# Terms and Conditions – Employment Verification by Equifax

By requesting the Services, you agree that these terms and conditions, including any Schedules, govern their supply and we will supply our Services to you after we accept your request for the Services. No confirmation, shipment or delivery docket, quote, purchase order, invoice or other document issued by you or on your behalf (including the terms on any pre-printed purchase order form) in relation to the Services will vary of form part of these Terms and Conditions.

**1. Defined Terms**

In these Terms and Conditions:

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

b. "ACIC" means the Australian Criminal Intelligence Commission;

c. "AFP" means the Australian Federal Police;

d. "Agreement" means these Terms and Conditions, any Schedule(s) and any document incorporated by express reference as part of these Terms and Conditions;

e. "Approved Purpose" means pre-employment and employment screening in accordance with the consent given to you by the relevant Individual;

f. "Authorised Clients" has the meaning ascribed in paragraph 3f;

g. "Authorised Officer" means the officer appointed, or otherwise identified, by you for purposes of clauses 3(g)(i) and 8(f);

h. "Change In Control" means a change in the control (as that term is defined in Division 6 of the Corporations Act) of a party.

i. "Client" means the company or entity that has requested to use our Services.

j. "Commencement Date" means 1 July 2018 or such later date as you establish account arrangements with us to use our Services;

k. "Corporations Act" means the *Corporations Act 2001* (Cth);

l. "Equifax", "we", "us" and "our" mean Equifax Australasia HR Solutions Pty Ltd ABN 74 153 363 494;

m. "Individual" means each person on whom you request Equifax to perform the Services;

n. "Initial Term" means the date starting on the Commencement Date and ending on the Termination Date.

o. "Insolvent" means being an insolvent under administration or insolvent (each as defined in the Corporations Act) or having a controller (as defined in the Corporations Act) appointed, or being in receivership, in receivership and management, in liquidation, in provisional liquidation, under administration, wound up, subject to any arrangement, assignment or composition, protected from creditors under any statute, dissolved (other than to carry out a reconstruction while solvent) or being otherwise unable to pay debts when they fall due or having something with the same or a similar effect happen under the laws of any jurisdiction.

p. "Law" means any statute, ordinance, or code and includes regulations, codes and other instruments under any of them and consolidations, amendments, re-enactments, or replacements of any of them;

q. "Personal Information" has the meaning given to it in the *Privacy Act 1988 (Cth)*;

r. "Privacy Legislation" means the *Privacy Act 1988 (Cth)* and any legislation from time to time in any Australian jurisdiction (which includes the Commonwealth of Australia and any state or Territory of Australia) affecting privacy, Personal Information or the collection, handling, storage, processing, use or disclosure of Personal 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)* and *Telecommunications Act 1997 (Cth)*;

s. "Renewal Term" means the period set out in a Schedule or otherwise a period of 3 months;

t. "Schedule" means each Schedule executed by the parties containing terms which govern the provision and use of the Services as outlined in that Schedule and may include Third Party Services;

u. "Services" means the services provided to you, including the information, data, products, services and reports provided to you by Equifax in response to your request;

v. "Termination Date" means the termination date set out in a Schedule or otherwise 31 March 2019;

w. "Terms and Conditions" means these terms and conditions and any additional terms and conditions in a Schedule;

x. "Third Party Services" means any services or data that has been supplied to Equifax by a third party, or any data that arises out of the performance of any Services which are provided to Equifax by a third party; and

y. "You" means the company or entity that has requested to use our Services.

**2. Supply of Information**

a. Equifax agrees to undertake the checks that you request and report on these in the fastest time possible. We are not liable for any delay or failure to provide information arising from, caused by or contributed to by you or any third party, however we will always employ best endeavours to complete the checks and will always notify you if this cannot be done in a timely manner.

b. You must provide us with all information, materials, assistance and decisions required to enable us to provide the Services and otherwise perform our obligations under these Terms and Conditions.

c. We cannot commence any work in respect of a verification request until we receive the necessary consents that we require from the Individual who is the subject of the request.

d. We will make a maximum of three attempts to verify information or obtain missing information before closing a verification or search as "unverified".

e. We reserve the right to close off an outstanding verification request after 15 working days from the date that the request is made by you, if you, or the Individual who is the subject of the request, have not responded to our notice for further instruction, and we have notified you of our intention.

