FACE MATCHING SERVICES

PARTICIPATION AGREEMENT

The Commonwealth of Australia as represented by the Department of Home Affairs

and

Each other **Participant**

Conformed Copy

FACE MATCHING SERVICES
PARTICIPATION AGREEMENT

Contents

PART 1	FMS LEGAL FRAMEWORK	2
1	Definitions and interpretation	2
2	Relationship with IGA and NDLFRS Hosting Agreement	18
3	Participants	19
4	FMS legal framework	21
5	Services	22
6	Document Repository	23
7	Costs and charges	24
8	Liability of Participants	26
9	Term and termination of this Agreement	29
10	Effect of withdrawal from or termination of this Agreement	30
11	Suspension and termination of Participant Access by the Hub Controller	32
12	Termination and suspension of Participant Access by Participants	36
13	Intervening Events	37
14	Intellectual property	38
15	Security classification	38
16	Privacy and Freedom of Information	39
17	Compliance Statements	42
18	Notices and contact details	44
19	Dispute Resolution	45
20	General	47
PART 2	HUB ACCESS CONDITIONS	50
21	Interoperability Hub	50
22	Security requirements and security breaches	51
23	Requesting Agency usage of the Interoperability Hub	54
24	Training Standards	57
25	Interoperability Hub Service Levels	59
26	Agency Commitments	62

27 Hub Controller's access to resolve technical issues 63

28 Provision of information to the Hub Controller and Users 63

29 Interactions with the public 64

30 Subcontracting and Coordinating Agencies 65

PART 3 DATA SOURCE ACCESS CONDITIONS 67

31 Face Matching Services 67

32 FMS Catalogue and Data Sources 67

34 Assuring and protecting Identity Information 70

35 Destruction of Identity Information 72

36 Disclosure of Identity Information to Third Parties 73

37 Safeguarding minors 73

38 Record keeping 74

39 Requesting Agency Annual Audits 74

40 Facial Recognition System 78

PART 4 PARTICIPANT ACCESS ARRANGEMENTS 80

41 Priority of Participant Access Arrangements 80

42 Entry into and Variation of Participant Access Arrangements 80

43 Pre-Agreed DHA Arrangements 82

44 Registration of Participant Access Arrangements 83

45 Commencement of a Participant Access Arrangement 83

46 Legislative basis of Participant Access Arrangements 83

47 Content requirements for Participant Access Arrangements 87

48 Requirement to provide agency list 87

49 Preservation of accrued rights 88

50 Variation 88

PART 5 SERVICE DETAILS 89

51 Service details 89

52 The Face Verification Service (FVS) 89

53 The Face Identification Service (FIS) 90

54 The One Person One Licence Service (OPOLS) 94

SIGNING PAGE 95

SCHEDULE 1 DEED OF ACCESSION 96

1 Definitions and Interpretation 97

2 New Participant 97

3 Covenant 98

4 Notices 98

5 Costs 98

6 Consideration 98

7 Representatives of the same legal entity 98

8 Governing law 99

SCHEDULE 2 NOTICE DETAILS 100

FACE MATCHING SERVICES
PARTICIPATION AGREEMENT

DATE 2019

PARTIES

1. **Commonwealth of Australia** as represented by the **Department of Home Affairs** (ABN 33 380 054 835) of 6 Chan Street, Belconnen ACT 2617 Australia (the **Commonwealth** and a **Participant**)

2. **The Crown in Right of the State of Victoria** as represented by the **Roads Corporation** (ABN 61 760 960 480) of 60 Denmark Street, Kew 3101 (**VicRoads** and a Participant)

BACKGROUND

A. On 5 October 2017, the Commonwealth of Australia, the State of New South Wales, the State of Victoria, the State of Queensland, the State of Western Australia, the State of South Australia, the State of Tasmania, the Australian Capital Territory and the Northern Territory of Australia entered into the Intergovernmental Agreement on Identity Matching Services.

B. The Intergovernmental Agreement established the framework enabling provision of the Face Matching Services under this Agreement.

C. The Commonwealth, State, and Territory Agencies enter into this Agreement to provide a legally binding framework within which they will share Identity Information via the Face Matching Services pursuant to clause 7.2 of the Intergovernmental Agreement.

D. This Agreement sets out the roles, rights and obligations of Data Holding Agencies, Requesting Agencies and the Hub Controller as the operator of the Interoperability Hub.

E. This Agreement provides the framework within which Agencies will negotiate details of data sharing arrangements, so that these arrangements meet minimum privacy and security safeguards in order to support information sharing across jurisdictions.

F. This Agreement is made in accordance with, and subject to the policies of, the Governing Body.

PART 1 FMS LEGAL FRAMEWORK

1 DEFINITIONS AND INTERPRETATION

1.1 Definitions

In this Agreement, unless the context otherwise requires:

Access Policy means, at any point in time in respect of a Service, the current version of the documented set of requirements approved by the Governing Body that a Participant must comply with in order to access the Service as published by the Framework Administrator on the Document Repository.

Additional Service means any service, that is not a Face Matching Service that uses the Interoperability Hub, that the Governing Body authorises to be offered by a Participant pursuant to this Agreement from time to time.

Agency means any agency, government sector agency, public sector agency or public sector body as defined in the *Public Service Act 1999* (Cth) or equivalent state or territory public service legislation, including any NDLFRS Contributor, law enforcement agency or relevant Commonwealth agency that is participating in or may wish to participate in any of the Services.

Agreement means this document, including any schedules, annexures, attachments and documents incorporated by reference, as amended from time to time.

Annual Audit means an annual audit conducted in accordance with clause 39 of the Data Source Access Conditions.

Annual Audit Report mean the report made by an Auditor in relation to an Annual Audit.

Auditor means a professional auditor who is appropriately qualified and experienced in the conduct of audits in relation to privacy and protection of Personal Information, information technology security, contractual compliance and organisational governance and meeting the requirements, if any, specified by the Governing Body.

Authorised Disclosure Purpose means, in relation to a Participant Access Arrangement, a purpose (if any) specified in the Participant Access Arrangement as an 'Authorised Identity Information Disclosure Purpose' for which a Requesting Agency can disclose information obtained through one or more Services to a third party.

Authorising Officer means a person appointed by a Requesting Agency as referred to in Part 5 (Service Details) of this Agreement.

Baseline Security Clearance means a "Baseline" security clearance as referred to in the *Australian Government personnel security protocol* which, as at the date of this Agreement, is available at https://www.protectivesecurity.gov.au/personnel/eligibility-and-suitability-of-personnel/Pages/default.aspx

Biographic Information means biographic Identity Information pertaining to an individual, such as their name and date of birth.

Business Day means a calendar day other than a Saturday, Sunday or public holiday on which banks are open for business in Canberra, Australia.

Client Administrator means, in relation to a Participant, any individual nominated by that Participant as a client administrator in accordance with any requirements of this Agreement or a Participant Access Arrangement. Details of the Client Administrator's role and function will be made available in the Document Repository.

Compliance Policy means, at any point in time, the current version of the compliance policy approved by the Governing Body and published by the Framework Administrator on the Document Repository.

Compliance Statement means a written statement, complying with all requirements for a "Compliance Statement" as specified in clause 17, issued by a Participant to the Hub Controller in relation to its compliance with its obligations under this Agreement.

Data Holding Agency means a Participant that contributes Identity Information used in the Services to provide Responses to Queries from Requesting Agencies. For the purposes of the NDLFRS, NDLFRS Contributors are, subject to satisfying the requirements of this Agreement and the NDLFRS Hosting Agreement and without limiting any other capacity in which they may be a Participant, Data Holding Agencies.

Data Hosting Agency means the Agency of the Commonwealth of Australia responsible for managing and operating the NDLFRS where it holds a replicated copy of Identity Information contributed by NDLFRS Contributors.

Data Source means a database of Government Identification Documentation.

Data Source Access Conditions means the terms and conditions set out in Part 3 of this Agreement.

Deed of Accession means the deed of accession in the form set out in Schedule 1 or as otherwise determined by the Governing Body.

Dispute means any dispute arising under or in connection with this Agreement.

Document Repository means the online secure portal comprising the document repository maintained by the Framework Administrator containing definitive versions of documents relating to the NFMBC, including as referred to in this Agreement.

Effective Date means, in relation to a Participant Access Arrangement, the date on which the Hub Controller notifies the relevant Participants that the Interoperability Hub has been configured to support the Participant Access Arrangement.

Executive Management means, in relation to a Participant, a person who directly supervises or is superior to the Participant's Senior Representatives.

Face Identification Service or **FIS** means the Face Matching Service of that name specified in the FMS Catalogue, which as at the date of this Agreement enables a Facial Image to be compared against multiple images held on a database of government records to establish an individual's identity.

Face Matching Service means a service in the FMS Catalogue and includes as at the date of this Agreement the Face Identification Service, the Face Verification Service and the One Person One Licence Service.

Face Verification Service or **FVS** means the Face Matching Service of that name specified in the FMS Catalogue, which as at the date of this Agreement enables a Facial Image associated with an individual to be compared against a Facial Image held on a specific government record associated with that same individual to confirm that individual's identity.

Facial Image includes digital photographs, still images captured from video, scanned photographs and other technical information related to those images (such as the time and date of capture and data capture standards used).

Facial Recognition System means a Data Holding Agency's (or, in the case of NDLFRS, the Data Hosting Agency's) system which includes face detection, quality assessment, face template creation and identification components that enable requests for verification and/or identification and provides results to the Nominated User or system that made the request.

FMS means the Face Matching Services.

FMS Catalogue means, at any point in time, the current version of the "Face Matching Services Catalogue" published by the Framework Administrator on the Document Repository detailing each Face Matching Service that is available at any point in time.

FMS Participation Framework means the framework for Services established under this Agreement as governed and as may be amended from time to time in accordance with this Agreement.

Framework Administrator means the Commonwealth, or any replacement entity appointed by the Governing Body, in its capacity as the Participant administering the FMS Participation Framework.

Function means a function of a Service as defined in the relevant Participant Access Arrangement.

Governing Body means the National Identity Security Coordination Group.

Government Identification Documentation means any document or record, whether in physical or electronic form, containing Identity Information issued by a government body or entity.

Hub Access Conditions means the terms and conditions set out in Part 2 of this Agreement.

Hub Access Documentation means, at any point in time, the current version or versions of the manual or manuals, or other documentation, for the Interoperability Hub published by the Framework Administrator on the Document Repository or otherwise made available to Participants.

Hub Access Participant means, as relevant, a Data Holding Agency or a Requesting Agency that has access to the Interoperability Hub under a Participant Access Arrangement.

Hub Controller means the Commonwealth in its capacity as the Participant controlling and administrating the Interoperability Hub (or, as relevant, any replacement entity appointed by the Governing Body).

Hub Operator means the Hub Controller or such other entity, such as a managed services provider, contracted by the Hub Controller to operate the Interoperability Hub.

Hub Production Environment means the information technology environment used to deploy the production version of the Interoperability Hub and Portal that allows Users to conduct Transactions and perform administrative functions.

Identity Information means information, or a document, relating to an individual (whether living, dead, real or fictitious) that is capable of being used (whether alone or in conjunction with other information or documents) to identify or purportedly identify the individual.

IDMS Administrator means the Identity Matching Services Administrator, being the Hub Controller's organisational unit responsible for managing the Interoperability Hub, applicable Services, and Users accessing them.

Information Security Manual means, in relation to a Participant, either:

(a) the Australian Government Information Security Manual which governs the security of government ICT systems, as produced and updated from time to time by the Australian Signals Directorate; or

(b) an alternate information security controls and guidance approved by the Framework Administrator.

Intellectual Property Rights means all intellectual property rights, whether or not such rights are registered or capable of being registered, including but not limited to, the following:

(a) patents, copyright, rights in circuit layouts, designs, trade marks (including goodwill in those marks), and domain names;

(b) any application or right to apply for registration of any of the rights referred to in paragraph (a); and

(c) all rights of a similar nature to any of the rights in paragraphs (a) and (b) which may subsist in Australia or elsewhere.

Intergovernmental Agreement means the Intergovernmental Agreement on Identity Matching Services dated 5 October 2017 between the Commonwealth of Australia, the State of New South Wales, the State of Victoria, the State of Queensland, the State of Western Australia, the State of South Australia, the State of Tasmania, the Australian Capital Territory and the Northern Territory of Australia.

Interoperability Hub means the technical system that provides a mechanism for the secure and auditable transmission of Facial Images and associated information, or other information contemplated by this Agreement, between Participants.

Intervening Event means an event that is, or a series of events that are, outside of a Participant's reasonable control and includes:

(a) force majeure, a national security event, terrorist activity, natural disasters, acts of war, riots and strikes outside that party's control;

(b) a Government policy decision; and

(c) a default of a Participant's external service providers, provided that the Participant exercises all reasonable measures to mitigate the effect of that default,

to the extent that relevant Participant is prevented from performing its responsibilities under this Agreement or any part of it.

Legally Assumed Identity means an assumed identity acquired under Part IAC of the *Crimes Act 1914* (Cth) or a corresponding assumed identity law, the *AFP Act 1979* (Cth), the *Witness Protection Act 1996* (Cth) or a corresponding witness protection program conducted by a State or Territory under a complementary witness protection law that is in force.

Legally Assumed Identity Record means a record, of any type, of a Legally Assumed Identity.

Mandatory User Requirements means the minimum requirements the User of a Service needs to comply with in order to gain and maintain access to that Service, as specified in the relevant Participant Access Arrangement.

Match means that a Facial Recognition System identifies a Facial Image (or as relevant Biographic Information) in a relevant Data Source as matching relevant Identity Information in a Query.

Match Candidate means a potential Match which has a Match Score above the Matching Threshold.

Match Function means the function of the Face Verification Service that allows a Nominated User to submit a document number, person's Facial Image and required Biographic Information to a Data Holding Agency's Data Sources to confirm whether it matches the person's Government Identification Documentation.

Match Score means a score determined by an algorithm within a Facial Recognition System that quantifies the assessed probability that a Facial Image (or as relevant Biographic Information) in a relevant Data Source matches relevant Identity Information submitted in a Query.

Matching Threshold means the Match Score that must be achieved or exceeded for a Facial Recognition System to consider a Facial Image (or, as relevant, Biographic Information) in a relevant Data Source as being a Match Candidate for relevant Identity Information in the Query.

National Identity Security Coordination Group or **NISCG** means the body which is responsible to the Ministerial Council for Police and Emergency Management for the management of the "Identity Matching Services" (as defined in the Intergovernmental Agreement).

NDLFRS means the National Driver Licence Facial Recognition Solution, being the information technology system by which details used on driver licences and other State and Territory government issued documents may be accessed via the Services.

NDLFRS Contributor means:

(a) a Road Agency; or

(b) an Agency of a State or Territory that supplies data to the NDLFRS that is not a Road Agency,

that is named as an NDLFRS Contributor under the NDLFRS Hosting Agreement.

NDLFRS Hosting Agreement means the agreement relating to the Hosting of the National Driver Licence Facial Recognition Solution between the Data Hosting Agency and each NDLFRS Contributor as amended from time to time.

NFBMC means the National Facial Biometric Matching Capability which comprises infrastructure, legislative and governance arrangements that enable the sharing and matching of Identity Information by Participants.

Nominated User means either:

(a) an individual; or

(b) an information technology system (where this is permitted by the relevant Participant Access Arrangement),

who is appointed by a Requesting Agency and given permission to submit Queries in relation to at least one Service.

Notice has the meaning given in clause 18.1.

One Person One Licence Service or **OPOLS** is a service which as at the date of this Agreement enables a Facial Image to be compared, on a

constrained one-to-many basis, to other images hosted on the NDLFRS to identify whether a licence holder or applicant holds multiple licences in the same or a different identity across participating jurisdictions.

OPOLS Reviewer means a person with a specialist identity resolution or fraud prevention function, who is trained in accordance with the training requirements of clause 24, and is responsible for reviewing the results of an OPOLS Query.

Outage means an occurrence within:

(a) the Interoperability Hub; or

(b) a Data Holding Agency's information and communications technology environment,

that results in the partial or complete cessation of one or more Services.

Participant means a party to this Agreement from time to time and any person who has become a party to this Agreement by executing the Deed of Accession in accordance with clause 3.3 and which, for the avoidance of doubt, must not be an individual.

Participant Access Arrangement means an arrangement in the form of the Participant Access Arrangement Template, formed between the Hub Controller, a Requesting Agency and one or more Data Holding Agencies (or the Hub Controller on their behalf), in relation to the Interoperability Hub and agreed Data Sources.

Participant Access Arrangement Template means the template for Participant Access Arrangements in the form maintained by the Hub Controller from time to time as approved by the Governing Body.

Personal Information has the meaning given to "personal information" in the Privacy Act. .

