must satisfy itself as to:
a. the Applicant's identity; and
b. the linkage between the Applicant and the claimed identity.

3.5. Requirements to confirm Applicant's identity

3.5.1. In satisfying itself, the Legal Entity Customer must sight four documents consisting of:
a. at least one of the documents listed as a 'Commencement of Identity Document';
b. at least one of the documents listed as a 'Primary Use in Community Document' that is also a photo identity document; and
c. at least two of the documents listed as a 'Secondary Use in the Community Document'.

3.5.2. The Legal Entity Customer may, for the purpose of clause 3.5.1, sight the documents:
a. locally, by sighting an original of the documents presented by the Applicant in person; or
b. remotely, by sighting a copy of each document that has been submitted by the Applicant via post or electronic submission.

3.5.3. The combination of the Applicant's identity documents must include the Applicant's full name, date of birth and a photograph of the Applicant. If the Applicant does not have an identity document containing a photograph from one of the documents listed as a 'Commencement of Identity Document' or from one of the documents listed as a 'Primary Use in Community Document', the Applicant must submit a passport style photograph that has been certified by a person listed in Schedule 2 of the *Statutory Declarations Regulations 1993* (Cth) that the photograph is a photograph of the Applicant.

3.6. Special provisions for Applicants unable to meet the clause 3.5 identity requirements

3.6.1. There are special provisions that apply to the following categories of Applicants who may be unable to meet the identity requirements in clause 3.5:
a. persons whose birth was not registered;
b. people who are homeless

c. recent arrivals in Australia;
d. people living in remote areas;
e. people who are transgender or intersex;
f. people affected by natural disasters;
g. people with limited access to identity documents for reasons associated with how they were raised, such as institutional or foster care;
h. people with limited participation in society; and
i. young people who are yet to establish a social footprint or evidence of community participation.

3.6.2. The Legal Entity Customer must meet the minimum requirements for these categories as advised by the ACIC to the Accredited Body and notified by the Accredited Body to the Legal Entity Customer.

3.7. Collection of Applicant's Informed Consent

3.7.1. The Legal Entity Customer will not submit to the Accredited Body any request for a nationally coordinated criminal history check unless it or the Legal Entity Customer has collected the Applicant's Informed Consent for the nationally coordinated criminal history check.

3.7.2. For the purpose of this Contract, an Informed Consent is a consent form (in physical or electronic format) that:

a. is completed by the Applicant and includes the Applicant's signature (in physical or electronic format) and date of signature; and
b. if the Applicant is under 18 years of age — is completed, dated and signed by a parent or legal guardian of the Applicant and includes the signature (in physical or electronic format) of the parent or legal guardian and date of signature; and
c. sets out at a minimum:
    i. the Applicant's surname and given name(s);
    ii. an acknowledgement that the Applicant consents to a nationally coordinated criminal history check being undertaken on all names under which the Applicant was, is or has been known, as provided by the Applicant as per **clause 3.3.1.**
    iii. the purpose of the nationally coordinated criminal history check;
    iv. the purpose(s) for which the Applicant's Personal Information is being collected and the purpose(s) for which the nationally coordinated criminal history check is being undertaken;
    v. any person to whom, or organisation to which, Personal Information (including Police Information) may be disclosed and in what circumstances (including the Accredited Body, the ACIC, Australian police agencies and third parties);
    vi. where consent is required for a Permitted Offshore Transfer, the details of to whom and in which country or countries the Applicant's Personal Information will be disclosed;
    vii. any Law which requires that the Applicant's Personal Information be collected and the consequences of non-compliance;
    viii. an acknowledgement that the Applicant understands that their Personal Information may be used for general law enforcement purposes, including those purposes set out in the *Australian Crime Commission Act 2002* (Cth);
    ix. information that the Applicant is required to contact the Legal Entity Customer in the first instance in relation to any dispute about the result of the nationally coordinated criminal history check in relation to the Applicant;
    x. information about the Legal Entity Customer's nationally coordinated criminal history dispute process including the contact details of its complaints and privacy officer;
    xi. if a Law requires Police Information about the Applicant to be disclosed to another person or organisation — information that the Police Information will be disclosed to that person or organisation and the basis for the disclosure; and
    xii. the Legal Entity Customer's full name and contact details.