f. You acknowledge that Equifax obtains all data supplied as part of the Services from third parties and relies on those suppliers of data to take reasonable steps to ensure that the data is accurate. You further acknowledge that Equifax does not independently verify the data and agree that Equifax does not provide any guarantee or warranty as to the accuracy or completeness of the data to you.

g. Equifax will provide the Services. You acknowledge and agree that Equifax may, after discussion with you, at its option and by providing 5 Business Days' notice to you, suspend provision of the Services or terminate the agreement formed by these Terms and Conditions if:

   i. the requirements of any law render (or are likely to render) the provision of the Services contrary to that or any other Law; or

   ii. any change in data access terms, regulatory policy or published view of a regulator renders (or is likely to render) the provision of the Services contrary to the established regulatory position or these terms and conditions.

   Where Equifax determines, acting reasonably, that it cannot continue to provide one or more of the Services under these Terms and Conditions, then it may cease to provide that Service, without any further obligation accruing to it under these Terms and Conditions.

h. In respect of Third Party Services, the liability and indemnities of the parties are set out in the respective Schedule(s) or if not specified therein, then in accordance with the terms of this clause.

**3. Your use of our Services**

a. You must use the Services, and any information provided to you as a part of the Services for the Approved Purpose only and at all times comply with these Terms and Conditions and all applicable Laws in all jurisdictions that relate to your access to and use of the Services.

b. You must:

   i. in your use of the Personal Information, comply with the *Privacy Act 1988* (Cth) and any additional Privacy Legislation by which you are bound. If you are a small business operator under the Privacy Act, then you agree to choose to be treated as an organisation bound by the Privacy Act in accordance with section 6EA of the Privacy Act;

   ii. use the Personal Information only for the Approved Purpose in accordance with your obligations under these Terms and Conditions;

   iii. restrict access to the Personal Information to employees who need to access the Personal Information to fulfil your obligations under these Terms and Conditions;

iv. take all reasonable steps to ensure that the Personal Information is protected against misuse and loss, or unauthorised access, modification or disclosure, including:

A. undertaking any staff training as may be required;

B. monitoring staff and third-party use of the Personal Information;

C. obtaining a written agreement from any third party to whom the Personal Information is disclosed to comply with Privacy Laws and contractual provisions having the same effect as this clause 3 of these Terms and Conditions;

D. during and after the term of this Agreement not do anything with the Personal Information that will cause you or Equifax to breach any Privacy Legislation and co-operate with Equifax to resolve any complaint made under any Privacy Legislation;

E. not transfer any Personal Information provided in connection with these Terms and Conditions to a country or territory outside of Australia, without Equifax's prior written consent;

F. immediately notify Equifax if you become aware of a breach of the Privacy Legislation in connection with this Agreement.

c. Equifax must:

i. comply with all applicable privacy laws, rules and regulations, including the *Privacy Act 1988* (Cth);

ii. only collect Personal Information under or in connection with this Agreement that is required in order to provide the Services to you;

iii. only use and disclose the Personal Information it receives under or in connection with this Agreement for the purposes of providing the Services to you;

iv. provide individuals a collection notice that meets the requirements of the *Privacy Act 1988* (Cth);

v. be responsible for ensuring that any sub-contractors engaged in providing the Services also comply with this clause 3(c);

vi. hold data provided by the Client or their candidates (**Data**) securely and take steps to prevent misuse, interference and loss of the Data and to prevent unauthorised access, modification or disclosure of the Data;

vii. advise the client if it receives a complaint about the handling of the Data and take steps to resolve the complaint;

viii. advise client in the event of a data breach or incident involving the Data, take steps to remedy the breach and prevent it from re-occurring;

ix. permit client to undertake annual privacy and security reviews to monitor compliance with this clause 3(c) of the Agreement:

x. destroy the Data when it is no longer legally required to be kept unless otherwise notified by the client or the extent that it is required by law to retain a copy of the Data;

xi. return or destroy all the Data at the end of the Term, as directed by the client, and certify in writing that it has done so.

d. In addition to the above, you acknowledge and agree that where in order to provide the Services Equifax needs to pass Personal Information to a third party, you have or will obtain valid authority of the relevant Individual to allow Equifax to provide the Services.