Permitted Purposes means, in relation to use of a Service under a Participant Access Arrangement, purposes specified as 'Permitted Purposes' in the Participant Access Arrangement or in this Agreement, but not including any purpose that is inconsistent with the requirements of this Agreement.

Portal means the user interface associated with the Interoperability Hub that allows Users to access Services or perform administrative functions.

Post-Incident Report means a report by a Participant that:

(a) contains details of an incident that affected, affects, or could affect, the Interoperability Hub or the Services (whether identified as a result of a Security Breach or otherwise);

(b) contains details of what caused, or could cause, the incident; and

(c) includes recommendations to mitigate relevant risks and minimise vulnerabilities,

and addressing such other matters as reasonably required by the Hub Controller or Framework Administrator.

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

Privacy Governance Framework and Management Standards means:

(a) the Privacy Management Framework issued by the Office of the Australian Information Commissioner; or

(b) the framework of a State or a Territory that sets out comparable standards to the one referred to in paragraph (a) above,

which must:

(c) embed a culture of privacy that enables compliance;

(d) establish robust and effective privacy practices, procedures and systems;

(e) evaluate privacy practices, procedures and systems to ensure continued effectiveness; and

(f) enhance responses to privacy issues.

Privacy Impact Assessment is a systematic assessment of the sharing of Identity Information between a Data Holding Agency and a Requesting Agency under an actual or proposed Participant Access Arrangement for the purpose of identifying any impacts on the privacy of individuals, and making recommendations for managing, minimising or eliminating any impacts identified, and that is conducted in accordance with the Office of the Australian Information Commissioner's Guide to Undertaking Privacy Impact Assessments.

Privacy Impact Assessment Expert means a person or organisation:

(a) with specialist knowledge, skills and experience in conducting Privacy Impact Assessments;

(b) with extensive knowledge of the Privacy Act and any other legislation or regulations that might apply to the handling of Identity Information and Personal Information;

(c) with an extensive understanding of privacy matters in Australia generally; and

(d) who otherwise meets any requirements specified by the Governing Body for a person to be a Privacy Impact Assessment Expert for the purposes of this Agreement.

Privacy Impact Assessment Report means a written report by the Privacy Impact Assessment Expert conducting a Privacy Impact Assessment setting out the details, findings and recommendations of the relevant Privacy Impact Assessment.

PSPF means the Protective Security Policy Framework maintained by the Attorney-General's Department, which sets out policy, guidance and better practice advice for governance, personnel, physical and information security, and which includes mandatory requirements to assist Agency heads to identify their responsibilities to manage security risks to their people, information and assets, as amended or replaced from time to time, and which as at the date of this Agreement is available at https://www.protectivesecurity.gov.au.

Query means Identity Information submitted by a Requesting Agency either through the Portal (or by a System-to-System connection (where permitted)) that is intended to be compared against the Identity Information held in a Data Source.

Relevant Capacity means the capacity in which a Participant is party to this Agreement pursuant to clause 3.1.

Representative means, in relation to a Participant, any individual nominated by that Participant as a Representative in accordance with any requirements of this Agreement or a Participant Access Arrangement.

Requesting Agency means a Participant that submits a Query to a Data Holding Agency through the Services.

Required Transaction Records means:

(a) For each NDLFRS Contributor acting in its capacity as a Requesting Agency the following records relating to Transactions:

(i) whether any Identity Information was disclosed to a third party;

(ii) how Identity Information has been retained and/or destroyed by the Requesting Agency;

(iii) date and time of each Transaction in Canberra local time;

(iv) result – e.g. success or failure;

(v) Unique User ID (username); and

(vi) Transaction Group ID.

(b) For each Data Holding Agency and each Requesting Agency, the following records relating to Transactions:

(i) whether any Identity Information was disclosed to a third party;

(ii) how Identity Information has been retained and/or destroyed by the Participant;

(iii) date and time of each Transaction in Canberra local time;

(iv) Service function accessed (eg retrieve/match/search/identify);

(v) status of Transaction (e.g. Received, with Holding Agency, returned, Delivered, removed);

(vi) state (eg Success, Failure);

(vii) Unique User ID (username); and

(viii) Transaction Group ID.

(c) For each Requesting Agency only, the following records in addition to those specified above:

(i) system name (eg Portal);

(ii) a report containing the number of instances the relevant Service was accessed by each User; and

(iii) in relation to FIS only - authorisation details (which includes the Permitted Purpose and the specific grounds that give rise to the Permitted Purpose, Supervising Officer, Authorising Officer, legislative provision, internal reference number),

along with any other records required to be maintained pursuant to the terms of any relevant Participant Access Arrangement from time to time.

Response means Identity Information or a system response sent by a Data Holding Agency via the Interoperability Hub to a Requesting Agency in response to a Query submitted by that Requesting Agency.

[redacted]

Restricted Access Request Template means the template for a Restricted Access Request in the form maintained by the Hub Controller from time to time as approved by the Governing Body.

Retrieve Function means the function of the Face Verification Service that allows a Nominated User to submit a document number and person's Biographic Information to a Data Holding Agency's Data Source(s) to retrieve either that person's Facial Image, that person's Biographic Information, or both.

Road Agency means an Agency with responsibility for driver licencing, and includes an Agency that carries out those functions as a delegate or agent of the Road Agency, or an Agency that supports the functions of an individual with statutory responsibility for driver licensing.

Role means a category of Users supported by the Interoperability Hub.

Sandpit Environment means a shared information technology environment between the Hub Controller and a Participant used for integration testing and other purposes with the Interoperability Hub by the Participants to test and validate the Participant's technical ability to access and use relevant Services.

Sanitising Agency means a Participant that has responsibility for Legally Assumed Identities, while (and only to the extent) it is exercising responsibilities under clause 34 for ensuring that each Legally Assumed Identity Record contained in Data Sources accessible through the Interoperability Hub is located and sanitised.

Search Function means the function of the FMS that allows a Nominated User to submit a person's biographic details and Facial Image to the Data

Holding Agency's Data Sources to verify that person's Government Identification Documentation held on that Data Source.

Security Accreditation Certificate means a document, in relation to a Participant, that:

(a) certifies that a Participant's relevant system has risk-based security controls that are appropriate for its specified security classification level, and

(b) is in accordance with the Information Security Manual.

Security Breach means, in relation to a Participant, any breach of security relating to that Participant that is relevant to this Agreement, including where:

(a) a Requesting Agency reasonably suspects or has evidence that a User has disclosed any or all of his or her Unique User ID Number, password or credentials to any other person without authorisation;

(b) a Requesting Agency loses, or loses control over, Identity Information; or

(c) Identity Information is not disclosed consistently with the terms of the Participant Access Arrangement under which it was provided.

Security Classification means, in relation to a piece of information, the security classification designated by the Commonwealth and/or a State or Territory of Australia, as applicable.

Security Risk Management Plan means a document, in relation to a Participant, that:

(a) identifies security risks and appropriate mitigation measures for relevant information technology systems of the Participant, in accordance with the Information Security Manual;

(b) documents the relevant risk tolerance threshold(s) of the Participant; and

(c) documents relevant processes, procedures and other measures put in place by the Participant to ensure consistent and coordinated management of relevant risks across the Participant's organisation.

Senior Client Administrator means, in relation to a Participant, any individual nominated by that Participant as a Senior Client Administrator in accordance with any requirements of this Agreement or a Participant Access Arrangement.

Senior Representative means, in relation to a Participant, any individual nominated by that Participant as a Senior Representative in accordance with any requirements of this Agreement or a Participant Access Arrangement.

Service means, as relevant:

(a) a Face Matching Service; and/or

(d) an Additional Service.

Service Levels means, in relation to a Participant Access Arrangement, the service levels (if any) specified in the Participant Access Arrangement.

Statement of Legislative Authority means a detailed explanation of the legislative provisions and other relevant information that a Participant believes establishes that:

(a) where the Participant is a Requesting Agency, that its access to a specified Data Source via the relevant Services (including its submission of Queries and receipt and use of Responses) will be lawful; or

(b) where the Participant is a Data Holding Agency, that its provision of (and, as relevant, its offer to provide) access to a specified Data Source via the relevant Services will be lawful.

Supervising Officer means a person appointed by a Requesting Agency that has a supervisory and oversight responsibilities for the Nominated User submitting the FIS queries over their use of the FIS.

Supported Response Detail means an item of information that the Interoperability Hub supports being made available in a Response to a Query if the Data Source Owner provides it to Requesting Agency in accordance with a Participant Access Arrangement.

System Security Plan means a document, in relation to a Participant, that is in accordance with the Information Security Manual.

System-to-System means, where supported by a Service, Queries submitted by a Requesting Agency to a Data Holding Agency through the Interoperability Hub via a Requesting Agency information technology system, or third-party information technology system used by the Requesting Agency.

Transaction means both a Query and Response sent through the Interoperability Hub.

UAT Environment means the system and user acceptance testing information technology environments used for end-to-end integration testing, performance, and user-acceptance testing of the Interoperability Hub, which Participants will use to undertake the tests to ensure that the Interoperability Hub meets their requirements.

Unique User ID Number means the specific number assigned to a User to access the Services.

User means, in relation to a Participant, an individual (or, where permitted by the relevant Participant Access Arrangement, an information technology system) that has been issued with a User Account authorised by the Participant and has access to a relevant Service, and includes Nominated Users, Senior Client Administrators, Client Administrators and such other user categories named in the relevant Participant Access Arrangement.

User Account means an account created in the Interoperability Hub system for the purposes of authenticating an individual (or, as relevant, an information technology system) and permissions granted to that individual or system relating to the relevant Services.

User Registry means any or all of the registers of Users of a Participant which comply with the requirements of Appendix F of the relevant Participant Access Arrangement.

User-level Access Permissions means, in relation to a Participant Access Arrangement, a subset of information a User with a particular Role can access through a relevant Service, as specified in the Participant Access Arrangement.

Variation Request Form has the meaning given in clause 42(c).

1.2 **Interpretation**

1.2.1 In this Agreement, unless the context otherwise requires:

(a) a reference to time is to the local time Canberra, Australia;

(b) headings and bold type are for convenience only and do not affect the interpretation of this Agreement;

(c) words importing the singular include the plural and vice versa;

(d) words importing a gender include any gender;

(e) other parts of speech and grammatical forms of a word or phrase defined in this Agreement have a corresponding meaning;

(f) an expression importing a natural person includes any company, partnership, joint venture, association, corporation or other body corporate;

(g) a reference to any thing (including, but not limited to, any right) includes a part of that thing (but nothing in this paragraph implies that performance of part of an obligation constitutes performance of the obligation);

(h) a reference to a Part, clause, item, paragraph or party, Schedule or Annexure is a reference to a Part, clause, item or paragraph of, or a party, Schedule or Annexure to, this Agreement;

(i) a reference to a document includes all amendments or supplements to, or replacements or novations of, that document;

(j) a reference to a party to a document includes that party's successors and permitted assigns;

(k) no provision of this Agreement will be construed adversely to a party solely on the ground that the party was responsible for the preparation of this Agreement or that provision;

(l) a reference to a body, other than a party to this Agreement (including, without limitation, an institute, association or authority), whether statutory or not:

(i) which ceases to exist; or

(ii) whose powers or functions are transferred to another body,

is a reference to the body which replaces it or which substantially succeeds to its powers or function; and

(m) a reference to a statute, ordinance, code or other law or rule includes regulations and other instruments under it and consolidation, amendments, re-enactments or replacement.

1.3 **Document takes effect as a deed**

(a) This Agreement is executed by the Participants, and takes effect, as a deed on the date specified at the front of this Agreement.

(b) References in this Agreement to "this Agreement" are to be read as references to "this deed".

1.4 **Machinery of government changes**

To the extent a Participant or another entity referred to in this Agreement is an Agency, a reference to such Participant or entity also includes, as relevant, any Agency that is (or Agencies that are), as a result of a machinery of government change, performing any relevant function or responsibility that is or was formerly performed at any relevant time by the relevant Participant or entity referred to in this Agreement.

1.5 **Several liability**

Liability of each Participant under this Agreement is several, not joint or joint and several.

2 RELATIONSHIP WITH IGA AND NDLFRS HOSTING AGREEMENT

2.1 **Relationship with the Intergovernmental Agreement**

(a) Each Participant acknowledges that the purpose of this Agreement is to implement certain Services to further the objectives of the Intergovernmental Agreement to share and match identity information, with robust privacy safeguards, to prevent identity crime and promote law enforcement, national security, road safety, community safety and service delivery outcomes.

(b) This Agreement is to be construed in a manner that is consistent with the Intergovernmental Agreement.

(c) Where there is an inconsistency between this Agreement and the Intergovernmental Agreement, the Intergovernmental Agreement prevails to the extent of that inconsistency.

2.2 **Relationship with NDLFRS Hosting Agreement**

(a) Each Participant acknowledges and agrees that:

(i) the Data Hosting Agency and the NDLFRS Contributors have entered or will enter into the NDLFRS Hosting Agreement under which, amongst other things, the Data Hosting Agency will host Data Sources provided by NDLFRS Contributors that may be used in connection with the Services;

(ii) NDLFRS Contributors that make available Data Sources that are hosted pursuant to the NDLFRS Hosting Agreement are treated under this Agreement as Data Holding Agencies; and

(iii) notwithstanding the terms of any Participant Access Arrangement, if an NDLFRS Contributor's Identity Information is withdrawn or no longer available on NDLFRS for any reason, then any Services under this Agreement that require use of such Identity Information will not be provided for the duration of that withdrawal or unavailability of the relevant Identity Information.

3 PARTICIPANTS

3.1 Roles of Participants

(a) Subject to clause 3.1(b), without limiting any other provision of this Agreement, a Participant that satisfies the criteria in the second column of the table below will be deemed to be acting in the corresponding capacity specified in column 1 of the table below for the purposes of this Agreement:

Participant Role	Applies to
Framework Administrator	Commonwealth, or any replacement entity appointed by the Governing Body, in its capacity as the Participant administering the FMS Participation Framework
Hub Controller	Commonwealth in its capacity as the Participant controlling and administrating the Interoperability Hub (or, as relevant, any replacement entity appointed by the Governing Body)
Hub Access Participant	Any Data Holding Agency or a Requesting Agency that has access to the Interoperability Hub under a Participant Access Arrangement
Data Holding Agency	A Participant that contributes Identity Information used in the Services to provide Responses to Queries from Requesting Agencies
Requesting Agency	a Participant that submits a Query to a Data Holding Agency via the Interoperability Hub under a Participant Access Arrangement
Sanitising Agency	a Participant that has responsibility for Legally Assumed Identities, while (and only to the extent) it is exercising responsibilities under clause 34 for ensuring that each

Participant Role	Applies to
	Legally Assumed Identity Record contained in Data Sources accessible through the Interoperability Hub is located and sanitised

(b) The Participants acknowledge that:

(i) a Participant may be party to this Agreement in more than one Relevant Capacity;

(ii) the Relevant Capacity in which a Participant acts may change from time to time depending on the activities they are performing under this Agreement;

(iii) new Participant capacities may be added from time to time (whether or not specified in the table in clause 3.1(a)) where permitted under this Agreement; and

(iv) a Participant which is not acting in any of the Relevant Capacities referred to in clause 3.1(a) or specified elsewhere in this Agreement will nonetheless remain a Participant for the purposes of, and be bound by, this Agreement until they cease to be a Participant in accordance with clause 9.

(c) Regardless of a Participant's Relevant Capacity, nothing in this Agreement limits a Participant's obligation to comply with any provisions of this Agreement expressed to apply to Participants generally.

3.2 Initial Commonwealth capacities

As at the date of this Agreement, the Participants acknowledge that the Commonwealth is a Participant in its capacity as the Framework Administrator and the Hub Controller.

3.3 Accession of New Participants

An entity that is not a Participant as at the date of this Agreement, will become a Participant to this Agreement when each of the following conditions is satisfied (to the extent not already satisfied):

(a) it has executed a Deed of Accession; and

(b) the Framework Administrator has notified the entity that it has accepted the executed Deed of Accession and that the entity has become a Participant.

3.4 **Binding effect on new and existing Participants**

Each Participant acknowledges that an entity that has acceded to this Agreement as a Participant by executing a Deed of Accession which has been accepted by the Framework Administrator in accordance with clause 3.3 will be bound by, and subject to the rights and obligations conferred by, this Agreement as a Participant from the date of its accession.

3.5 **General obligations**

Each Participant will, at all times:

(a) fully cooperate with each other to ensure timely progress and fulfilment of this Agreement;

(b) act reasonably and in good faith with respect to matters that relate to this Agreement;

(c) perform its obligations and responsibilities by the dates specified in this Agreement;

(d) work with each other Participant in a collaborative manner; and

(e) comply with all laws applicable to it.