4. Limitations of Service

4.1.1. The Legal Entity Customer acknowledges and agrees that the provision of a nationally coordinated criminal history check to the Legal Entity Customer is for use on the following conditions:

a. the ACIC makes no representation or warranty of any kind in respect to accuracy; and
b. the ACIC does not accept responsibility or liability for any omission or error in the nationally coordinated criminal history check.

4.1.2. The Legal Entity Customer must ensure that any Police Information or Personal Information in a nationally coordinated criminal history check provided under this Contract to any person includes the Disclaimer at **Schedule 2** (as amended from time to time).

5. Suspension of Service

5.1.1. The Accredited Body may, at its discretion and in addition to any other rights it has under this Contract, suspend or reduce the Legal Entity Customer's level of access to, or use of, the Service where:

a. the Legal Entity Customer has breached a term or condition of this Contract; or
b. the Accredited Body reasonably suspects that the Legal Entity Customer has committed or may commit a breach of a term or condition of this Contract,

until such time as the breach by the Legal Entity Customer has been remedied to the Accredited Body's satisfaction.

5.1.2. The Legal Entity Customer must continue to perform its obligations under this Contract notwithstanding any suspension or reduction of the Service.

5.1.3. In the event that:

a. the ACIC suspends or reduces the Accredited Body's level of access to, or use of, the Service; and
b. that suspension or reduction affects the Accredited Body's ability to provide the Service to the Legal Entity Customer,

the Legal Entity Customer acknowledges that its level of access to, or use of, the Service will also be suspended or reduced by the Accredited Body or the ACIC.

6. Protection of Police Information and other Personal Information

6.1. Obligations of Legal Entity Customer and its Personnel in relation to Personal Information

6.1.1. The Legal Entity Customer acknowledges that its use of the Service involves:

a. the collection, use and disclosure by the Legal Entity Customer of Personal Information that is required to complete and submit an application to use the Service and obtain a nationally coordinated criminal history check; and
b. the collection, use and possible disclosure by the Legal Entity Customer of Police Information.

6.1.2. Irrespective of whether or not the Legal Entity Customer would otherwise be bound, by entering into this Contract, the Legal Entity Customer agrees to be bound by the Privacy Act as if it were an Agency.

6.1.3. The Legal Entity Customer must in its use of the Service:

a. collect, use or disclose Personal Information and Police Information only for the nationally coordinated criminal history check category and related administration;
b. not collect, transfer, store or otherwise use Personal Information or Police Information outside Australia, or allow parties outside Australia to have access to Personal Information or Police Information, unless a Permitted Offshore Transfer circumstance applies;
c. not disclose Police Information other than for the purpose for which the Applicant gave

Informed Consent unless it has the prior written approval of the ACIC;

d. not commit any act, omission or engage in any practice which is contrary to the Privacy Act;
e. not do any act or engage in any practice that would be a breach of an APP or a Registered APP Code (where applied to the Legal Entity Customer) unless that act or practice is explicitly required under this Contract;
f. implement Safeguards to keep Personal Information and Police Information secure;
g. comply with any directions or guidelines in relation to the treatment of Personal Information and Police Information, notified to the Legal Entity Customer by the Accredited Body; and
h. ensure that all Personnel who are required to deal with Personal Information and Police Information are made aware of the obligations of the Legal Entity Customer set out in this clause 6.1.

6.1.4. The Legal Entity Customer must, on request by the Accredited Body or the ACIC, promptly provide the Accredited Body or the ACIC with a copy of the Legal Entity Customer's privacy policy.

6.2. Restrictions on altering nationally coordinated criminal history Checks

6.2.1. The Legal Entity Customer must not alter the content of a nationally coordinated criminal history check provided to the Legal Entity Customer by the Accredited Body or by the ACIC, including:

a. any Police Information;
b. any Personal Information; and
c. the Disclaimer for Limitations of Service as at **Annexure C**.