e. Except as expressly permitted by these Terms and Conditions and subject to clause 3(e) below, you must:

i. not re-sell, re-package or re-use information or permit third parties to use information supplied as part of the Services otherwise than as expressly permitted under these Terms and Conditions; or

ii. not use the information supplied as part of the Services for any purpose other than your internal business use and for the purposes for which it was supplied, save for disclosure as part of your statutory obligations including under the Privacy Legislation.

f. Where you are placing orders for the Services on behalf of your customer (**Authorised Clients**), you are permitted to use the Services and any information provided to you as a part of the Services for the sole purpose of providing recruitment or other employment-related services to the Authorised Client, provided that you do not use the Services for your own benefit. You:

i. warrant that you the authority to act as agent for the Authorised Client;

ii. shall ensure that each Authorised Client complies with this Agreement as if it were a party hereto;

iii. will be responsible for the acts and omissions of all Authorised Clients as fully as if they were your acts or omissions;

iv. indemnifies Equifax and its related bodies corporate (as that term is defined in the Corporations Act) against any liabilities, damages, losses, expenses, demands, claims, suits or judgements, including solicitors' fees, costs and expenses as a result of any acts or omissions of your Authorised Clients.

g. You warrant that:

i. the contact details you provide us for correspondence are suitable for maintaining the confidentiality of the information we send you and you agree to notify us immediately if you change it;

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

iii. if an Individual wishes to formally dispute the accuracy of any report provided by either ACIC or AFP, you will refer that Individual 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.

h. Each party owns, and will continue to own, all Intellectual Property Rights subsisting in any material it provides or makes available to the other party under or in connection with these Terms and Conditions (**Pre-existing Intellectual Property**).

i. All Intellectual Property Rights in documents, ideas, equipment, processes and systems which are acquired or created by Equifax in the course of supplying the Services to you are retained by Equifax (**New Intellectual Property**). Equifax grants you a perpetual, irrevocable royalty free licence to use the New Intellectual Property for the purposes of these Terms and Conditions.

j. You further acknowledge and agree that the Services and the information we provide to you are proprietary to us and comprise works of original authorship, including compiled information containing our selection, arrangement, coordination and expression of such information or pre-existing material it has gathered or assembled, confidential and trade secret information, and information that has been created, developed and maintained by us at considerable expense of time and money, such that misappropriation or unauthorised use by you or others for commercial gain would unfairly (and may irreparably) harm us.

**4. Exclusions and Limitations of Liability**

a. Nothing contained in this Agreement excludes, restricts, limits or modifies any:

i. implied condition, warranty or other term of these Terms and Conditions where pursuant to applicable Law to do so is unlawful or void; or

ii. liability in respect of a default or other breach of these Terms and Conditions where pursuant to applicable Law to do so is unlawful or void.

b. You acknowledge that the conditions and warranties contained in these Terms and Conditions are the only conditions and warranties in relation to these Terms and Conditions (other than those which cannot be excluded or limited by law) and to the maximum extent permitted by law:

i. that the Services are provided "as is" without warranty of any kind;

ii. 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 by you of the Services in assisting you to comply with any Law;

iii. We do not warrant that the provision of the Services will achieve any particular result. The Services are not a replacement for any other information, or for your decision-making policies and procedures. Accordingly, Equifax does not accept liability for any employment decision you or your Authorised Clients make using any information provided to you as a part of the Services and you assume all risk in connection with your use of, or reliance on, the Services (including any information obtained or derived through the Services); and

iv. Equifax makes no warranties or representations about information and data, including Personal Information, sourced from third parties that it provides under this Agreement, or its reliability, accuracy, completeness, or currency.

c. If applicable Law implies any guarantee in respect of the Services, the liability of Equifax for breach of any such implied guarantee will be limited to the cost of replacing those services or providing those services again.