4 FMS LEGAL FRAMEWORK

4.1 **Compliance with this Agreement**

Each Participant must comply with this Agreement, including as may be amended from time to time in accordance with clause 4.2.

4.2 **Modifications to this Agreement**

(a) The Participants acknowledge and agree that:

(i) the provisions of this Agreement are designed to be consistent with policies determined by, and any requirements of, the Governing Body;

(ii) this Agreement may need to be amended to reflect any changes to policies determined by, and any requirements of, the Governing Body; and

(iii) this Agreement will be reviewed by the Governing Body:

(A) within a reasonable time of passing of any legislation which enables or is otherwise relevant to the Commonwealth's participation in the NDLFRS or any matter under this Agreement; or

(B) if no such legislation referred to in clause 4.2(a)(iii)(A) has passed, within twelve months of the date this Agreement taking effect.

(b) The Framework Administrator must not notify an amendment to this Agreement pursuant to clause 4.2(c) unless the amendment has the unanimous support of the members of the Governing Body.

(c) Where the Framework Administrator proposes an amendment in accordance with clause 4.2(b), the Framework Administrator must notify each other Participant giving details of the proposed amendment.

(d) An amendment notified by the Framework Administrator will take effect on the calendar day that is three months after the amendment has been notified to all Participants (other than the Framework Administrator) in accordance with clause 4.2(c), unless the Framework Administrator subsequently notifies each Participant before expiry of the three month period that the amendments will not take effect.

(e) Participants must either:

(i) comply with any amendments that take effect in accordance with clause 4.2(d); or

(ii) withdraw from this Agreement in accordance with clause 9.4.

(f) A Participant that does not withdraw from this Agreement in accordance with clause 9.4 will be deemed to have accepted any amendments that take effect in accordance with clause 4.2(d).

(g) Each Participant will at all times act reasonably and in good faith in relation to any negotiations concerning amendments proposed to this Agreement.

5 SERVICES

5.1 Provision of Services

(a) Each Participant acknowledges that Services under this Agreement are provided subject to compliance with Part 2 (Hub Access Conditions),

Part 3 (Data Source Access Conditions), and each other relevant provision of this Agreement and each relevant Participant Access Arrangement.

(b) A change to, or the addition or removal of, any:

(i) Service;

(ii) Data Source; or

(iii) other details in the FMS Catalogue,

will not of itself constitute an amendment to this Agreement for the purposes of clause 4.2.

5.2 **Provision of Additional Services**

(a) Any Additional Service to be offered under this Agreement will be notified by the Framework Administrator to the other Participants, providing all relevant details and conditions of access and use.

(b) Any Participant wishing to participate in any Additional Services must comply with any conditions of access and use notified pursuant to clause 5.2(a).

(c) Participants participating in Additional Services acknowledge and agree that Additional Services are provided subject to each applicable provision of this Agreement in addition to any conditions of access and use notified pursuant to clause 5.2(a).

(d) The addition or removal of, or change to, any Additional Service will not constitute an amendment to this Agreement for the purposes of clause 4.2.

6 **DOCUMENT REPOSITORY**

(a) The Framework Administrator will:

(i) establish and maintain the Document Repository as an online portal accessible to Participants;

(ii) notify each Participant how they can access documents located on the Document Repository; and

(iii) make the documents published on the Document Repository accessible to each Participant.

(b) The Participants acknowledge that the Framework Administrator may make certain documents on the Document Repository available only to certain Participants, depending on access requirements and security concerns.

(c) The Framework Administrator will update documents published on the Document Repository from time to time and notify relevant Participants of this.

7 COSTS AND CHARGES

7.1 Basis upon which Participants are to be charged

Each Participant acknowledges and agrees that its use of any Services will be subject to the fees and charges agreed in the relevant Participant Access Arrangement or other written agreement between the relevant Participants.

7.2 Interoperability Hub Access costs

(a) Unless otherwise agreed with the Hub Controller, each Hub Access Participant is responsible for its own costs associated with its use of the Interoperability Hub, including technical links and System-to-System interface with the Interoperability Hub and associated costs, and for the provision of management information on the performance of the Services it provides via the Interoperability Hub.

(b) The Hub Controller may charge a Hub Access Participant, if the Hub Access Participant has a capacity as a Requesting Agency, to recover the costs of relevant Services, access to the Interoperability Hub and/or Transactions. Any such charges must be set out in the Participant Access Arrangement or other written agreement between the relevant Participants.

(c) If a charging scheme is introduced for the use of any Services, the Hub Controller will be the sole biller.

7.3 Fees charged by Participants

(a) Each Participant acknowledges that the Governing Body will conduct a review of financial arrangements in accordance with the provisions of clause 10.12 of the Intergovernmental Agreement.

(b) Participants must not charge fees until the Governing Body's review is complete and only then subject to the outcome of that review.

7.4 **Fee collection by the Hub Controller**

(a) A Hub Access Participant, where it is a Data Holding Agency, may authorise the Hub Controller to collect any charges it imposes on Requesting Agencies accessing its Data Sources under the terms of any Participant Access Arrangement, when:

(i) the Data Holding Agency Hub Access Participant requests the Hub Controller to do so in writing, and

(ii) a Requesting Agency has assented to charging arrangements with the Data Holding Agency Hub Access Participant under a Participant Access Arrangement.

(b) Any such arrangement between a Hub Access Participant and the Hub Controller must be documented in writing (in this clause, **Fee Collection Arrangement**).

(c) Any charges collected by the Hub Controller in accordance with a Fee Collection Arrangement will be remitted to the relevant Hub Access Participant in accordance with the terms of that Fee Collection Arrangement.

7.5 **Invoicing and payment**

(a) Invoices for any fees payable by a Participant must be issued in accordance with:

(i) the relevant Participant Access Arrangement;

(ii) as otherwise agreed between the relevant Participants in writing; or

(iii) in the absence of invoicing details being included in the Participant Access Arrangement or being otherwise agreed, in accordance with any requirements determined by the Hub Controller.

(b) Each Participant must pay any amounts required of them in accordance with the payment terms set out in any invoice issued to them in accordance with this Agreement.

(c) Unless otherwise agreed between the relevant Participants, all invoices must be paid within thirty calendar days. If a Participant disputes some or all of an invoice, the Participant must still pay the amount of the invoice not in dispute.

8 LIABILITY OF PARTICIPANTS

8.1 Representations or warranties

Each Participant acknowledges and agrees that to the extent permitted by law, each Participant makes no representations or warranties to another Participant except as are expressly set out in this Agreement.

8.2 Acknowledgements

(a) Each Participant acknowledges and agrees that:

(i) all Services; and

(ii) all data or information provided by the Participant in any way under or in relation to this Agreement and/or systems provided or used by the Participant to provide or support any part of a Service or any obligation of the Participant or any other matter related to this Agreement,

are provided and used on an 'as is' and 'as available' basis only.

(b) Each Participant acknowledges and agrees that:

(i) in entering into this agreement, it has not relied on any representation or warranty made by any Participant other than as set out in this Agreement;

(ii) its use of Identity Information obtained via any Service is at its sole and exclusive risk and that it is solely responsible for any decision or disclosure it makes in relation to, or in any way wholly or partially based on, such Identity Information; and

(iii) it must ensure that its functions, accountabilities, operations and process can be satisfactorily conducted and discharged at all times regardless of the availability of any Service or any information or data expected to be provided via it.

8.3 Exclusion of certain losses

To the extent permitted by law, no Participant shall have any liability to any other Participant for or in relation to:

(a) loss of profit or revenue;

(b) loss of anticipated savings of any kind;

(c) loss of bargain;

(d) pure economic loss;

(e) loss or corruption of data;

(f) loss of opportunity;

(g) loss of production;

(h) loss of goodwill; or

(i) overhead or administrative expenses.

8.4 **Limitation of liability**

(a) Subject to clause 8.4(b), the liability of a Participant under or in connection with this Agreement, including for breach of contract, or in tort (including negligence), or for any other common law or statutory cause of action arising out of the operation of this Agreement, is limited to $100,000 in aggregate, whether that liability arises during the term of, or following termination or expiry of, this Agreement, and regardless of whether a Participant has ceased to be a Participant.

(b) The limitation in clause 8.4(a) does not apply in relation to any liability arising under or in connection with this Agreement for:

(i) reckless or dishonest acts or conduct or acts or conduct done in bad faith;

(ii) fees or charges payable under this Agreement;

(iii) personal injury, including sickness or death;

(iv) loss of, or damage to, tangible property;

(v) infringement of Intellectual Property Rights;

(vi) a breach of any obligation relating to confidentiality, security, protection of Identity Information or Personal Information or privacy; or

(vii) fraudulent, unlawful or illegal acts or conduct.

8.5 **No liability when acting at direction of Governing Body or Participant**

Notwithstanding any other provision of this Agreement:

(a) to the extent permitted by law, no Participant will have any cause of action against any other Participant under or in connection with this Agreement, including for breach of contract, or in tort (including negligence), or for any other common law or statutory cause of action, where the Participant is performing an obligation under this Agreement at the direction or instruction, or pursuant to a requirement, of the Governing Body or another Participant;

(b) no Participant is obliged to act in accordance with the directions or instructions, or pursuant to a requirement, of the Governing Body or another Participant (even where a provision of this agreement requires the Participant to do so) if the Participant, acting in good faith, reasonably considers that such direction, instruction or requirement is inconsistent with this Agreement or the Participant's obligations at law (including if applicable under the PGPA Act); and

(c) a Requesting Agency has no right to give any:

(i) direction to; or

(ii) impose any requirement on; or

(iii) give any instruction to (other than an instruction specifically required by this agreement)

another Participant (and should a Requesting Agency do so, the Participating Agency has no obligation to consider or comply with the Requesting Agency's direction, requirement or instruction).

8.6 **Cooperation**

(a) The Interoperability Hub and the Services provided through it are the result of co-operative endeavour between many entities, including Hub Access Participants. Accordingly, each Hub Access Participant acknowledges that its access to, and the exchange of Identity Information via, the Interoperability Hub is on an as-is basis.

(b) The Interoperability Hub relies on the cooperation and best efforts of all Hub Access Participants. Each Participant must utilise its best efforts towards such co-operative endeavour.

(c) Each Participant must, acting in good faith, use their reasonable endeavours to assist each other Participant to the extent required for the other Participant(s) to comply with their compliance and reporting obligations under this Agreement or the NDLFRS Hosting Agreement.

9 TERM AND TERMINATION OF THIS AGREEMENT

9.1 Term of this Agreement

This Agreement commences on the date of this Agreement and terminates:

(a) in respect of a Participant where clause 9.2 or clause 9.4 applies, on the date determined in accordance with the relevant clause; or

(b) otherwise, where clause 9.3 applies, on the date determined in accordance with clause 9.3.

9.2 Termination of this Agreement for cause by the Framework Administrator

(a) The Framework Administrator must terminate this Agreement in respect of a Participant by giving written notice to that Participant:

(i) where it has been directed to do so by the Governing Body; and

(ii) if the Participant has had, or is eligible to have, its Participant Access Arrangement or access to the Interoperability Hub terminated in accordance with this Agreement.

(b) Any termination under paragraph (a) above will have effect six months after the date the notice is given, or such earlier date determined by the Governing Body (and the Participant is suspended from acting as a Requesting Agency during the period from the date of notification until the date the termination takes effect).

9.3 Termination of this Agreement by Framework Administrator

(a) The Framework Administrator may terminate this Agreement at any time by giving not less than twelve months' written notice to each other Participant.

(b) If the Framework Administrator terminates this Agreement under clause 9.3(a), the Participants will, on and from the date the termination notice is given by the Framework Administrator, work together in good faith to wind-up the arrangements contemplated by this Agreement.

9.4 **Withdrawal from this Agreement**

(a) Subject to clause 9.4(c), a Participant may by notice in writing to the Framework Administrator (or, in the case of the Framework Administrator or Hub Controller, to the other Participants) withdraw from this Agreement:

(i) if clause 4.2(e) applies, with effect from the date the amendments proposed under clause 4.2(d) are to take effect, provided the Participant gives such notice within six weeks of the date of the notice of the amendments proposed under clause 4.2(d); or

(ii) for any reason:

A. in the case of the Framework Administrator or the Hub Controller, with effect from the date that is twelve months after it gives notice in writing to the Framework Administrator that it wishes to withdraw from this Agreement; or

B. in the case of a Requesting Agency, immediately by giving notice in writing to the Framework Administrator that it wishes to withdraw from this Agreement; or

C. in the case of any other Participant, with effect from the date that is six months after it gives notice in writing to the Framework Administrator that it wishes to withdraw from this Agreement.

(b) Where a Participant withdraws from this Agreement pursuant to clause 9.4(a), this Agreement will terminate with respect to that Participant, and the Participant's rights and obligations will terminate, with effect from the date specified in accordance with clause 9.4(a).

(c) A Participant may not withdraw from this Agreement unless it has no outstanding financial obligations to another Participant (unless otherwise agreed by the affected Participant(s) in writing).

10 **EFFECT OF WITHDRAWAL FROM OR TERMINATION OF THIS AGREEMENT**

10.1 **Agreement to continue**

(a) If the Framework Administrator terminates this Agreement in respect of a Participant pursuant to clause 9.2 or a Participant withdraws from this Agreement pursuant to clause 9.4, this Agreement continues in force for

each other Participant whose participation has not been terminated or that has not withdrawn.

(b) Former Participants may not:

(i) access the Services; or

(ii) be charged for use of Services, except to the extent the charges:

A. were incurred before the relevant termination or withdrawal; or

B. are expressly payable under this Agreement following that termination.

10.2 **No claims for compensation**

A Participant that has withdrawn from this Agreement has no right to claim compensation or payment in respect of any assets, including Intellectual Property Rights or money, it has contributed in connection with this Agreement or the Services.

10.3 **Adjustment of fees following termination or withdrawal**

(a) Where a Participant ceases to be a Participant to this Agreement, whether due to termination or withdrawal, the Framework Administrator and the relevant Participant will negotiate to agree payment of a financial settlement between the Participant and the Framework Administrator.

(b) The Framework Administrator and the relevant Participant will endeavour to agree the quantum of the financial settlement on the basis that no remaining Participant to this Agreement should be subject to additional financial liabilities as a result of the relevant Participant ceasing to be a Participant to this Agreement.

(c) The relevant Participant must pay to the Framework Administrator any amount agreed under this clause 10.3. The Framework Administrator must apply any such amount to the operation and maintenance of the Interoperability Hub.

(d) The Framework Administrator and the relevant Participant must conduct the negotiations referred to in this clause 10.3 reasonably and in good faith without undue delay.

(e) Where the Framework Administrator and the relevant Participant cannot agree to the quantum and payment terms of a financial settlement under this clause 10.3, the disagreement will constitute a Dispute and clause 19 will apply.

10.4 **Preservation of accrued rights**

Termination of this Agreement, or withdrawal or termination of a Participant from this Agreement, shall not prejudice any right or liability that accrued to any Participant prior to the date of such termination or withdrawal (without limitation including liability to pay charges arising prior to or as a result of the termination or withdrawal).

10.5 **Survival**

Unless the contrary intention appears, the expiry or earlier termination of this Agreement with respect to any Participant will not affect the continued operation of any provision relating to:

(a) licensing of Intellectual Property;

(b) confidentiality;

(c) security;

(d) privacy;

(e) books and records;

(f) liability; and

(g) audit and access to information for audit purposes,

or any other provision which expressly or by implication from its nature is intended to continue.

11 **SUSPENSION AND TERMINATION OF PARTICIPANT ACCESS BY THE HUB CONTROLLER**

11.1 **Suspension of Services and Hub Access**

(a) The Hub Controller may suspend the access of any Hub Access Participant or any User of the Hub Access Participant, to the Services or the Interoperability Hub in the event that any of the following occurs:

(i) the Hub Access Participant has breached obligations under this Agreement or the Participant Access Arrangement (including, without limitation, complying with time frames and Service Levels) on more than one occasion;

(ii) a Data Holding Agency with whom the Hub Access Participant has a Participant Access Arrangement makes a written direction in accordance with clause 12.1 to the Hub Controller to suspend the Hub Access Participant; or

(iii) the Hub Controller considers on reasonable grounds that the Hub Access Participant's access to the Interoperability Hub, or the Services provided through it, has the potential to cause an adverse effect on the security, privacy, reputation, stability or integrity of the Services.

(b) In respect of any suspension under clause 11.1(a), the Hub Controller:

(i) must inform the relevant Participant of the period for which the Participant and/or its User(s) will be suspended (subject to clause 11.1(c)); and

(ii) must refer the suspension to the Governing Body for its consideration within seven calendar days.