6.2.2. The Legal Entity Customer may:

a. make minor alterations to the format or presentation of the nationally coordinated criminal history check to the extent that any alternation does not change the content of any Police Information or Personal Information or the Disclaimer for Limitations of Service as at **Annexure C**.

6.3. Retention of nationally coordinated criminal history checks and related material

6.3.1. The Legal Entity Customer must securely retain:

a. each Application for a nationally coordinated criminal history check and any documents presented remotely by the Applicant for the purposes of clause 3.5, for a minimum period of twelve (12) months after the receipt of the nationally coordinated criminal history check to which the Application relates; and
b. each Applicant's Informed Consent for a nationally coordinated criminal history check for a minimum period of twelve (12) months following the receipt of the nationally coordinated criminal history check to which the consent relates.

6.4. Disposal of nationally coordinated criminal history checks and related material

6.4.1. The Legal Entity Customer must destroy or securely dispose of all hard and electronic copies (including backed up versions held on servers or other media) of:

a. each nationally coordinated criminal history check within twelve (12) months following the receipt of the nationally coordinated criminal history check;
b. each Application for a nationally coordinated criminal history check and any documents presented remotely by the Applicant for the purposes of clause 3.5, within three (3) months following the required document retention period under clause 6.3.1a; and
c. each Applicant's Informed Consent for a nationally coordinated criminal history check within three (3) months following the required document retention period under clause 6.3.1b,

unless a longer document retention period is required by Law, in which case the Legal Entity Customer must dispose of the material within one (1) month following the end of the document retention period required by Law.

6.5. Legal Entity Customer to give notice of breach or possible breach of clause 6

6.5.1. The Legal Entity Customer must notify the Accredited Body immediately if the Legal Entity Customer becomes aware of a breach or possible breach of any of the obligations contained in, or referred to in this clause 6, whether by the Legal Entity Customer or its Personnel.

7. Audits and access to premises and information

7.1. Right to conduct audits and compliance activities

7.1.1. The ACIC, including its authorised Personnel, may conduct audits relevant to the Legal Entity Customer's compliance with this Contract. Audits may be conducted of:

a. the Legal Entity Customer's operational practices and procedures as they relate to this Contract;
b. the Legal Entity Customer's compliance with its privacy and confidentiality obligations under this Contract including that the nationally coordinated criminal history check has been used only for the nationally coordinated criminal history check category; and
c. any other matters determined by the ACIC to be relevant to the use of the Services or the performance of this Contract.

7.2. Process of Conducting the Audits

7.2.1. The Legal Entity Customer must participate promptly and cooperatively in any audits conducted by the ACIC or its authorised Personnel.

7.2.2. Each Party must bear its own costs associated with any audits.

7.3. Access to Legal Entity Customer sites or premises

7.3.1. For the purposes of the ACIC conducting audits under this clause 7, the Legal Entity Customer must, as required by the ACIC or its authorised Personnel:

a. grant the ACIC and its authorised Personnel access to the Legal Entity Customer's premises and data, records and other material relevant to the performance of this Contract; and
b. arrange for the ACIC and its authorised Personnel to inspect and copy data, records and other material relevant to the performance of this Contract.

7.4. ACIC conduct in relation to audit and access

7.4.1. The rights referred to in clauses 7.1 and 7.3 are, wherever practicable, subject to:

a. the ACIC providing the Legal Entity Customer with at least three (3) business days' prior notice; and
b. the Legal Entity Customer's reasonable security requirements or codes of behaviour,

except where the ACIC or its authorised Personnel believes that there is a suspected or actual breach of law.

7.5. Auditor-General and Privacy Commissioner and Ombudsman rights

7.5.1. The rights of the ACIC under this clause 7 apply equally to:
a. the Auditor-General or a delegate of the Auditor-General;
b. the Privacy Commissioner or a delegate of the Privacy Commissioner;
c. the Commonwealth Ombudsman or a delegate of the Commonwealth Ombudsman,

for the purpose of performing the Auditor-General's, Privacy Commissioner's or the Commonwealth Ombudsman's statutory functions or powers.