d. Subject only to clause 4(a) above, in no event will Equifax be liable to you or to any third party for:
   i. any loss, damage, cost or expense of any nature arising or caused directly or indirectly by any breach of your obligations or responsibilities set out in these Terms and Conditions;
   ii. any and all liability for any loss or damage in relation to any decisions made as a result of the use of the Services;
   iii. any loss or damage in relation to the accuracy, completeness, currency or quality of information sourced from third parties that is provided as part of the Services;
   iv. any damages or losses which are not direct or do not flow naturally from the relevant default, even if those damages or losses may reasonably be supposed to have been in the contemplation of both parties as a probable result of the default;
   v. any indirect, incidental or consequential loss or damage or special, exemplary or punitive damages; or
   vi. any economic loss (including without limitation any loss of profits, business interruption, loss of revenue, loss of business opportunity, business advantage and/or expectation benefit),

   whether such liability is asserted on the basis of any common or civil law, in equity, pursuant to any statute, under any contract, in tort (including negligence or strict liability) or otherwise (and notwithstanding that Equifax has been advised of the possibility of any particular liability, loss or damage).

e. In respect of any default or other breach of this Agreement by Equifax (but subject always to the exclusion and/or limitation of Equifax's liability set out elsewhere in these Terms and Conditions), Equifax's total liability shall be limited to the value of the total fees paid or payable by you for Services the subject of the default or to which the default relates.

f. The parties acknowledge and agree that clause 4(e) does not apply to:
   i. a breach of clause 3(c);
   ii. the death of or injury to any agent, employee, invitee, visitor or other person to the extent caused by an act or ommission of Equifax;
   iii. any fraudulent acts or omissions, wilful misconduct, dishonesty, misrepresentation, misleading or deceptive or illegal conduct by Equifax.

**5. Indemnity**

a. You indemnify and hold harmless Equifax and its related bodies corporate, its officers employees and agents ("those indemnified") against all damages, loss, costs, expenses (including legal costs) or liabilities incurred or suffered by those indemnified arising out of:
   i. any unauthorised disclosure by you of Confidential Information;
   ii. any act or omission by you in reliance upon the Services;
   iii. any failure by you to comply with all Laws applicable to these Terms and Conditions; and
   iv. any warranty you provide being incorrect or misleading in any way.

b. Notwithstanding any other provision in this Agreement, your total aggregate liability in relation to this Agreement, including in relation to any indemnity in this Agreement (other than under clause 5.a), shall be limited to the value of the fees paid or payable by you to Equifax for the Services.

**6. Our Fees**

a. You must pay the fees for the Service you request in accordance with our prevailing price list as available at www.equifax.com.au/employmentverification at the time that you request a Service or as may otherwise be set out in a Schedule or any other current pricing agreement between us (including any cancellation fees you have incurred).

b. We will send you invoices monthly for all our fees and charges unless you are set up for pre-billing. Payments terms shall be set out on the relevant invoice or if none are specified, then 30 days from the date of the invoice. We reserve the right to suspend or cease providing services if our invoices are not paid promptly.

c. You agree to keep confidential the terms of supply including our fees, charges and pricing arrangement with you under this and any other agreement between us.

d. Pricing under this agreement is confidential and must not be disclosed to third parties.

e. In addition to the fees at 6(a) above (and if not otherwise specified in a Schedule or other pricing agreement between us), Equifax will charge additional fees for searches it conducts outside of Australia and New Zealand which are based on the country and type of verification request. Equifax will notify you of these additional fees and obtain your prior written consent to proceed before commencing the search.

f. Equifax will also charge any disbursements levied by third party information providers such as academic institutions, agencies, professional bodies etc. These will be charged at cost and capped at $250.

g. A verification request cannot be cancelled without our express agreement and subject to your payment of the following cancellation fees, expenses and third-party costs (if any):

| | | | |
|---|---|---|---|
| Applicable cancellation fee | Where consent and administration has commenced | Request is cancelled within 5 working days for consent and administration | $10 + GST |
| | | Request is cancelled between 5 - 40 working days for consent and administration | $25 + GST |
| | | Request is cancelled more than 40 working days or Equifax has not received any communication from you with respect to an outstanding request for services for consent and administration | 100% fee for the request |
| | Where checks have commenced | 100% fee for the request | |
| Expenses | All reasonable expenses incurred by Equifax in providing the Services up to the date of cancellation | | |
| Third party costs | As our third-party information providers charge us on submission of each verification, you shall also pay Equifax's reasonable and direct costs (on a pass-through basis only) of terminating its agreements with any relevant third-party suppliers used in relation to the Services | | |

**7. Term and Termination**

a. This agreement begins on the Commencement Date and continues for the Initial Term, unless terminated earlier in accordance with these Terms and Conditions. This agreement will continue beyond the Initial Term for one or more Renewal Terms unless a party notifies the other party at least 30 days prior to expiry of the Initial Term or then current Renewal Term that it does not wish the agreement to continue.