(c) Upon any suspension under clause 11.1(a) being referred to the Governing Body, the Governing Body may (subject to clause 8.5(b)):

(i) determine to terminate the suspension, in which case the Hub Controller will reinstate the rights that have been suspended;

(ii) nominate a different period of suspension and/or vary the rights that have been suspended, in which case the Hub Controller will enforce the suspension for those rights and for that period; or

(iii) uphold the Hub Controller's original decision, in which case the Hub Controller will continue to enforce its original decision.

(d) During the period of any suspension:

(i) the Hub Controller and the relevant Hub Access Participant will work cooperatively to cease, remedy or ameliorate any activity or circumstances which lead to the suspension being imposed or continued; and

(ii) notwithstanding the suspension of some or all of its or its Users' rights pursuant to clause 11.1(a), the relevant Participant's obligations under this Agreement are not otherwise affected.

11.2 **Termination of access for cause**

(a) The Hub Controller must (subject to clause 8.5(b)), where directed to do so by the Governing Body, terminate:

(i) the Participant Access Arrangement applying between it and any Participants; or

(ii) a Hub Access Participant's, or any and all of the Hub Access Participant's Users', access to and use of:

A. one or more Data Sources;

B. one or more Services; and/or

C. the Interoperability Hub,

in the event that one or more Hub Access Termination Events occur in relation to the Hub Access Participant or its Users. Any such termination will take effect six months from the date such termination is notified to the Participant, or from such earlier date determined by the Governing Body (and the Participant is suspended from acting as a Requesting Agency during the period from the date of notification until the date the termination takes effect).

(b) Each of the following is a **Hub Access Termination Event**:

(i) one or more of the Hub Access Participant's obligations under this Agreement or a Participant Access Arrangement (including, without limitation, complying with time frames and Service Levels) are not met;

(ii) the Hub Controller previously suspended the Hub Access Participant or its User under clause 11.1; and

(iii) in the Hub Controller's opinion, the Hub Access Participant's or any of its Users' use of the Interoperability Hub or the Services:

A. causes, or may cause, severe and prolonged disruption to other users of the Services or the Interoperability Hub; or

B. results, or may result, in an unacceptable level of risk to the security, privacy, reputation, stability or integrity of the Interoperability Hub.

11.3 **Termination of Participant access on determination by Governing Body**

(a) The Hub Controller must (subject to clause 8.5(b)) otherwise terminate a Participant's or any of its Users' access to one or more Data Sources, the Services or the Interoperability Hub where directed to do so by the Governing Body.

(b) Any termination under clause 11.3(a) will take effect six months from the date such termination is notified to the relevant Participant, or from such other date determined by the Governing Body (and the Participant is suspended from acting as a Requesting Agency during period from the date of notification until the date the termination takes effect).

11.4 **Opportunity for the Hub Access Participant to respond**

(a) Where practicable, before suspension under clause 11.1 or termination under clauses 11.2 or 11.3, the Hub Controller will:

(i) provide to the Hub Access Participant no less than seven calendar days' notice of the proposed suspension or termination and the reasons for the proposed suspension or termination; and

(ii) offer the Hub Access Participant the opportunity to respond with a statement that contains evidence of how the Hub Access Participant will cease, remedy or ameliorate any activity or circumstances which enabled the suspension or termination.

(b) Where the Hub Controller provides a notice pursuant to clause 11.4(a)(i) of these Hub Access Conditions and the offer pursuant to clause 11.4(a)(ii), the Hub Access Participant must ensure any statement it wishes to make is sent to the Hub Controller as soon as practicable and in any event within seven calendar days.

(c) If the statement from the Hub Access Participant in accordance with clause 11.4(b) is not received by the Hub Controller within seven calendar days of the date of the notice given pursuant to clause 11.4(a), or the Hub Controller is not satisfied with the response received from the Hub Access Participant, the Hub Controller is entitled to proceed with suspension under clause 11.1 or termination under clauses 11.2 or 11.3.

12 TERMINATION AND SUSPENSION OF PARTICIPANT ACCESS BY PARTICIPANTS

12.1 Modification or Suspension of Access

(a) The Executive Management of a Data Holding Agency may, in relation to data held by the Data Holding Agency, by written notice direct the Hub Controller to immediately suspend or modify Interoperability Hub access rights or permissions of a Requesting Agency or any or all of its Users under a Participant Access Arrangement, as specified in the notice, if the Data Holding Agency believes on reasonable grounds stated in the notice that the suspension or modification directed is necessary:

(i) to ensure the Data Holding Agency is not, or will not be, in breach of any law;

(ii) to prevent a stated serious breach of the terms of the relevant Participant Access Arrangement or this Agreement; or

(iii) because a Dispute between the Data Holding Agency and the Requesting Agency has not been resolved to the Data Holding Agency's Executive Management's satisfaction, despite the Dispute resolution process set out in clause 19.

(b) Where the Hub Controller receives a direction under clause 12.1(a), it will act as soon as reasonably practicable to comply with the written notice and in any event, within seven calendar days of receipt of the notice.

12.2 Termination for default of the Requesting Agency

A Data Holding Agency may terminate a Participant Access Arrangement applying between it, the Hub Controller and a Requesting Agency by written notice to the Hub Controller and the Requesting Agency where:

(a) the Requesting Agency is in breach of its obligations under this Agreement or the Participant Access Arrangement; and

(b) the Requesting Agency has not remedied the breach within forty-five calendar days of being notified to do so by the Data Holding Agency.

12.3 **Termination for default of the Data Holding Agency**

A Requesting Agency may terminate a Participant Access Arrangement applying between it, the Hub Controller and a Data Holding Agency by written notice to the Hub Controller and the Data Holding Agency where:

(a) the Data Holding Agency is in breach of its obligations under this Agreement or the Participant Access Arrangement; and

(b) the Data Holding Agency has not remedied the breach within forty-five calendar days of being notified to do so by the Requesting Agency.

12.4 **Termination without cause**

(a) A Data Holding Agency who is party to a Participant Access Arrangement may terminate the relevant Participant Access Arrangement to the extent it relates to them without cause and without liability to the other parties by giving not less than six months' prior written notice to each other party to the Participant Access Arrangement.

(b) A Requesting Agency who is party to a Participant Access Arrangement may terminate the relevant Participant Access Arrangement to the extent it relates to them without cause and without liability to the other parties by giving not less than five Business Days' prior written notice to each other party to the Participant Access Arrangement.

13 **INTERVENING EVENTS**

(a) If a Participant is unable to perform an obligation under this Agreement because of an Intervening Event, then:

(i) as soon as reasonably practicable (and in any event no later than five Business Days) after the Intervening Event arises, that Participant must notify each other relevant Participant (including the Framework Administrator, if it is not the notifying Participant) of the extent to which the notifying Participant is unable to perform its obligation;

(ii) subject to clause 13(c), where a Participant complies with clause 13(a)(i), that Participant's obligation to perform those obligations will be suspended for the duration of the delay arising directly out of the Intervening Event; and

(iii) in all cases, the Participants must use their best endeavours to minimise the impact of any Intervening Event.

(b) No Participant is excused from any obligation to pay money because of an Intervening Event, despite any other provision of this Agreement.

(c) Where an Intervening Event arises due to a default of a Participant's external service providers, the Participant must have first exercised all reasonable measures to mitigate the effect of that default before its obligation to perform the relevant obligations will be suspended.

14 INTELLECTUAL PROPERTY

(a) Nothing in this Agreement affects or transfers the ownership of Intellectual Property Rights held by a Participant.

(b) Each Participant grants each other Participant a licence to use its Intellectual Property Rights to the extent required for the Participant to exercise its rights and obligations under this Agreement.

15 SECURITY CLASSIFICATION

(a) Each Participant:

(i) must not, and must not permit any of its authorised personnel or subcontractors, to access information subject to a Security Classification unless the individual concerned has a security clearance to the appropriate level and the need-to-know, and must prevent access by any such individual whose security clearance has lapsed or been revoked or who no longer requires such access;

(ii) must notify the Framework Administrator and any other relevant Participants immediately upon becoming aware of any unauthorised access to information subject to a Security Classification and the extent and nature of that access (whether incidental or accidental access, or by any of its personnel or subcontractors), and must comply with any reasonable directions of the Framework Administrator in order to rectify the Security Breach; and

(iii) must, and must ensure that its authorised personnel and subcontractors, store and handle security classified information and resources in premises and facilities that meet the minimum standards set by the Commonwealth for storage and handling of such information and/or resources, as applicable, of the relevant Security Classification level.

(b) Each Participant acknowledges that the Security Classification of:

(i) all Personal Information used in connection with the Services is "Unclassified – *Sensitive Personal*"; and

(ii) all audit data relating to the Services, Interoperability Hub or this Agreement is "Unclassified – *For Official Use Only*".

16 PRIVACY AND FREEDOM OF INFORMATION

16.1 Compliance with privacy legislation

(a) Subject to clause 16.1(d), in respect of this Agreement, the NFMBC and its use of Services:

(i) each Participant must; and

(ii) each Participant must procure that its Users,

comply with the relevant privacy legislation that applies to it by law or under this Agreement as follows:

(iii) in the case of an Australian State or Territory or an Agency of such State or Territory, Australian State or Territory privacy legislation that applies to them as an Australian State or Territory or an Agency of such State or Territory; or

(iv) in the case of an Australian State or Territory or an Agency of such State or Territory, where there is no such State or Territory privacy legislation, the Australian Privacy Principles in Schedule 1 of the Privacy Act as if such Participant or User were an APP entity that is an agency within the meaning of the Privacy Act. To the extent that the Australian Privacy Principles refer to the other Commonwealth legislation, any Australian State or Territory legislation or policies that operate to achieve substantively the same effect will apply.

(v) in the case of a Participant that is the Commonwealth of Australia or an Agency or instrumentality of the Commonwealth of Australia, the Privacy Act.

(b) In the case of an Agency of such State or Territory referred to in clause 16.1(a)(iv), APP 12 is taken not to apply in circumstances where an application for access to personal information has been made to the Agency pursuant to the applicable Australian State or Territory Freedom of Information legislation.

(c) Each Participant:

(i) must; and

(ii) must procure that its Users,

comply with any additional privacy obligations notified to them by the Framework Administrator, where required by the Governing Body.

(d) Subject to the operation of applicable law, each of the following entities is exempt from the requirement to comply with the Australian Privacy Principles in Schedule 1 of the Privacy Act:

(i) the Corruption and Crime Commission of Western Australia;

(ii) the Independent Commissioner against Corruption of South Australia;

(iii) Australian Criminal Intelligence Commission;

(iv) Australian Commission for Law Enforcement Integrity;

(v) Australian Security Intelligence Organisation; and

(vi) Australian Secret Intelligence Service.

16.2 **Correction of and access to Personal Information**

(a) Each Data Holding Agency is responsible for addressing any requests (for access, modification or otherwise) from an individual made under applicable privacy or freedom of information legislation in respect of any of the individual's Personal Information held in a Data Source offered by that Data Holding Agency.

(b) Each Data Holding Agency must take reasonable steps to:

(i) correct Personal Information comprised in its Data Sources to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading; and

(ii) give an individual access to their Personal Information comprised in any of its Data Sources where required under applicable privacy or freedom of information legislation.

(c) Clause 16.2(b)(i) applies where, as appropriate and without limiting that clause:

(i) the Data Holding Agency is satisfied that the Personal Information is inaccurate, out-of-date, incomplete, irrelevant or misleading, having regard to a purpose for which it is held; or

(ii) the individual to whom the Personal Information relates requests access to, or the correction of, the Personal Information whether:

A. the request is made by the individual directly to the Data Holding Agency; or

B. the request is made by the individual to another Participant and the Participant refers the request to an NDLFRS Contributor.

(d) Where a Participant becomes aware that Personal Information held by another Participant (other than itself) is inaccurate, out-of-date, incomplete, irrelevant or misleading, having regard to a purpose for which it is held, the Participant must take reasonable steps to notify the other Participant of the deficiency, to enable the Participant to take reasonable steps to correct that Personal Information.

16.3 **Freedom of information**

(a) In respect of this Agreement, the NFMBC and its use of Services, each Participant must, and it is intended that each User under a Participant Access Arrangement must, comply with any freedom of information legislation that is applicable to it in its jurisdiction.

(b) Each Participant:

(i) acknowledges that freedom of information requests relating to or otherwise connected this Agreement, the NFMBC, the Services and/or the Interoperability Hub are of a cross-jurisdictional nature; and

(ii) agrees to take reasonable steps to collaborate in responding to freedom of information requests received by Participants, including Participants in other jurisdictions.

16.4 **Requirement to develop a privacy management framework**

Each Participant, other than to the extent to which it acts as a Sanitising Agency:

(a) must develop and/or amend, as necessary, its Privacy Governance Framework and Management Standards to ensure they are adequate

and reflect the management of the flow of information through the Services it uses or proposes to use under this Agreement; and

(b) must provide to the Hub Controller a copy of its Privacy Governance Framework and Management Standards promptly upon request by the Hub Controller.

16.5 **Survival**

This clause 16 survives termination of this Agreement for any reason.

17 **COMPLIANCE STATEMENTS**

17.1 **Requirement for Compliance Statements**

(a) Each Participant acknowledges the importance of ensuring compliance with requirements to maintain and enhance the integrity of the Interoperability Hub.

(b) Subject to clause 17.1(f), each year each Participant must complete and submit to the Hub Controller for consideration by the Governing Body a Compliance Statement that, at a minimum:

(i) documents any breaches of each Participant Access Arrangement to which it is party;

(ii) if the Participant is a Data Holding Agency, documents any breaches of any applicable Service Levels;

(iii) is signed off by the Participant's Senior Representative;

(iv) confirms that its use of and/or service provision to the Interoperability Hub being in accordance with:

A. the Participant Access Arrangement; and

B. this Agreement;

(v) confirms that its technical, privacy and security safeguards are working effectively to protect the integrity of the Interoperability Hub and the Services (or any deficiencies in relation to the same); and

(vi) provides details of recommendations that may be made to it in relation to its use of and/or service provision to the Interoperability Hub to the Governing Body as information becomes available. This

information may come from reports to the Participant from areas such as:

A. audits of the Office of the Australian Information Commissioner;

B. review bodies of states/territories; and

C. other audits or reviews.

(c) Each Participant must maintain records or other evidence that supports the statements made in a Compliance Statement. The Hub Controller may request copies of such records or evidence.

(d) Each Compliance Statement must cover:

(i) a twelve month period beginning on 1 February of the previous year and ending one year later; and

(ii) where a Participant has only provided or used a Service for part of a year, the relevant portion of the year referred to in clause 17.1(d)(ii) above for which the Service was provided or used.

(e) Each Participant must submit the Compliance Statement by 31 March (or the first Business Day after that calendar day) each calendar year.

(f) Each Participant acknowledges and agrees that:

(i) the Data Hosting Agency under the NDLFRS Hosting Agreement is responsible for preparing and obtaining approval prior to submitting Compliance Statements on behalf of NDLFRS Contributors acting in their capacity under this Agreement as Data Holding Agencies;

(ii) NDLFRS Contributors acting in their capacity of Data Holding Agencies need not otherwise comply with the requirements of this clause 17.1; and

(iii) where a Compliance Statement prepared by or on behalf of an NDLFRS Contributor does not include all required information, the Compliance Statement must include a statement setting out the information that has been omitted and the reason it has been omitted.

17.2 **Access to information**

Each Participant must provide to each other Participant such information as reasonably requested by that Participant which is necessary for it to complete its Compliance Statement.

18 **NOTICES AND CONTACT DETAILS**

18.1 **Notices**

(a) As at the date of this Agreement, the notice details for each Participant are set out in Schedule 2 to this Agreement. A Participant may update its notice details by providing notice of its new details to each other Participant.

(b) Any notices, statements, reports or information to be given to a Participant (**Notices**), including any Notice relating to a Dispute, must be given in accordance with this clause.

(c) Notices:

(i) must be in writing and signed by a person duly authorised by the sender

(ii) must be addressed and delivered to the intended recipient by hand, by prepaid post, by fax or by email at the address, fax number or email address last notified by the intended recipient to the sender. The preferred mode of contact is email; and

(iii) are taken to be given and made:

A. in the case of hand delivery, when delivered

B. in the case of delivery by post, three Business Days after the date of posting (if posted to an address in the same country) or seven Business Days after the date of posting (if posted to an address in another country)

C. in the case of a fax, on the calendar day and at the time it is sent, provided that the sender's facsimile machine issues a report confirming the transmission of the number of pages in the Notice; and

D. in the case of an email, on the calendar day and at the time that the email was sent unless the sender received an automated notice that the email was not delivered or an

automated notice that the recipient did not have access to their emails.

(d) Unless otherwise specified, a Participant must give a Notice:

(i) where the notification is to occur after an event, within three Business Days after that event, or

(ii) where the notification is to occur before an event, five Business Days before an event occurring, as appropriate.

(e) This clause does not limit the way in which a notice can be deemed to be served under any law.