7.5.2. Nothing in this Contract limits or restricts in any way any duly authorised function, power, right or entitlement of the persons listed in clause 7.5.1.

8. Access to documents

8.1.1. If the Commonwealth receives a request for access to a document created by or in the possession of the Legal Entity Customer that relates to this Contract, the ACIC or Accredited Body may at any time by notice require the Legal Entity Customer to provide the document to the ACIC and the Legal Entity Customer must, at no additional cost to the Commonwealth or the Accredited Body, promptly comply with the notice.

8.1.2. If the Legal Entity Customer receives a request for access to a document in its possession that relates to this Contract, the Legal Entity Customer must consult with the Accredited Body and the ACIC upon receipt of the request.

9. Intellectual Property

9.1. Ownership of Police Information

9.1.1. Intellectual Property in Police Information is owned by the Commonwealth and the Australian police agencies. Nothing in this Contract affects the ownership of Intellectual Property in Police Information (including any copy thereof) provided to the Legal Entity Customer.

9.1.2. The Accredited Body grants to the Legal Entity Customer a royalty-free, non- exclusive licence to use and communicate Police Information in accordance with this Contract.

9.2. No change to ownership of other relevant documents

9.2.1. Nothing in this Contract affects the Commonwealth's ownership of Intellectual Property in any other material relevant to or associated with the Service, including branding, graphic design, policies, guidance materials, certificates and forms.

10. Security of Commonwealth's Confidential Information

10.1. Legal Entity Customer to secure Commonwealth's Confidential Information

10.1.1. The Legal Entity Customer agrees to secure all of the Commonwealth's Confidential Information (including Police Information) against loss and unauthorised access, use, modification or disclosure.

10.1.2. The Legal Entity Customer may wish to provide Applicants with the opportunity to submit Personal Information electronically. If so, the Legal Entity Customer must secure Personal Information belonging to Applicants against loss and unauthorised access, use, modification or disclosure, and notify the Applicant of these risks.

10.2. Written undertakings

10.2.1. The Legal Entity Customer must, on request by the Accredited Body or the ACIC at any time, promptly arrange for the Legal Entity Customer's Personnel to give a written undertaking in a form acceptable to the Accredited Body or the ACIC relating to the use and non-disclosure of the Commonwealth's Confidential Information (including Police Information).

10.3. Period of Confidentiality

10.3.1. The obligations under this clause 10 survive the expiry or termination of this Contract and exist in perpetuity, unless otherwise notified by the Accredited Body or the ACIC.

10.3.2. The obligations contained in this clause 10 are in addition to those specified in clauses 4 and 9.

11. Termination

11.1. Termination or reduction in scope for convenience

11.1.1. The Accredited Body may terminate this Contract or reduce the scope of this Contract (including by reducing or removing any nationally coordinated criminal history check categories) by notice at any time, as a result of a termination or reduction of Scope of the Accredited Body's Agreement with the ACIC.

11.1.2. The Legal Entity Customer will not be entitled to any compensation whatsoever including for loss of prospective profits or loss of any benefits that would have been conferred on the Legal Entity Customer if the termination or reduction had not occurred. The Accredited Body will only be liable for repayment of any outstanding nationally coordinated criminal history checks requested, and paid for, by the Legal Entity Customer prior to the effective date of termination.

11.1.3. This clause 11.1 does not affect the Accredited Body's other rights under this Contract or otherwise at law.

11.2. Termination for default

11.2.1. The Accredited Body may terminate this Contract immediately by notice to the Legal Entity Customer if any of the following termination events occur:

a. the Legal Entity Customer breaches a material provision of this Contract where the breach is not capable of remedy;
b. the Legal Entity Customer breaches any provision of this Contract and does not rectify the breach within 14 days after receipt of the Accredited Body's notice to do so;
c. the Accredited Body is satisfied on reasonable grounds that the Legal Entity Customer is unable or unwilling to satisfy the terms of this Contract;
d. the Legal Entity Customer comes under any form of administration or assigns its rights otherwise than in accordance with this Contract;
e. the Legal Entity Customer is unable to pay all its debts as and when they become payable or fails to comply with a statutory demand;
f. proceedings are initiated with a view to obtaining an order for winding up the Legal Entity Customer;
g. the Legal Entity Customer becomes bankrupt or enters into a scheme of arrangement with creditors;
h. anything analogous to, or of a similar effect to, anything described in subclauses 11.2.1.d to 11.2.1(g) occurs in respect of the Legal Entity Customer; or
i. another provision of this Contract allows for termination under this clause 11.2.