b. You may immediately terminate this Agreement, in whole or in part, by notice to Equifax:
   i. if Equifax breaches clause 3(c)(i), 3(c)(v) or 3(c)(vi);
   ii. if the continued provision of the Services would jeopardise the client's ability to comply with its independence obligations;
   iii. if Equifax breaches a provision of this Agreement and fails to remedy it within 30 days of receiving a notice from you detailing the breach and requesting that it be rectified;
   iv. Equifax becomes Insolvent.

c. Equifax may terminate this Agreement, in whole or in part, by notice to you:
   i. if you breach a provision of this Agreement and fails to remedy it within 30 days of receiving a notice from Equifax detailing the breach and requesting that it be rectified;
   ii. You become Insolvent;
   iii. You have a Change in Control;
   iv. Under clause 2g.

d. In addition to its other rights of termination, where Equifax holds a reasonable belief that you are in breach of any of the conditions set out in this Agreement Equifax may suspend provision of the whole or any part of the Services until such time as the breach is remedied.

e. The termination of this agreement does not affect any remedies which either party may have under this agreement or otherwise.

**8. General**

a. This agreement is governed by the laws of New South Wales and you submit to the non-exclusive jurisdiction of the courts of that State.

b. If there is any inconsistency between these terms and conditions or a Schedule, the following order of priority shall apply (in descending order) to the extent of that inconsistency: terms of the Schedule, then these terms and conditions.

c. Each indemnity is a continuing obligation separate and independent from any other obligations and survives termination of this Agreement.

d. It is not necessary for a party to incur expense or make payment before enforcing a right of indemnity conferred by this Agreement.

e. Equifax may cancel or suspend delivery of any Services in the event of any delay or non-performance due directly or indirectly to, wars, terrorism, strikes, lockouts, act of God, governmental or quasi-governmental restraint, or any other cause beyond our reasonable control.

f. Where you have provided us with an email contact address or mobile phone number, you consent to receiving electronic correspondence concerning the Services from us at the email address or mobile phone number provided, unless you notify us otherwise.

g. You acknowledge and agree that the agreement formed by these Terms and Conditions is personal to you. If you wish to obtain the Services on behalf of a related body corporate (as that term is used in the Corporations Act) you must first obtain Equifax's consent, such consent to be given in Equifax's absolute discretion and on such terms as Equifax determines. If Equifax consents you will act in your own right and as the agent of each related body corporate with respect to the obligations of each related body corporate under these Terms and Conditions and you:

   i. warrant that you have the authority to act as agent for that Related Body Corporate; and

   ii. will continue to be liable for the obligations of that related body corporate, despite the relationship of agency. Nothing in the agreement shall prevent Equifax from enforcing its rights against any related body corporate to whom Equifax provides the Services and for whom you act as agent.

# SCHEDULE - NATIONAL POLICE CHECKING SERVICES TERMS AND CONDITIONS

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 Equifax and the Client.

**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 following meanings:

**Accredited Body** means Equifax.

**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 general Terms and Conditions.

**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 which is the later of:

(a) the last day of the Initial Term; or

(b) the last day of a Renewal Term (unless the agreement with Equifax continues into a further Renewal Term),

and 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, the Client.

**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) necessary 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 15.1 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**<br>Clause 14 | The person correctly authorised by the Legal Entity Customer and occupying the position of Authorised Officer as defined in the general Terms and Conditions. |
| **3.** | **Legal Entity Customer's Address for Notices**<br>Clause 14 | As identified by the Legal Entity Customer under the general Terms and Conditions. |
| **4.** | **Accredited Body's Authorised Officer and Address for Notices**<br>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 – Workforce Solutions, the current contact details for whom are:<br>Level 15, 100 Arthur Street North Sydney, NSW 2060, Australia<br>P +61 2 9278 7862<br>fahad.sheikh@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 other purpose.

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 may contain 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 court orders;
   f. pending matters awaiting court hearing;
   g. traffic offence history ('**Disclosable Court Outcome**').

5. If this nationally coordinated criminal history check contains a Disclosable Court Outcome, the entity submitting the application is required to:
   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 police records;

(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 the application.

**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.