18.2 **User contact details**

Each Participant must provide the contact details of its Users to the Hub Controller and each other Participant who needs to know such contact details from time to time.

18.3 **Incident notification**

In addition to the contact information set out in Schedule 2 of this Agreement, each Participant must provide their relevant contact details and their operating hours to each other Participant in order to report, and must promptly report to the Hub Controller:

(a) Outages relating to the Interoperability Hub;

(b) general incidents relating to the Interoperability Hub;

(c) critical incidents relating to the Interoperability Hub; and

(d) urgent / emergency requests.

19 **DISPUTE RESOLUTION**

19.1 **Best efforts to resolve disputes at the Senior Representative level**

If any Dispute arises, the Participants involved agree to at first instance use their best efforts to resolve the Dispute by discussion and amicable settlement, as facilitated by their respective Senior Representatives.

19.2 **Referral of Disputes to Executive Management**

(a) Where a Participant involved in a Dispute is not satisfied that further discussions under clause 19.1 will resolve the Dispute within a time

frame acceptable to it, the Participant may, by written notice to the other Participants involved in the Dispute, refer the Dispute for resolution by the Executive Management of each relevant Participant. The notice given by the Participant must:

(i) nominate a member of its Executive Management with authority to settle the Dispute to represent the Participant in discussions; and

(ii) provide a written summary of the facts and issues that the Participant has identified as relevant to the Dispute, and any other information that will assist in discussions to resolve the Dispute.

(b) Within seven calendar days of a Participant receiving a notice pursuant to clause 19.2(a), the recipient must, by written notice to the other relevant Participant(s) involved in the Dispute:

(i) nominate a member of its Executive Management with authority to settle the Dispute to represent the Participant in discussions; and

(ii) provide a written response to the statement it received under clause 19.2(a)(ii).

19.3 **Reasonable efforts to resolve Disputes at the Executive Management level**

Each relevant Participant will procure that the members of the Executive Management nominated pursuant to clause 19.2 will make all reasonable efforts to engage in and progress discussions and endeavour in good faith to resolve the Dispute.

19.4 **Continued compliance**

Each Participant must at all times continue to comply with their obligations pursuant to this Agreement despite the existence of any Dispute.

19.5 **No limitations**

Nothing in this clause 19 prevents:

(a) where that action is otherwise permitted by this Agreement:

(i) suspension of access to the Interoperability Hub or any Data Source;

(ii) variation to the Hub Access Conditions or the Data Source Access Conditions or any other provision of this Agreement, in accordance with the provisions of this Agreement; or

(iii) full or partial termination of a Participant Access Arrangement or other arrangement under this Agreement; or

(b) a Participant seeking an injunction or other interlocutory relief at any time.

20 GENERAL

20.1 Disclosure

Nothing in this Agreement limits any obligations of the Commonwealth, the Framework Administrator or the Hub Controller to publish information relating to usage of the Services, provided that the Commonwealth, the Framework Administrator and the Hub Controller will, where reasonably practical and appropriate, consult with relevant Participants before publication of such information.

20.2 Costs

Unless expressly provided otherwise, each Participant is responsible for bearing its own costs in connection with the preparation and performance of this Agreement.

20.3 Representatives of the same legal entity

(a) To the extent that a Participant is the same legal entity as one or more other Participants, the provisions of this Agreement, as between those Participants representing the same legal entity, take effect as a memorandum of understanding and are not legally binding.

(b) This clause 20.3 does not affect the binding nature of this Agreement as between Participants that are distinct legal entities.

20.4 Governing law

(a) This Agreement is governed by the laws in force in the Australian Capital Territory.

(b) Each Participant irrevocably submits to the non-exclusive jurisdiction of the courts of the Australian Capital Territory.

20.5 **Prohibition and enforceability, severability**

(a) Each provision contained in each clause of this Agreement is enforceable independently of each other provision of this Agreement.

(b) The validity and enforceability of any provision of this Agreement will not be affected by the invalidity or unenforceability of any other provision.

(c) Any provision of, or the application of any provision of, this Agreement which is prohibited in any jurisdiction is, in that jurisdiction, ineffective only to the extent of that prohibition.

(d) If any provision of this Agreement is or becomes void or unenforceable, that part is to be severed from this Agreement with the intention that the balance of this Agreement is to remain in full force and effect.

20.6 **Waivers**

(a) Waiver of any right arising from a breach of this Agreement or arising upon default under this Agreement must be in writing and signed by each Participant granting the waiver.

(b) A failure or delay in exercise, or partial exercise, of a right arising from a breach of this Agreement does not result in a waiver of that right.

(c) A Participant is not entitled to rely on a delay in the exercise or non-exercise of a right arising from a breach of this Agreement or on a default under this Agreement as constituting a waiver of that right.

(d) A Participant may not rely on any conduct of any other Participant as a defence to exercise of a right by that other Participant.

(e) This clause 20.6 may not itself be waived except by writing.

20.7 **Assignment**

Rights arising out of or under this Agreement are not assignable by a Participant without the prior written consent of each other Participant.

20.8 **Further assurances**

Each Participant must do all things and execute all further documents necessary to give full effect to this Agreement.

20.9 **Entire agreement**

This Agreement and the Intergovernmental Agreement supersede all previous agreements in respect of their subject matter and embody the entire agreement between the Participants.

20.10 **Counterparts**

This Agreement may be executed in any number of counterparts. All counterparts, taken together, constitute one instrument.

20.11 **Variation**

Except as otherwise expressly provided for in this Agreement (including clause 4.2), a variation of any term of this Agreement must be in writing and signed by the Participants.

PART 2 HUB ACCESS CONDITIONS

21 INTEROPERABILITY HUB

21.1 Overview

(a) The Interoperability Hub is the technical system that provides, amongst other things, a mechanism for the secure and auditable transmission of Facial Images and associated information between agencies or entities participating in the NFBMC.

(b) The Interoperability Hub will be operated, maintained and controlled by the Hub Controller.

(c) Access by a Participant other than the Hub Controller (including any Data Holding Agency and any Requesting Agency) to the Interoperability Hub is conditional upon the Participant having entered into a Participant Access Arrangement in accordance with Part 4 of this Agreement.

(d) Each Participant Access Arrangement will govern the terms of the relevant Participant's use of the Interoperability Hub in relation to the Services provided for in that Participant Access Arrangement.

21.2 Access to the Interoperability Hub

(a) From the Effective Date of a Participant Access Arrangement, the Hub Controller will permit the relevant Hub Access Participants to test their connection to the Portal and the Interoperability Hub in the Sandpit Environment.

(b) The Hub Controller will allow a Hub Access Participant to have access to the Hub Production Environment or UAT Environment if the Hub Controller and the Governing Body are satisfied that:

(i) all applicable requirements of the Access Policies for the relevant Services have been met by the Hub Access Participant; and

(ii) the Hub Access Participant has met its responsibilities under its Participant Access Arrangement.

(c) The Hub Controller may prevent access by a Hub Access Participant to the Hub Production Environment or UAT Environment if the Hub

Controller and Governing Body cease to be satisfied that the requirements of clauses 21.2(b)(i) or 21.2(b)(ii) are being met.

(d) The Hub Controller will not allow a Requesting Agency to access Data Sources held by a Data Holding Agency through the Hub Production Environment until the Requesting Agency has entered into a Participant Access Arrangement with the Data Holding Agency.

22 SECURITY REQUIREMENTS AND SECURITY BREACHES

22.1 Hub Access Participant Security accreditation

(a) Each Hub Access Participant that intends to connect to the Interoperability Hub using a system-to-system connection must, before connecting any of its information technology systems to the Interoperability Hub:

(i) prepare and implement a Security Risk Management Plan; and

(ii) either:

A. prepare and implement a System Security Plan; or

B. receive a Security Accreditation Certificate and

provide a copy of it to the Hub Controller.

(b) A Hub Access Participant that intends to access the Interoperability Hub through the Portal only must conduct a security risk assessment in a format approved by their internal information technology security adviser (or equivalent), a copy of which must be provided to the Hub Controller for comment.

(c) The Hub Controller will notify the relevant Hub Access Participant within a reasonable time whether, acting reasonably, it has any comments on the documents referred to in clauses 22.1(a)(i), 22.1(a)(ii)A and/or 22.1(b) (the **Security Documentation**), as applicable, or whether it accepts them as provided.

(d) If the Hub Controller accepts the Security Documentation, as applicable, the Hub Controller will notify the relevant Hub Access Participant that it may connect its information technology systems to the Interoperability Hub and/or connect through the Portal, as the case may be.

(e) If the Hub Controller has comments on the Security Documentation, as applicable, the Hub Controller will request the relevant Hub Access Participant to resubmit the relevant document(s) having regard to the comments made by the Hub Controller until such time as they are accepted by the Hub Controller, in which case clause 22.1(d) will apply.

22.2 **Hub Controller security accreditation**

(a) The Hub Controller must obtain a current Security Accreditation Certificate in accordance with any requirements of the PSPF.

(b) The Hub Controller must provide a copy of:

(i) its Security Accreditation Certificate to a Participant as soon as reasonably practicable after receiving a written request from the Participant to do so; and

(ii) any new or updated Security Accreditation Certificate to each Participant within 14 days of it being issued or updated.

22.3 **Security breaches**

Each Participant, other than Sanitising Agencies:

(a) that becomes aware of or has reasonable grounds to suspect:

(i) a Security Breach; or

(ii) a security vulnerability of any kind (whether or not a Security Breach has been involved),

in relation to any of its information technology systems that are connected to the Interoperability Hub that affects, or could affect, the NFBMC or any of the Services, must:

(iii) take immediate action to rectify the Security Breach or other security vulnerability;

(iv) if the Participant is the Hub Controller, notify each other directly affected Participant as soon as reasonably possible and in any event within 12 hours; and

(v) if the Participant is not the Hub Controller, notify the Hub Controller and any other directly affected Participant within 48 hours;

(b) must complete a Post-Incident Report within two weeks of the relevant Security Breach;

(c) must send the Post-Incident Report for a Security Breach and any recommendations to:

(i) each other directly affected Participant (if any);

(ii) if the Participant is not the Hub Controller, the Hub Controller; and

(iii) the Office of the Australian Information Commissioner, where required under the Privacy Act (provided no exceptions apply and the Participant has provided notice under clause 22.3(d)(ii)), or any other relevant Privacy Commissioner, ombudsman or government oversight body where required under applicable legislation;

(d) agrees that, where a Participant seeks to notify affected individuals or publish a statement for affected individuals about a Security Breach, whether bound to do so under the Privacy Act or otherwise:

(i) unless agreed otherwise by relevant Participants, the Participant who is most directly related to the affected individuals will undertake such notification or publication;

(ii) a Participant providing a notice or publishing a statement under clause 22.3(c)(iii) will provide reasonable notice of its intention to do so to each other affected Participant (if any); and

(iii) each Participant will provide all reasonable assistance to each other Participant to enable compliance with their respective obligations under applicable legislation in relation to notifying Security Breaches or suspected Security Breaches.

22.4 **Remediation**

(a) Within one week after a Participant conducts a Post-Incident Report under clause 22.3(b), the Participant must submit a remediation plan to:

(i) If the Participant is the Hub Controller, to each other affected Participant (if any); or

(ii) if the Participant is not the Hub Controller, the Hub Controller,

which includes timeframes for implementing recommendations of the Post-Incident Report.

(b) The Participant must use its best endeavours to remedy issues in conformity with the Information Technology Infrastructure Library public framework.

(c) The Participant is responsible for all costs associated with carrying out their remediation plan.

23 REQUESTING AGENCY USAGE OF THE INTEROPERABILITY HUB

23.1 Requesting Agency must ensure all use is appropriate

A Requesting Agency Hub Access Participant must ensure that all access to and use of

(a) any Services;

(b) the Interoperability Hub; and

(c) Data Sources,

by it is (and can be demonstrated to be) in strict accordance with this Agreement (without limitation including its Participant Access Arrangements).

23.2 Requesting Agency Client Administrators

(a) A Requesting Agency Hub Access Participant must at all times ensure that it has at least:

(i) 2 Client Administrators; and

(ii) if required for the relevant Service, 1 Senior Client Administrator,

for each Service to which the Requesting Agency has access.

(b) A Requesting Agency Hub Access Participant may appoint additional:

(i) Client Administrators; and/or

(ii) Senior Client Administrators,

subject to:

(iii) there being a reasonable need for the person to be appointed in order to perform their duties; and

(iv) any limits advised by the Hub Controller.

(c) A Requesting Agency Hub Access Participant must ensure that its:

(i) Client Administrators; and

(ii) Senior Client Administrators,

at all times meet all Mandatory User Requirements for each such Role.

(d) A Requesting Agency Hub Access Participant must ensure that current details of each Senior Client Administrator are at all times registered with the Hub Controller. Senior Client Administrators may not be recognised by the Hub Controller unless their current details are registered with the Hub Controller.

(e) In addition to any other accountability or obligation, each Requesting Agency Hub Access Participant will procure that each Senior Client Administrator (if any) appointed by it for a Service is responsible for ensuring that the Requesting Agency's Client Administrator/s for that Service comply with their obligations.

(f) Participants acknowledge that Client Administrators are responsible for:

(i) ensuring Nominated Users, Supervising Officers and Authorising Officers of the Services meet the appointment criteria set out in this Agreement and relevant Participant Access Arrangements;

(ii) creating User Accounts and changing User roles as set out in relevant Participant Access Arrangements;

(iii) re-authorising Nominated Users, Supervising Officers and Authorising Officers and ensuring they meet the User requirements; and

(iv) removing the access of Nominated Users, Supervising Officers and Authorising Officers to the Services as soon as possible upon request from the Hub Controller to remove access.

23.3 **Creating User Accounts**

(a) User Accounts and User-level Access Permissions may be created, amended and/or terminated in accordance with:

(i) the provisions of the Hub Access Documentation; and

(ii) the systems established by the Interoperability Hub.

(b) Each Participant must ensure that at all times:

(i) its Users satisfy all applicable Mandatory User Requirements; and

(ii) the Roles and User-Level Access Permissions granted to its Users are commensurate with the requirements of their Users' functions and activities.

23.4 **Queries must be submitted by Nominated Users only**

Each Requesting Agency Hub Access Participant must ensure that only its Nominated Users submit Queries to, or have access to, the relevant Data Source.

23.5 **Management of Users**

(a) A Requesting Agency Hub Access Participant must establish and maintain a User Registry. The User Registry must include such details as required by the Hub Controller from time to time.

(b) The Hub Controller, or the Data Holding Agency under any Participant Access Arrangement that a Requesting Agency has entered into, may request a copy of this User Registry.

23.6 **Responsibility for User non-compliance**

(a) Participants are responsible for the acts of their Users at all times.

(b) Where a User fails to comply with a requirement of this Agreement, the Participant that appointed that User is responsible for rectifying that non-compliance in accordance with the Compliance Policy.

(c) Participants must within a reasonable timeframe inform the Hub Controller of any such non-compliance, the steps take to address the non-compliance, and on resolution of such non-compliance.

(d) This clause 23.6 does not limit the operation of clause 23.7.

23.7 **Termination of Users**

(a) If at any time any of the Mandatory User Requirements for appointing a User are no longer satisfied, the Hub Access Participant must, and the Hub Controller may, terminate that User's access to the Services by:

(i) removing the User from the User Registry; and

(ii) removing the User's access to the Services as soon as practicable.

(b) Without limiting a Hub Access Participant's obligations under clause 23.7(a), a Hub Access Participant may request the Hub Controller by written notice to remove the User's access to relevant Services on behalf of the Hub Access Participant if at any time any of the Mandatory User Requirements for appointing a User are no longer satisfied. Where the Hub Controller receives such a notice, the Hub Controller will use its reasonable endeavours to remove the User's access to the relevant Services as soon as possible.

24 TRAINING STANDARDS

24.1 Privacy and awareness training

Requesting Agencies must provide training for Nominated Users and Authorising Officers in security awareness and privacy obligations (which may already occur as part of their ongoing employment).

24.2 Interoperability Hub Portal training

(a) All Nominated Users and, in the case of the FIS, Authorising Officers also, must undergo training on how to use the Interoperability Hub Portal interface, including how to interpret the results of a Query.

(b) The Hub Controller will make available to Participants e-learning materials relating to the Interoperability Hub Portal.

24.3 Facial recognition and image comparison training

(a) Participants must ensure that all of their:

(i) FVS Nominated Users that receive a Facial Image in a Response to a Query;

(ii) FIS Nominated Users; and

(iii) OPOLS Reviewers,

satisfy the training requirements set out in this clause 24.3.

(b) In relation to FVS:

(i) FVS Users that receive a Facial Image in a Response to a Query must undergo facial recognition and image comparison training.