11.2.2. This clause 11.2 does not affect the Accredited Body's other rights under this Contract or otherwise at law.

12. Dispute Resolution

12.1. This clause 12 applies only to disputes regarding this Contract. Disputes arising from nationally coordinated criminal history checks are to be handled by the Accredited Body in accordance with the Accredited Body's ACIC Agreement.

12.1.1. The Legal Entity Customer agrees to provide the ACIC with any information or materials reasonably requested by the ACIC, in order to allow the ACIC to resolve any dispute between itself and the Accredited Body.

12.1.2. A Party must comply with the following procedure in respect of any dispute arising under this Contract:

a. the Party claiming that there is a dispute will send the other Party a notice setting out the nature of the dispute ('Dispute Notice');
b. the Parties will try to resolve the dispute through direct negotiation, including by referring the matter to persons who have the authority to intervene and direct some form of resolution.

12.1.3 If the Parties are unable to resolve the dispute within 2 weeks of the relevant Party receiving the Dispute Notice, either Party may refer that dispute for resolution in accordance with the dispute resolution process accessible at *www.equifax.com.au/acicdispute*.

13. Survival

13.1.1. The termination or expiration of this Contract will not affect the continued operation of this clause 13 and any provision of this Contract which expressly or by implication from its nature is intended to survive including clauses 6 (protection of Police Information and other Personal Information) and 7 (Audits and access to premises and information).

14. Notices

14.1.1. A Party ('First Party') giving notice to the other Party under this Contract must do so in writing and that notice must be signed by the First Party's authorised officer, marked for the attention of the other Party's authorised officer and hand delivered or sent by prepaid post or email to the other Party's address for notices.

14.1.2. A notice given in accordance with clause 14.1.1 is received:
a. if hand delivered or if sent by pre-paid post, on delivery to the relevant address; or
b. if sent by email, when received by the addressee or when the sender's computer generates written notification that the notice has been received by the addressee, whichever is earlier.

SCHEDULE 1 (LEGAL ENTITY CUSTOMER CONTRACT SCHEDULE)

Item No.	Description	Particulars
1.	**Nationally coordinated criminal history check category**	Employment / Probity / License purposes only
2.	**Legal Entity Customer's authorised officer** Clause 14	The person correctly authorised by the Legal Entity Customer and occupying the position of Authorised Officer as defined in this fit2work SOW.
3.	**Legal Entity Customer's Address for Notices** Clause 14	As identified by the agreement with the Accredited Body for delivery of its fit2work services.
4.	**Accredited Body's Authorised Officer and Address for Notices** Clause 14	In the absence of a designated Account Representative for the Legal Entity Customer, the person correctly authorised by the Accredited Body occupying the position of Product Manager fit2work, the current contact details for whom are: 119 Cecil Street, South Melbourne 3205, VIC Australia P +61 3 9036 4437 *Wolfgang.Perner@equifax.com*

SCHEDULE 2 DISCLAIMER

NATIONALLY COORDINATED CRIMINAL HISTORY CHECK

LIMITATIONS ON ACCURACY AND USE OF THIS INFORMATION

1. This nationally coordinated criminal history check provides a point in time check about the applicant for an authorised nationally coordinated criminal history check category and purpose. Information obtained through this check should not be used for any otherpurpose.

2. The accuracy and quality of information provided in this nationally coordinated criminal history check depends on accurate identification of the applicant which is based on information, including aliases, about the applicant provided in the application and the comprehensiveness of police records.

3. While every care has been taken by the Australian Criminal Intelligence Commission ('ACIC')to conduct a search of police information held by it and Australian police agencies that relates to the applicant, this nationally coordinated criminal history check may not include all police information about the applicant. Reasons for certain information being excluded from the nationally coordinated criminal history check include the operation of laws that prevent disclosure of certain information, or that the applicant's record is not identified by the search process across the agencies' relevant information holdings.