(ii) Such training must consist of either:

A. the relevant training package supplied by the Hub Controller to assist Participants to meet this requirement; or

B. where approved by the Hub Controller in advance, alternative training arrangements to provide FVS Users with a similar or greater level of knowledge.

(iii) The Hub Controller must not grant approval under clause 24.3(b)(ii)B without first consulting Data Holding Agencies.

(c) In relation to FIS:

(i) FIS Users must undergo facial recognition and image comparison training.

(ii) Such training must consist of either:

A. the relevant training package supplied by the Hub Controller to assist Participants to meet this requirement; or

B. where approved by the Hub Controller in advance, alternative training arrangements to provide FIS Users with a similar or greater level of knowledge.

(iii) The Hub Controller must not grant approval under clause 24.3(c)(ii)B without first consulting Data Holding Agencies.

(d) In relation to OPOLS:

(i) OPOLS Reviewers that receive a Facial Image in a Response to a Query must undergo facial recognition and image comparison training.

(ii) Such training must consist of either:

A. the relevant training package supplied by the Hub Controller to assist Participants to meet this requirement; or

B. where approved by the Hub Controller in advance, alternative training arrangements to provide OPOLS Reviewers with a similar or greater level of knowledge.

(iii) The Hub Controller must not grant approval under clause 24.3(d)(ii)B without first consulting Data Holding Agencies.

24.4 **Waiver of training requirements**

(a) Where Nominated Users and OPOLS Reviewers can demonstrate to the reasonable satisfaction of the Hub Controller that they have sufficient skills and experience in facial recognition and image comparison to use the Services, the Hub Controller may waive some or all of the training requirements set out in this clause 24.

(b) Before providing such waiver, the Hub Controller must consult Data Holding Agencies.

24.5 **Additional training**

Each Hub Access Participant must ensure its Users undergo training in accordance with this Agreement and any further requirements as specified in any relevant Participant Access Arrangement the Hub Access Participant has entered into.

25 **INTEROPERABILITY HUB SERVICE LEVELS**

25.1 **Provision of the Services and Availability**

(a) The Hub Controller will at all times during the term of this agreement provide the Services in accordance with the Service Levels set out in each Participant's Participant Access Arrangement.

(b) The Hub Controller:

(i) will provide the Services in a proper, timely and efficient manner in accordance with the requirements of this agreement;

(ii) will act in good faith; and

(iii) unless otherwise agreed between the Participants, and subject to the outcomes of the fee review referred to in clause 7.3 of this Agreement, will provide any and all equipment, software, network hardware and other resources necessary for the operation of the Interoperability Hub.

25.2 **Response times**

(a) The Hub Controller will use its best endeavours to ensure that Transactions are generally processed by the Interoperability Hub within 10 seconds.

(b) The Hub Controller will use its best endeavours to process the Hub Access Participant's Queries and/or Responses.

25.3 **Priority of requests**

(a) The Hub Controller will use its best endeavours to ensure that Queries are actioned by the Interoperability Hub according to their priority.

(b) Each Participant acknowledges that the default priority of all Transactions is "intermediate".

(c) The Hub Controller may alter the order in which Transactions are resolved should a set of transactions be deemed high priority by the Hub Controller.

(d) If an event occurs, the Hub Controller may prioritise any Queries or Responses that may assist in resolving that event.

25.4 **Queued Queries or Responses**

(a) The Hub Controller may queue Responses to, or Queries from, a Requesting Agency when:

(i) the Requesting Agency exceeds the Transaction quota, or estimated peak Transaction volume, as provided for in a Participant Access Arrangement the Requesting Agency has entered into, provided that the Hub Controller first notifies the Requesting Agency that the Transaction quota has been exceeded; or

(ii) an Intervening Event or other event is occurring.

(b) The Hub Controller may report the impact of the Hub Access Participant's Queries on the Interoperability Hub to the Governing Body when prioritising requests or taking action under this clause 25.4.

25.5 **Access information**

(a) The Hub Controller will provide each Hub Access Participant with information, specifications, documentation and data (including the Hub Access Documentation) necessary for the Hub Access Participant to utilise the Services, which includes:

(i) guidance for Users on how to use the Interoperability Hub through the Portal and System-to-System interfaces (user guide);

(ii) any externally configurable values set across the NFBMC for Participants by Data Holding Agency administrators; and

(iii) documentation for the Interoperability Hub and Services.

(b) The Hub Controller will provide the documents referred to in clause 25.5(a) (and any updates to them) on the Document Repository or such other location notified by the Hub Controller or Framework Administrator, in relation to either a single Data Source or multiple Data Sources.

(c) All information referred to in clause 25.5(a) will be at a *For Official Use Only* classification or lower.

25.6 **Notifications by the Hub Controller**

(a) The Hub Controller will notify each Hub Access Participant of:[1]

(i) any events or circumstances that are likely to result in a disruption to the Services, or any scheduled outages;

(ii) updates to any documents in clause 25.5(a);

(iii) any Security Breach or other security vulnerability other Participants have notified the Hub Controller of (whether under clause 22, a Participant Access Arrangement or otherwise) if the Hub Controller considers the Security Breach or other security vulnerability has, or may adversely affect, the security, privacy, reputation, stability or integrity of the Hub Access Participant or its information technology systems, and

(iv) where the Hub Access Participant is a Requesting Agency, any access or disclosures the IDMS Administrator has made under clause 27.

(b) The Hub Controller will use its best efforts to ensure that the Services meet the Service Level standards (if any).

25.7 **Hub privacy assessments**

The Hub Controller will ensure that an entity independent of the Hub Controller conducts a privacy assessment in relation to the Interoperability Hub annually.

[1] Participants are to note that should a Participant cause one of the events referred to in clause 25.6(a)(i) or clause 25.6(a)(iii), this could result in suspension under clause 11.

26 AGENCY COMMITMENTS

26.1 Data Holding Agency Commitments

(a) Each Data Holding Agency Hub Access Participant that is not an NDLFRS Contributor must:

(i) comply with:

A. any Service Levels; and

B. all Participant Access Arrangements with Requesting Agencies;

(ii) participate in (and fully support) at least one disaster recovery exercise related to the Interoperability Hub per year as required by the Hub Controller; and

(b) Each Data Holding Agency Hub Access Participant must provide all cooperation, assistance and information reasonably required by a Requesting Agency for it to comply with its audit obligations under this Agreement (except, in the case of an NDLFRS Contributor, to the extent the NDLFRS Contributor does not hold the information requested by the Requesting Agency).

(c) Each Data Holding Agency Hub Access Participant:

(i) will provide the Services in a proper, timely and efficient manner in accordance with the requirements of this agreement; and

(ii) will act in good faith.

26.2 Requesting Agency Commitments

(a) A Requesting Agency Hub Access Participant acknowledges that the Hub Controller will only transmit Identity Information in Response to a Query that is specified in the User-Level Access Permissions determined by the relevant Data Holding Agency.

(b) A Requesting Agency Hub Access Participant must use its best efforts to notify the Hub Controller of the expected number of its Queries and the date and time of any Queries where it anticipates a surge or significant increase in short-term volume of its Queries above its normal usage pattern.

27 HUB CONTROLLER'S ACCESS TO RESOLVE TECHNICAL ISSUES

(a) Each Hub Access Participant acknowledges that to enable the provision of the Services and access to the Interoperability Hub, the IDMS Administrators will have all of the privileges and access granted to any Client Administrators under any Participant Access Arrangement the Hub Access Participant enters into.

(b) For the purposes of resolving technical issues with the Services or access to the Interoperability Hub (including but not limited to triaging technical faults or reproducing technical faults) each Data Holding Agency Hub Access Participant hereby consents to IDMS Administrators running Transactions against its Data Sources and to disclosing Queries, Responses or Transactions to the Hub Operator or relevant Participants.

(c) Any action taken under clause 27(b) may only occur in the following circumstances:

(i) the IDMS Administrators have been specifically requested to resolve a technical issue with access to the Interoperability Hub or the Services by a Hub Access Participant; and

(ii) the operations which the IDMS Administrators performs under clause 27(b) use either:

A. test data agreed with the Hub Access Participant;

B. Identity Information, where the individual to whom it relates has consented in writing to the operation to be performed under subclause 27(b); and/or

C. Identity Information, where the IDMS Administrator has another lawful basis to perform the operation; and

(iii) the relevant disclosure is made on a *For Official Use Only* basis.

28 PROVISION OF INFORMATION TO THE HUB CONTROLLER AND USERS

(a) A Requesting Agency Hub Access Participant's Representative must circulate to the Hub Access Participant's Users any relevant information which the Hub Controller provides to the Representative.

(b) A Data Holding Agency Hub Access Participant's Representative must notify the Hub Controller if its provision of Responses to a Requesting Agency Hub Access Participant is likely to be delayed.

(c) As soon as possible, whether before it occurs or afterwards, the Hub Access Participant must notify the Hub Operator of an Outage by recording the Outage through the Portal outage functionality.

29 **INTERACTIONS WITH THE PUBLIC**

(a) A Hub Access Participant must:

(i) respond to any enquiries or complaints by members of the public:

A. where the Participant is the subject of the enquiry or complaint; and

B. which relate to the Identity Information provided to Users of the Services;

(ii) where the Hub Access Participant is a Data Holding Agency, provide an accessible process for members of the public to correct any information held by the Hub Access Participant; and

(iii) review decisions relating to privacy, in accordance with its own procedures.

(b) Where a Participant receives a complaint from a member of the public relating to the Services or the NDLFRS and the complaint relates to a different Participant, then:

(i) the Participant that received the complaint must notify the Participant to which the complaint relates, providing all relevant details; and

(ii) the Participant to which the complaint relates must take responsibility for addressing the complaint.

(c) Each Hub Access Participant acknowledges that the Hub Controller is the central point of contact for any public enquiries about the Interoperability Hub and the Hub Access Participant must cooperate with the Hub Controller when the Hub Controller undertakes any coordination necessary for public statements.

30 SUBCONTRACTING AND COORDINATING AGENCIES

30.1 Subcontracting

(a) A Hub Access Participant may outsource or subcontract any aspect of its connection to the Interoperability Hub to one or more external service providers.

(b) The Hub Controller may outsource or subcontract to one or more external service providers any and all aspects of the Interoperability Hub or other matters to be performed by the Hub Controller under or in connection with any Participant Access Arrangement.

(c) Nothing in this clause 30.1 derogates from a Participant's obligations under this Agreement. Each Participant is responsible and liable under this Agreement for any acts or omissions undertaken on its behalf by a subcontractor.

(d) Where requested, each Hub Access Participant and the Hub Controller (as relevant) will:

(i) promptly provide all reasonable assistance to enable the other to comply with its obligations under its contracts with its external service providers; and

(ii) cooperate with the other's external service providers as reasonably required to further the best interests of the Services.

(e) Each Participant must ensure that each of its subcontractors, unless exempt from compliance with privacy legislation under clause 16.1(d):

(i) if subject to State or Territory privacy legislation, complies with its obligations under that legislation; or

(ii) otherwise, complies with the Australian Privacy Principles in Schedule 1 of the Privacy Act as if such subcontractor was an APP entity within the meaning of the Privacy Act.

30.2 Delegate Agencies

(a) Subject to clause 30.2(b), a Requesting Agency or a Data Holding Agency, or one or more Requesting Agencies and/or Data Holding Agencies within the same jurisdictions acting jointly, may appoint another Agency (in this clause 30.2, the **Delegate Agency**) from within

the same jurisdiction (which need not be a Participant) to coordinate or undertake on its or their behalf:

(i) the management of User Accounts (including, but not limited to, the creation, modification and deactivation of User Accounts);

(ii) monitoring use of the Services by Requesting Agencies:

A. using a Service to access Data Sources within that jurisdiction (except where use of the Services is for protecting Legally Assumed Identities); and/or

B. within that jurisdiction in respect of their access to any available Data Sources (except where use of the Services is for protecting Legally Assumed Identities);

(iii) the conduct of Annual Audits in accordance with this Agreement; and/or

(iv) the performance of any other obligations or functions under this Agreement.

(b) Before:

(i) appointing or replacing a Delegate Agency; or

(ii) defining or modifying the scope of a Delegate Agency's responsibilities,

the relevant Requesting Agencies and/or Data Holding Agencies must obtain the prior approval of the Governing Body for:

(iii) the appointment of the Delegate Agency; and

(iv) the specific functions to be performed by the Delegate Agency.

(c) Nothing in this clause 30.2 derogates from a Participant's obligations under this Agreement. Each Participant is responsible and liable under this Agreement for any acts or omissions undertaken on its behalf by a Delegate Agency.

PART 3 DATA SOURCE ACCESS CONDITIONS

31 FACE MATCHING SERVICES

(a) The Face Matching Services enable a Requesting Agency to Query Data Sources made available by a Data Holding Agency and receive Reponses in accordance with their Participant Access Arrangement.

(b) To utilise the Face Matching Services, Queries and Responses must be sent and received by Participants via the Interoperability Hub.

(c) The Hub Controller will make the Interoperability Hub available to Participants in accordance with Hub Access Conditions and the Participant Access Arrangement between the relevant Participants and the Hub Controller.

(d) The details of each Face Matching Service are contained in the FMS Catalogue and the relevant Participant Access Arrangement.

(e) As at the date of this Agreement, the Face Matching Services comprise the following 3 services:

(i) the Face Verification Service;

(ii) the Face Identification Service; and

(iii) the One Person One Licence Service.

32 FMS CATALOGUE AND DATA SOURCES

32.1 FMS Catalogue

(a) The Hub Controller will maintain the FMS Catalogue.

(b) Each Data Holding Agency must agree with the Hub Controller the Data Sources, Functions and other items it will make available through the FMS Catalogue for each Service, and any of the Data Holding Agency's other requirements, by submitting such information to the Hub Controller in the form agreed with the Hub Controller.

(c) The Hub Controller may accept or reject the information submitted pursuant to clause 32.1(b) and if accepted, must include the relevant details in the FMS Catalogue. The Hub Controller may, without

limitation, reject all or any part of a proposal from a Data Holding Agency where the Hub Controller considers that:

(i) it is not be permitted by law;

(ii) it exceeds the scope of Services permitted under this Agreement; or

(iii) it cannot be accommodated by the Interoperability Hub.

(d) Each Data Holding Agency must ensure that its entries in the FMS Catalogue are at all times fully accurate and up to date with details of all Data Sources and Functions the Data Holding Agency offers to make available to Requesting Agencies in accordance with the relevant Participant Access Arrangement as part of the Services.

(e) A Data Holding Agency can vary or withdraw any offer in the FMS Catalogue at any time. This, however, does not affect Participant Access Arrangements in place before any such variation or withdrawal (which may only be varied or terminated in accordance with the provisions of the relevant Participant Access Arrangement and this Agreement).

32.2 **Control of Data Sources**

(a) Each Data Holding Agency at all times retains complete control of its Data Sources and access to them and, without limitation, may determine in its absolute discretion:

(i) which Data Sources and Functions it will make available to any Requesting Agency (including any standing offers);

(ii) which Nominated User Roles are permitted to access a Data Source via any Service and Function and, where relevant, the Permitted Purposes for which access and use may be provided to such Nominated User Roles;

(iii) which Requesting Agency Roles may Query the Data Holding Agency's Data Sources;

(iv) the mandatory and optional information required or permitted for Queries against the Data Source;

(v) what Supported Response Details will be provided or available in Responses to Queries to a Data Source by Requesting Agency (which can vary by Role); and

(vi) the conditions (if any) a Requesting Agency must comply with in order to access the Data Holding Agency's Data Sources (or any one of them).

(b) Notwithstanding the terms of any Participant Access Arrangement, if a Participant withdraws a Data Source or that Data Source is no longer made available through a Service for any reason, then any Services under this Agreement that require use of that Data Source will not be provided for the duration that such withdrawal or unavailability of the relevant Identity Information.

[redacted]

34 ASSURING AND PROTECTING IDENTITY INFORMATION

34.1 Protection of Identity Information

Both the Data Holding Agency and the Requesting Agency under a Participant Access Arrangement must comply with all:

(a) legislative requirements of the Commonwealth or a State or Territory; and

(b) other applicable Australian laws,

in their respective jurisdictions, insofar as those laws are relevant to the Participant Access Arrangement (without limitation including those relating to record keeping, identity information protection, privacy and protection of Personal Information).

[redacted]

34.3 **Quality assurance**

If a Requesting Agency receives from a Data Holding Agency a Response which contains Identity Information that the Requesting Agency considers or suspects (at the time of receipt of the Response or subsequently) is inaccurate or incorrect for any reason, including because the Identity Information (that

had appeared to be correct) failed to validate against relevant Government Identification Documentation, the Requesting Agency must notify the relevant Data Holding Agency of this as soon as reasonably possible, and provide in that notice all relevant details.