4. This nationally coordinated criminal history Check maycontain any of the following information about an applicant:
   (a) charges;
   (b) court convictions;
   (c) findings of guilt with no conviction;
   (d) court appearances;
   (e) good behaviour bonds or other courtorders;
   (f) pending matters awaiting courthearing;
   (g) traffic offence history ('**Disclosable CourtOutcome**').

5. If this nationally coordinated criminal history check contains a Disclosable Court Outcome, the entity submitting the application is requiredto:
   (a) notify the applicant of the nationally coordinated criminal history check;and
   (b) provide the applicant with a reasonable opportunity to respond to, or validate the information, in the nationally coordinated criminal history check.

6. To the extent permitted by law, neither the ACIC nor Australian police agencies accept responsibility or liability for any omission or error in the nationally coordinated criminal history check.

NATIONALLY COORDINATED CRIMINAL HISTORY CHECK PROCESS

The information in this nationally coordinated criminal history check has been obtained according to the following process:

(a) the ACIC searches its data holdings for potential matches with the name(s) of the applicant;
(b) the ACIC and the relevant Australian police agencies compare name matches with police information held in Australian policerecords;
(c) the relevant Australian police agency identifies any police information held in its police records and releases the information subject to relevant spent convictions, non-disclosure legislation or information release policies;and
(d) the ACIC provides resulting information to the entity submitting theapplication.

Annexure A – Identity Proofing Documents and Processes

1. Name of person on identity documents

(a) The identity documents listed in this Annexure must be issued in the name of the person seeking to prove identity or in a former name of that person.

(b) Where a change of name has occurred and any of the documents listed in this Annexure are provided in a former name, evidence must also be submitted of an Australian Registry of Births, Deaths and Marriages issued change of name certificate or a Australian marriage certificate issued by a State or Territory (this does not include church or celebrant issued certificates).

2. Commencement of Identity Documents

The following documents are Commencement of Identity Documents for the purposes of clause 3.5.1(a) of the Contract and must not be expired:

(a) a full Australian Birth Certificate (not an extract or birth card);

(b) a current Australian Passport (not expired);

(c) Australian Visa current at time of entry to Australia as resident or tourist;

(d) ImmiCard issued by the Department of Immigration and Border Protection that assists the cardholder to prove their visa / migration status and enrol in services;

(e) certificate of identity issued by the Department of Foreign Affairs and Trade to refugees and non Australian citizens for entry to Australia;

(f) document of identity issued by the Department of Foreign Affairs and Trade to Australian citizens or persons who possess the nationality of a Commonwealth country, for travel purposes; and

(g) certificate of evidence of resident status.

3. Primary Use in Community Document

The following documents are Primary Use in Community Documents for the purposes of clause 3.5.1(b) of the Contract and must not be expired:

(a) a current Australian driver licence, learner permit or provisional licence issued by a State or Territory, showing signature and/or photo and the same name as claimed;

(b) Australian marriage certificate issued by a State or Territory (this does not include church or celebrant issued certificates);

(c) a current passport issued by a country other than Australia with a valid visa or valid entry stamp or equivalent;

(d) a current proof of age or photo identity card issued by an Australian government agency in your name with photo and signature;

(e) a current shooter or firearm licence showing signature and photo (not minor or junior permit or licence); and

(f) for persons aged under 18 with no other Primary Use in Community Documents, a current student identification card with photo or signature.