35 DESTRUCTION OF IDENTITY INFORMATION

35.1 Destruction of Identity Information – Requesting Agency

Where Identity Information is obtained from a Data Holding Agency by a Requesting Agency via a Service, the Requesting Agency must:

(a) only retain that Identity Information for the minimum period of time that is necessary to both:

(i) fulfil the purpose for which the Identity Information was obtained; and

(ii) comply with relevant laws applicable in its jurisdiction as required by clause 34.1 (including any laws that require the retention of such Identity Information for a specific or indefinite period of time); and

(b) permanently erase or totally destroy all such Identity Information at the expiry of the period determined in accordance with clause 35.1(a) (if such period does expire).

(c) if requested by the Data Holding Agency, provide written certification of the erasure or destruction of the relevant Identity Information.

35.2 Destruction of Identity Information – Data Holding Agency

Where Identity Information is obtained by a Data Holding Agency from a Requesting Agency via a Query, the Data Holding Agency must:

(a) only retain that Identity Information for the minimum period of time that is necessary to both:

(i) process the Query and provide a Response to it; and

(ii) comply with relevant laws as required by clause 34.1;

(b) permanently erase or totally destroy all such Identity Information at the expiry of the period determined in accordance with clause 35.2(a); and

(c) if requested by the Requesting Agency, provide written certification of the erasure or destruction of the relevant Identity Information.

35.3 **Survival**

This clause 35 survives termination of this Agreement for any reason.

36 **DISCLOSURE OF IDENTITY INFORMATION TO THIRD PARTIES**

The Requesting Agency must not disclose Identity Information obtained via a Participant Access Arrangement to a third party unless:

(a) the Requesting Agency is legally required to disclose the relevant Identity Information, including, but not limited to, situations where the Identity Information is required by a court, for a criminal investigation or by a Royal Commission; or

(b) the Requesting Agency is legally authorised to disclose Identity Information, but not required to do so, and one of the following applies:

(i) the release of the Identity Information is for one or more Authorised Disclosure Purposes;

(ii) the Data Holding Agency agrees in writing that the Requesting Agency may disclose the Identity Information to the third party; or

(iii) the Requesting Agency has obtained informed consent in writing from the individual to whom the Identity Information relates.

This clause 36 survives termination of this Agreement for any reason.

37 **SAFEGUARDING MINORS**

Each Requesting Agency and Data Holding Agency must implement appropriate controls and other safeguards within their systems, processes and procedures to reflect special considerations that are relevant to facial recognition matching on persons under the age of eighteen years and in guiding actions and/or decisions taken as a result of such matching, without limitation including considering and taking into account:

(a) the greater risk of misidentification for persons under the age of eighteen years compared to persons over the age of eighteen years or older; and

(b) the best interests of any person who is under the age of eighteen years.

38 RECORD KEEPING

38.1 Transaction Records

(a) Each Requesting Agency and each Data Holding Agency must maintain all Required Transaction Records.

(b) Required Transaction Records must be retained at least until the later of:

(i) the date being ninety calendar days from the date the Data Holding Agency receives the Annual Audit Report covering the relevant Required Transaction Records;

(ii) the expiry of the period (if any) stated in the Participant Access Arrangement Details during which Required Transaction Records must be kept; and

(iii) the date on which the owner of the records can dispose of the records in accordance with the law.

38.2 General Record Keeping

Without limiting any other obligation under a Participant Access Arrangement or at law, each of the Requesting Agency and the Data Holding Agency must at its own cost:

(a) keep full and complete records in accordance with the Annual Audit requirements in clause 39; and

(b) ensure that all data, information and records relating to the Participant Access Arrangement (and performance of their respective obligations under it) are maintained in such a form and manner and time as to facilitate access and inspection required for auditing purposes as detailed in clause 39 or for any other purpose relevant to the Participant Access Arrangement.

38.3 Survival

This clause 38 survives termination of this Agreement for any reason.

39 REQUESTING AGENCY ANNUAL AUDITS

39.1 Application of this clause 39

All Participants other than Sanitising Agencies must comply with this clause 39.

39.2 **Overview**

(a) Each Requesting Agency (other than Sanitising Agencies) must ensure an Annual Audit is conducted in accordance with this clause 39.

(b) The purposes of the Annual Audit are to:

(i) confirm the Requesting Agency's compliance with the Participant Access Arrangement (subject to any non-compliances detailed in the Annual Audit Report); and

(ii) make recommendations, which if implemented, would address:

A. any non-compliance or shortcoming identified by the Annual Audit;

B. any shortcoming or issue identified by the Annual Audit that the Auditor considers should be addressed to ensure that Requesting Agency's compliance can be demonstrated and audited to a high standard; and

C. any other matter the Auditor considers should be noted.

39.3 **Conduct of Annual Audits**

(a) The Annual Audit must be conducted by an Auditor.

(b) The Requesting Agency must ensure the Auditor completes the Annual Audit and Annual Audit Report in conformity with the legal obligations in clause 34.1.

(c) The Annual Audit must, without limitation, include an inspection of the Requesting Agency's systems, processes, record keeping and overall use of the relevant Services under the Participant Access Arrangement.

(d) The Requesting Agency must inform the Data Holding Agency of the selection of the Auditor to be engaged.

(e) Subject to clause 39.3(f), the Auditor must be independent of the Requesting Agency.

(f) If the Data Holding Agency and the Requesting Agency agree that it is not feasible for an Auditor to be independent of the Requesting Agency, then:

(i) the Requesting Agency may instead use an Auditor that is not independent; and

(ii) the Annual Audit Report must include a statement containing the reasons why the Participants determined it was not feasible to engage an independent Auditor.

(g) The Requesting Agency and the Data Holding Agency must make the following information fully accessible to the Auditor for the purpose of conducting the Annual Audit:

(i) all information pertaining to the Participant Access Arrangement; and

(ii) any other information relevant for the purposes of the Annual Audit.

(h) The Hub Controller may maintain a list of Auditors from time to time.

39.4 **Content of Annual Audit Report**

The results of an Annual Audit must be detailed in an Annual Audit Report by the Auditor that must include, but is not limited to, the following:

(a) where applicable, details of any detected instances where the Requesting Agency's access to any Service, or use of Identity Information obtained under the Participant Access Arrangement, was not (or could not reasonably be verified to be) within the Requesting Agency's legislative authority according to the Requesting Agency's Statement of Legislative Authority at the time of access;

(b) where applicable, details of any instances where access to or use of information in relation to this Agreement breached any provision of this Agreement or a relevant Participation Access Agreement;

(c) where applicable, details of any Security Breaches in relation to the Requesting Agency and any action that was taken by the Requesting Agency (or the Data Holding Agency, the Hub Controller or anyone else) to rectify the Security Breaches;

(d) where applicable, details of any complaints received by the Requesting Agency in relation to its use of the Services or Identity Information obtained under the relevant Participant Access Arrangement(s), including from members of the public, and details of any action taken by each Participant in response to complaints received;

(e) the size and composition of the random samples used in the Annual Audit and a statement explaining how the samples are appropriate to support the conclusions of the Annual Audit Report;

(f) the handling by the Requesting Agency of Identity Information provided in Query Responses, including whether, and if so when, where and how, the Requesting Agency stored the Identity Information and whether the Requesting Agency complied with clause 35; and

(g) all relevant service specific Annual Audit Report requirements detailed in each Participant Access Arrangement to which the Requesting Agency is party.

39.5 **Face Identification Service-specific Annual Audit requirements**

Without limiting any requirement in relation to the Annual Audit, to the extent it relates to the Face Identification Service, the Annual Audit Report by the Auditor must also include, but is not limited to, the following matters:

(a) whether appropriate authorisation was obtained for Face Identification Service Queries where required by this Agreement and, particularly any instances where appropriate authorisation was not obtained;

(b) the number of Face Identification Service Queries carried out for the 'community safety' purpose and the nature of any Queries where, in the opinion of the Auditor, the authorisation of the Query failed to adequately take into account the increased privacy risk associated with this purpose;

(c) the number of Face Identification Service Queries carried out for the 'general law enforcement' purpose under the category of 'other indictable offences' and the type of offence that was associated with the Query;

(d) the number and purpose of Face Identification Service Queries where the Nominated User obtained a response containing greater than the default maximum number of Facial Image matches; and

(e) where applicable, the nature and frequency of Queries conducted where authorisation was obtained after the Query was submitted.

39.6 **Outcome of Annual Audit Report**

(a) The Requesting Agency must ensure that the Auditor provides the completed Annual Audit Report to the Framework Administrator's

Representative, and the Requesting Agency's and relevant Data Holding Agency's Representatives, as soon as practicable after the end of the relevant calendar year, and in any event no later than five months after the end of that year.

(b) The Participants acknowledge that the Framework Administrator will table the Annual Audit Reports obtained under subclause 39.6(a) for the approval or action of the Governing Body.

(c) If the Data Holding Agency is not satisfied with the conduct of the Annual Audit, it may initiate the Dispute resolution process set out in clause 19.

39.7 **Jurisdiction-wide audits**

39.8 Provided that all requirements of this clause 39 are otherwise satisfied, two or more Requesting Agencies subject to the same jurisdiction within Australia may participate in the same audit process and be covered by the same Annual Audit Report, rather than conducting separate audits and preparing separate Annual Audit Reports.

39.9 **Survival**

This clause 39 survives termination of this Agreement for any reason.

40 FACIAL RECOGNITION SYSTEM

40.1 Variation to Facial Recognition System for Services

(a) Subject to clause 40.1(b), a Data Holding Agency will, if requested by a Requesting Agency with whom it has a Participant Access Arrangement, notify the Requesting Agency of any proposed material changes to the Data Holding Agency's Facial Recognition System (or other relevant systems) which might impact the basis on which Match Scores are generated or impact threshold scores even if those changes do not amount to a variation of the Participant Access Arrangement.

(b) Clause 40.1(a) does not apply to Data Holding Agencies that are NDLFRS Contributors under the NDLFRS Hosting Agreement, in respect of which the Data Hosting Agency has responsibility in accordance with the NDLFRS Hosting Agreement.

(c) Each Requesting Agency must assess what, if any, changes the Requesting Agency should make to its use of Services under its Participant Access Arrangement as a result of such changes.

40.2 **Variation to Facial Recognition System for NDLFRS**

(a) Each Participant acknowledges and agrees that:

(i) the Matching Thresholds used in the NDLFRS, and the components that make up the NDLFRS, will be determined in accordance with the NDLFRS Hosting Agreement;

(ii) the Matching Thresholds used in Face Matching Services (including the FVS, FIS and OPOLS) on Data Sources made available by NDLFRS Contributors, will be determined in accordance with the NDLFRS Hosting Agreement; and

(iii) the Data Hosting Agency has no liability to any Participant or any other person in respect of the Matching Thresholds set in accordance with the NDLFRS Hosting Agreement.

40.3 **Risk management and redundancy**

(a) Each Participant acknowledges that use of any Service is at that Participant's sole risk.

(b) It is the responsibility of each Participant to ensure that it has suitable measures in place to allow it to meet its overall business objectives in the event that the Services are temporarily unavailable due to factors beyond the Participant's control.

PART 4 PARTICIPANT ACCESS ARRANGEMENTS

41 **PRIORITY OF PARTICIPANT ACCESS ARRANGEMENTS**

(a) This Agreement (including the Hub Access Conditions and Data Source Access Conditions) takes precedence over the terms of any Participant Access Arrangement and prevails to the extent of any inconsistency.

(b) Each Participant Access Arrangement applies in addition to, and is subject to the terms and conditions of, this Agreement, including the Hub Access Conditions and the Data Source Access Conditions.

42 **ENTRY INTO AND VARIATION OF PARTICIPANT ACCESS ARRANGEMENTS**

(a) Each Participant Access Arrangement will be between:

(i) a Requesting Agency;

(ii) the Hub Controller; and

(iii) one or more Data Holding Agencies (or the Hub Controller on their behalf, where permitted by this clause 42),

(b) Where a Requesting Agency wishes to enter into a Participant Access Arrangement, the Requesting Agency must complete and submit to the Hub Controller a Template Participant Access Arrangement setting out its request.

(c) Where a Requesting Agency wishes to submit Queries to a Data Source or otherwise access a Service to which it does not already have access, or otherwise vary the terms of an existing Participant Access Arrangement, it must complete and submit to the Hub Controller the variation request form contained in its Participant Access Arrangement (or in the manner otherwise agreed with the Hub Controller) (**Variation Request Form**) setting out its request.

(d) When it receives a completed Template Participant Access Arrangement or Variation Request Form from a Requesting Agency under clause 42(a), 42(b) or 42(c) and the approval of one or more Data Holding Agencies is required under clause 42(e), the Hub Controller must promptly provide a copy of the completed Template Participant Access

Arrangement or Variation Request Form (as applicable) to each such Data Holding Agency.

(e) Subject to clause 42(g), each relevant Data Holding Agency must promptly notify the Hub Controller whether or not it approves of the completed Template Participant Access Arrangement or Variation Request Form (as applicable) and if not, why not.

(f) The Hub Controller must then notify the Requesting Agency either that:

(i) the Hub Controller and each relevant Data Holding Agency (or if applicable, the Hub Controller on their behalf) has approved the completed Template Participant Access Arrangement or Variation Request Form (as applicable) submitted by the Requesting Agency; or

(ii) the Hub Controller and/or one or more Data Holding Agencies (or if applicable, the Hub Controller on their behalf) have declined to approve the completed Template Participant Access Arrangement or Variation Request Form (as applicable) submitted by the Requesting Agency, in which case the notice must outline why it was declined.

(g) A Data Holding Agency's approval of a completed Template Participant Access Arrangement or Variation Request Form (as applicable) submitted by a Requesting Agency will not be required if the Data Holding Agency has agreed with the Hub Controller that the Hub Controller may agree the arrangements contemplated by the proposed Participant Access Arrangement or Variation Request Form (as applicable) on behalf of the Data Holding Agency in accordance with clause 43..

(h) Where a completed Template Participant Access Arrangement or Variation Request Form (as applicable) has not been approved by the Hub Controller and/or one or more Data Holding Agencies, the relevant Requesting Agency may revise the Template Participant Access Arrangement or Variation Request Form (as applicable) it previously completed and re-submit it in accordance with this clause 42.

(i) Once a completed Template Participant Access Arrangement submitted by a Requesting Agency has been approved in accordance with this clause 42, it must be signed by each relevant Participant, after which it will become a Participant Access Arrangement between the Hub

Controller and relevant Requesting Agency and relevant Data Holding Agencies for the purposes of this Agreement.

(j) Once a completed Variation Request Form submitted by a Requesting Agency has been approved in accordance with this clause 42, it must be signed by each relevant Participant, after which it will amend the Requesting Agency's existing Participant Access Arrangement.

43 **PRE-AGREED DHA ARRANGEMENTS**

(a) A Data Holding Agency may agree with the Hub Controller certain parameters which, if satisfied by a completed Template Participant Access Arrangement or Variation Request Form (as applicable) submitted by a Requesting Agency, permit the Hub Controller to agree and enter into the resultant Participant Access Arrangement or Variation Request Form (as applicable) with a Requesting Agency on behalf of the Data Holding Agency without requiring the approval or signature of the Data Holding Agency under clause 42(e) (in this clause, a **Pre-Agreed DHA Arrangement**).

(b) A Data Holding Agency must not agree any Pre-Agreed DHA Arrangements with the Hub Controller unless the Data Holding Agency is independently satisfied on its own behalf that all aspects of any Participant Access Arrangement that would result from the Pre-Agreed DHA Arrangement will be lawful and consistent with the Data Holding Agency's obligations under this Agreement.

(c) Each Data Holding Agency and each Requesting Agency that is party to a Participant Access Arrangement which is agreed by the Hub Controller on behalf of a Data Holding Agency pursuant to a Pre-Agreed DHA Arrangement acknowledges and agrees:

(i) notwithstanding its approval of a Participant Access Arrangement on behalf of a Data Holding Agency, the Hub Controller accepts no liability on behalf of the Data Holding Agency in respect of the Participant Access Arrangement; and

(ii) each Requesting Agency and Data Holding Agency retains responsibility for its own obligations under this Agreement and compliance with legislative requirements for the handling of Personal Information.

(d) Each Participant acknowledges and agrees that, in respect of any Pre-Agreed DHA Arrangement:

(i) the Hub Controller may only enter into and/or implement a Participant Access Arrangement strictly in accordance with the terms of that Pre-Agreed DHA Arrangement; and

(ii) a Data Holding Agency may revoke and/or seek to amend its Pre-Agreed DHA Arrangement at any time by written notice.

44 REGISTRATION OF PARTICIPANT ACCESS ARRANGEMENTS

(a) Where a Participant Access Arrangement has been approved in accordance with this Agreement, the Hub Controller must promptly register the details of the Participant Access Arrangement on the Interoperability Hub.