4. Secondary Use in the Community Documents

The following documents are Secondary Use in Community Documents for the purposes of clause 3.5.1(c) of the Contract and must not be expired:

(a) DFAT issued Certificate of Identity;

(b) DFAT issued Document of Identity;

(c) DFAT issued United Nations Convention Travel Document Secondary (*Titre de Voyage*);

(d) Foreign government issued documents (e.g. driver licences);

(e) Medicare Card;

(f) Enrolment with the Australian Electoral Commission;

(g) Security Guard/Crowd Control photo licence;

(h) Evidence of right to a government benefit (DVA or Centrelink);

(i) Consular photo identity card issued by DFAT;

(j) Police Force Officer photo identity card;

(k) Australian Defence Force photo identity card;

(l) Commonwealth or state/territory government photo identity card;

(m) Aviation Security Identification Card;

(n) Maritime Security Identification Card;

(o) Credit reference check;

(p) Australian tertiary student photo identity document;

(q) Australian secondary student photo identity document;

Annexure B – Protection of Personal Information and Police Information Safeguards

1. Introduction

(a) In accessing the Service, Legal Entity Customers must implement the security management measures set out in this Annexure B to ensure against:

(i) misuse, interference, loss, unauthorised access, modification or disclosure of Applicant's Personal Information;
(ii) unauthorised access to and use of the Service;
(iii) unauthorised access to Police Information in the Service Support National Police Checking Service Support System (**NSS**); and
(iv) loss and unauthorised access, use, modification or disclosure of Police Information stored outside of NSS.

(b) This information is provided to assist Legal Entity Customers understand their obligations and comply with the ACIC's security management standards.

2. Information Security Policy

(a) The Legal Entity Customer must develop, document and maintain an Information Security Policy (**Policy**) that clearly describes how it protects information.

(b) The Policy should be supported by the Customer's senior management and be structured to include any legal framework relevant to the Policy, such as the *Australian Crime Commission Act 2002* (Cth) and this Contract.

(c) The Policy must include adequate details on how it is enforced through physical, technical and administrative controls, including details on:

(i) the type or class of information that the Policy applies;
(ii) information security roles and responsibilities relating to the Service;
(iii) security clearance requirements and its Personnel's responsibilities;
(iv) configuration and change control;
(v) technical access controls;
(vi) staff training;
(vii) networking and connections to other systems;
(viii) physical security (including media security); and
(ix) incident management.

(d) The Legal Entity Customer's privacy policy must reference the Policy, in terms of how the Applicant's Personal Information is held (as per APP 1.4(b)).

3. Technical Access

The Legal Entity Customer's ICT environment must be secured in accordance with the Policy and should:
(a) be protected by appropriately configured gateway environment (including firewalls);
(b) include technical access controls protecting any National Police Information stored electronically outside of NSS, for example, restricted file system permissions; and
(c) maintain a static IP address to avail web services (if applicable).

4. Technical Infrastructure

(a) Workstations and server infrastructure involved in the storage or processing of National Police Information and Personal Information should be secured in accordance with the Policy and should:

(i) run current and patched operating systems;

(ii) run current and patched software, including browsers (N-1 on browsers is acceptable providing patching is maintained);
(iii) have anti-virus software application installed up-to-date virus definition files; and
(iv) run application whitelisting software (desirable).

(b) Administrative or privileged access to infrastructure is to be minimised and only used when an administrative function is required.

5.
Digital Certificates

Digital certificates used in the connection to the Service must be managed securely and ensure:
(a) certificates are not distributed beyond that required for connection;
(b) certificates are only installed on the Legal Entity Customer's corporate infrastructure (certificates must not be installed on home or personal computers); and
(c) passwords relating to certificates are securely stored.

6.
Password policy

System accounts that are involved in the storage or processing of National Police Information should be subject to a password policy that sets out:
(a) no less than 10 character passwords including a minimum of one numerical and one upper case character;
(b) password reset cycle no longer than 90 days;
(c) users to select strong passwords (avoid dictionary words);
(d) ensure unused accounts are disabled and removed; and
(e) computers lock after 15 minutes of inactivity.

7.
Training

All Legal Entity Customer Personnel involved in storage or processing of National Police Information and Personal Information must be provided with the information security awareness training related to:
(a) their responsibilities as defined in the Policy;
(b) what constitutes authorised access to information; and
(c) their obligations with regard to reporting of information security issues or incidents.

8.
Incident Management

Any information security issues or incidents must be reported immediately to the Accredited Body where the consequence may impact or has impacted on the Accredited Body's or ACIC systems or information. This includes, but is not limited to, loss or compromise of digital certificates or associated passwords.