(b) The Hub Controller will maintain a record of each Participant Access Arrangement.

45 COMMENCEMENT OF A PARTICIPANT ACCESS ARRANGEMENT

A Participant Access Arrangement commences on the date notified by the Hub Controller to the relevant Data Holding Agency and the relevant Requesting Agency that the Interoperability Hub has been configured to support the Participant Access Arrangement.

46 LEGISLATIVE BASIS OF PARTICIPANT ACCESS ARRANGEMENTS

46.1 Compliance with legislative requirements

(a) Neither a Data Holding Agency nor a Requesting Agency may enter into a Participant Access Arrangement unless each is independently satisfied on its own behalf that all aspects of the Participant Access Arrangement will be lawful.

(b) A Data Holding Agency must ensure that each Participant Access Arrangement to which it is party contains a Data Holding Agency Statement of Legislative Authority detailing the basis on which the Data Holding Agency believes its offer to provide access to a Data Source via relevant Services as proposed under the relevant Participant Access Arrangement will be lawful.

(c) A Requesting Agency must ensure that each Participant Access Arrangement to which it is party contains a Requesting Agency Statement of Legislative Authority detailing the legislative provisions and other relevant information that the Requesting Agency believes establishes that its access to and use of a Data Source via the relevant

Services as proposed under the relevant Participant Access Arrangement will be lawful.

(d) Where appropriate, the Data Holding Agency and the Requesting Agency should seek legal advice on relevant matters including on the relevant legislative basis for collecting, using and disclosing the Identity Information prior to providing their respective Statements of Legislative Compliance as required by clauses 46.1(b) and 46.1(c).

46.2 **Privacy Impact Assessments**

(a) All Participants other than Sanitising Agencies must comply with this clause 46.2.

(b) Subject to clause 46.2(p), before entering into a Participant Access Arrangement, each Data Holding Agency and each Requesting Agency (other than Sanitising Agencies) must ensure that:

(i) a Privacy Impact Assessment is conducted for those uses of the Services that are proposed to be enabled by the Participant Access Arrangement; and

(ii) a Privacy Impact Assessment Report is obtained.

(c) A Privacy Impact Assessment may be conducted, and Privacy Impact Assessment Report may be obtained, for multiple Data Holding Agencies and multiple Requesting Agencies at the same time, provided that the Privacy Impact Assessment and Privacy Impact Report specifically addresses each Requesting Agency's use of the Services that is proposed to be enabled by each proposed Participant Access Arrangement.

(d) A person appointed to conduct a Privacy Impact Assessment must:

(i) subject to clause 46.2(h), be independent of the relevant Data Holding Agency or Data Holding Agencies and the relevant Requesting Agency or Requesting Agencies that are the subject to the Privacy Impact Assessment;

(ii) be a Privacy Impact Assessment Expert; and

(iii) have consented to conducting the Privacy Impact Assessment.

(e) A Privacy Impact Assessment must be commissioned:

(i) by the relevant Requesting Agency or Requesting Agencies at their cost (unless the relevant Data Holding Agency or Data Holding Agencies specifically agree in writing with the Requesting Agency that they or another third party will commission and pay for the Privacy Impact Assessment); and

(ii) on the basis that the Privacy Impact Assessment is conducted on behalf, and for the benefit, of:

A. each relevant Data Holding Agency;

B. each relevant Requesting Agency;

C. the Hub Controller; and

D. the Framework Administrator.

(f) The findings and recommendations of a Privacy Impact Assessment must be set out in a Privacy Impact Assessment Report.

(g) The relevant Data Holding Agency or Data Holding Agencies and Requesting Agency or Requesting Agencies cannot agree as between themselves that a third party or other Participant will pay for a Privacy Impact Assessment and Privacy Impact Assessment Report without the consent of such third party or other Participant.

(h) Where the relevant Data Holding Agency or Data Holding Agencies and Requesting Agency or Requesting Agencies agree that it is not feasible to comply with clause 46.2(d)(i), then they may agree to permit a person who is not independent of them to conduct the whole or any part of a Privacy Impact Assessment, provided that the Privacy Impact Assessment Report includes a statement containing the reasons why they determined it was not feasible to comply with clause 46.2(d)(i).

(i) The relevant Data Holding Agency or Data Holding Agencies and Requesting Agency or Requesting Agencies must co-operate with the Privacy Impact Assessment Expert(s) (or other person(s) appointed under clause 46.2(d)) in conducting the Privacy Impact Assessment and to provide such person(s) with the information needed for this purpose in a timely fashion.

(j) The relevant Data Holding Agency or Data Holding Agencies and Requesting Agency or Requesting Agencies must:

(i) jointly develop a formal response to the Privacy Impact Assessment Report within a reasonable time after the finalisation of the Privacy Impact Assessment Report; and

(ii) each use their best efforts to implement the response to the Privacy Impact Assessment Report.

(k) Each relevant Requesting Agency must provide a copy of the Privacy Impact Assessment Report to the Hub Controller and the Framework Administrator (which can be redacted where necessary) promptly following its receipt.

(l) Where following completion of a Privacy Impact Assessment:

(i) any material change is proposed to the use of the Services that is proposed to be enabled by the Participant Access Arrangement; or

(ii) any other matter arises or occurs that is relevant to the validity of the Privacy Impact Assessment Report,

the Privacy Impact Assessment must be re-conducted, and a new Privacy Impact Assessment Report provided, as soon as is reasonably possible (and, in any event, before the use of the Services that is proposed to be enabled by the Participant Access Arrangement can be agreed or implemented).

(m) Where a Privacy Impact Assessment Report was previously conducted in respect of multiple Requesting Agencies and/or Data Holding Agencies, nothing in this Agreement prevents any Requesting Agency from procuring a new Privacy Impact Assessment and Privacy Impact Assessment Report relating only to it and its relevant Data Holding Agencies.

(n) Requesting Agencies must publish the Privacy Impact Assessment Report(s) relevant to their use of the Services, unless the relevant Privacy Impact Assessment Report(s) have already been published by another Participant.

(o) A Requesting Agency required to publish or make available a Privacy Impact Assessment under this Agreement, where required to do so for security reasons, may:

(i) redact the relevant parts of the Privacy Impact Assessment to the extent necessary before publishing or otherwise making it available; or

(ii) publish or make available extracts of the Privacy Impact Assessment only.

(p) Where access to information through a Service is exempt from otherwise applicable Commonwealth or State or Territory privacy laws:

(i) the Requesting Agency (or if applicable, other relevant Agency including each entity referred to in clause 16.1(d)) may develop a privacy statement, instead of obtaining a Privacy Impact Assessment; and

(ii) such privacy statement must:

A. outline the legislative, policy and other safeguards that apply to the handling of Personal Information to be obtained via the Service;

B. be developed in consultation with the relevant Data Holding Agency or Data Holding Agencies from which the information will be obtained; and

C. be approved by the Governing Body.

47 CONTENT REQUIREMENTS FOR PARTICIPANT ACCESS ARRANGEMENTS

47.1 Basis for protection of Personal Information

Participant Access Arrangements must record all relevant arrangements for the protection of Personal Information that will be shared through Services accessed pursuant to the Participant Access Arrangement.

47.2 Basis for sharing information

Participant Access Arrangements must record all arrangements for sharing information through the Services accessed pursuant to the Participant Access Arrangement.

48 REQUIREMENT TO PROVIDE AGENCY LIST

The Hub Controller must provide to each Data Holding Agency:

(a) each October during the term of this Agreement, a list of Requesting Agencies that have accessed the Data Holding Agency's Data Sources in the preceding year; and

(b) on each occasion a Requesting Agency either obtains or ceases to have access to the Data Holding Agency's Data Sources, the identity of the Requesting Agency and details of that access (or cessation of access).

49 PRESERVATION OF ACCRUED RIGHTS

Termination of a Participant Access Arrangement shall not prejudice any right or liability that accrued to either the relevant Participants or the Hub Controller prior to the date of such termination (without limitation including liability to pay charges arising prior to or as a result of the termination of Participant Access Arrangement).

50 VARIATION

50.1 Participant Access Arrangement

The Hub Controller, a Data Holding Agency and a Requesting Agency may vary the Participant Access Arrangement applying between them at any time by mutual agreement in writing (or as otherwise agreed between them) providing that any such variation that involves a change to the Participant Access Arrangement registered with the Hub Controller shall not be effective until the Hub Controller updates the relevant registered details.

PART 5 SERVICE DETAILS

51 SERVICE DETAILS

51.1 Provision of Services

(a) This Part 5 (Service Details) of this Agreement sets out certain terms upon which FVS, FIS and OPOLS will be provided as Services as at the date of this Agreement.

(b) Participants must ensure that, subject to anything to the contrary in the FMS Catalogue, they and their Users (as applicable), comply with the requirements of this Part 5 (Service Details) and relevant Participant Access Arrangements in respect of their use of FVS, FIS and OPOLS.

(c) All provisions of this Part 5 (Service Details), including as relate to the Services, are subject to anything to the contrary in the FMS Catalogue.

52 THE FACE VERIFICATION SERVICE (FVS)

52.1 Overview of FVS

(a) FVS is a Face Matching Service. It has three functions (retrieve, match and search) that enable biographic details or a Facial Image associated with an individual to be compared, on a one-to-one basis, against an image held on a specific government record associated with that same individual.

(b) FVS allows a Nominated User to submit a person's Biographic Information details, document number and Facial Image by way of a Query to a relevant Data Source and to receive a Response to verify that person's Record.

52.2 FVS access requirements

(a) Only Nominated Users may submit queries through the FVS.

(b) Requesting Agencies must ensure that they only appoint as Nominated Users employees with a reasonable need to access the FVS to perform their functions and activities with the Agency.

(c) Any information technology (IT) system that a Requesting Agency proposes to be a Nominated User must have a reasonable need to use the FVS to perform operations required by the Requesting Agency.

(d) A Nominated User must not be provided with access to the FIS and FVS concurrently for the same Data Source, unless that Nominated User is acting on behalf of a Sanitising Agency and requires access to both FIS and FVS for the sole purposes of clause 34.

(e) Participants must ensure that any IT systems that are Nominated Users or that are otherwise connected to the Interoperability Hub (i.e. through system to system arrangements) receive and maintain appropriate security accreditation, in accordance with the requirements of the PSPF and Information Security Manual.

(f) If a Nominated User of a Requesting Agency no longer requires access to FVS, the Requesting Agency must terminate that Nominated User's access to FVS as soon as reasonably possible.

52.3 **FVS Matching Thresholds**

Each Participant acknowledges that each Data Holding Agency that is not an NDLFRS Contributor is entitled to set the Matching Threshold applicable to its Data Sources in respect of FVS.

53 THE FACE IDENTIFICATION SERVICE (FIS)

53.1 Overview of FIS

(a) The Face Identification Service (FIS) is a Face Matching Service. It has one function (identify) that searches or matches Facial Images on a one-to-many basis to help determine the identity of an unknown person, where little or no biographic details are available; or detect instances where a person may hold multiple fraudulent identities.

(b) FIS allows a Nominated User to submit a person's Facial Image (with or without any Biographic Information of any quality), together with other mandatory information (if any) by way of a Query to a relevant Data Source and to receive a Response detailing one or more Matching Facial Images from the Data Source (assuming there is a Match) up to the relevant Match limit.

53.2 FIS access requirements

(a) A Requesting Agency may access FIS for the following purposes only:

(i) preventing identity crime;

(ii) general law enforcement, provided that:

A. subject to subclause 53.2(a)(ii), the access for general law enforcement is limited to offences that carry a maximum penalty of at least three years imprisonment; and

B. the limitation in subclause 53.2(a)(ii)A does not apply in circumstances where the Requesting Agency is requesting information from a Data Holding Agency within the same jurisdiction as the Requesting Agency, provided that any access to the FIS for law enforcement purposes relating to offences carrying a penalty of less than three years imprisonment must be agreed by the Data Holding Agency in the relevant Participant Access Agreement;

(iii) national security;

(iv) protective security; and/or

(v) community safety.

(b) The purposes set out in clause 53.2(a) are to be read in conjunction with the FIS permitted purposes set out in the Intergovernmental Agreement and any enabling legislation.

(c) Each individual User's access to FIS must be subject to supervision by a more senior officer.

(d) Nominated Users for FIS are generally authorised to submit queries that meet the Permitted Purposes referred to in clause 53.2(a). Their use of the FIS must be monitored by a 'Supervising Officer'.

(e) A 'Supervising Officer' must:

(i) in the case of Participant that is a police agency, be an individual holding the highest non-commissioned officer rank (or any equivalent or higher rank), or an unsworn individual who is required to perform a supervisory role pursuant to current respective police force oversight arrangements; and

(ii) in the case of all other Participants, be an officer holding the position of Executive Level 1 (or any equivalent or higher rank).

(f) FIS queries conducted for the purpose of community safety must not be used to identify persons undertaking activities that involve the peaceful, lawful expression of political, religious or other views, such as public protests or demonstrations.

(g) An 'Authorising Officer' must:

(i) in the case of Participant that is a police agency, be an individual holding a commissioned officer rank (or any equivalent or higher rank), or an unsworn individual who is required to perform a supervisory role pursuant to current respective police force oversight arrangements; and

(ii) in the case of all other Participants, be an officer holding the position of Executive Level 2 (or any equivalent or higher rank).

(h) Only Nominated Users may submit queries through the FIS.

(i) Requesting Agencies must ensure that they only appoint as Nominated Users employees who have a specialist investigative, intelligence, incident response, forensic, or operational security function and who have a reasonable need to access FIS to perform their functions and activities with the Requesting Agency.

(j) Nominated Users granted access to FIS must have no less than a Baseline Security Clearance or a State or Territory equivalent, or as approved by the Governing Body.

(k) A Participant must notify their Client Administrator if any of their Nominated Users, Supervising Officers or Authorising Officers cease to require access to FIS, to enable the Client Administrator to ensure their access to FIS is terminated.

53.3 **Permitted Purposes and authorisation of FIS Queries**

(a) Requesting Agencies must obtain the approval of an Authorising Officer prior to submitting an FIS Query:

(i) in relation to any category of serious offence not specifically listed in the FIS Access Policy;

(ii) to identify witnesses to a crime;

(iii) for the purpose of community safety;

(iv) returning a greater number of Facial Image matches than the default maximum; and

(v) involving persons suspected to be under the age of eighteen years.

(b) FIS Users assigned the privilege of receiving greater than the default maximum number of Facial Image matches require authorisation in accordance with this clause.

(c) FIS Nominated Users must indicate a Supervising Officer for a Query. A Supervising Officer for a Query must be superior in rank to the FIS Nominated User. Requesting Agencies must ensure that FIS Nominated Users have selected an appropriate Supervising Officer.[2]

(d) Where the FIS Access Policy provides that an FIS Query requires explicit authorisation by an Authorising Officer, the FIS Nominated User must obtain that authorisation before the Query may be submitted to a Data Holding Agency. The FIS Authorising Officer for an FIS Query must not be the same person as the FIS Nominated User for that Query.[3]

53.4 **Responsibilities of Supervising Officers**

(a) Supervising Officers:

(i) must have a specialist investigative, intelligence, incident response, forensic or protective security function;

(ii) must have at least a Baseline Security Clearance (or equivalent), and

(iii) must not be a FVS Nominated User in relation to a Data Source for which the person has FIS access.

(b) Supervising Officers must ensure that FIS Queries are compliant with this clause 53. If a Supervising Officer detects non-compliance, they must undertake immediate action to address the non-compliance in accordance with relevant legislation and the Compliance Policy.

---

2 While the FIS Nominated User must indicate a Supervising Officer in the Portal, the Portal cannot determine if the Supervising Officer is superior in rank to the FIS Nominated User.

3 The authorisation process described by this paragraph is handled by the Portal.

(c) Every month, or more frequently as appropriate, Requesting Agencies must provide Supervising Officers with a summary of Queries submitted by the Nominated Users they supervise to review.

53.5 FIS Matching Thresholds

Each Participant acknowledges that each Data Holding Agency that is not an NDLFRS Contributor is entitled to set the Matching Threshold applicable to its Data Sources in respect of FIS.

54 THE ONE PERSON ONE LICENCE SERVICE (OPOLS)

54.1 Overview of OPOLS

(a) The One Person One Licence Service (OPOLS) is a Face Matching Service. It enables a narrowly focused check, on a constrained one-to-many basis, of Facial Images within the NDLFRS to identify whether a licence holder or applicant may hold another licence of the same type, in the same or different identity, in another jurisdiction.

(b) OPOLS provides a gallery of a very small number of the highest matching Facial Images, as determined by the facial recognition system of the NDLFRS (based on a pre-configured match threshold).

(c) Further details, and terms and conditions, of OPOLS will be set out in relevant Participant Access Arrangements.

54.2 OPOLS access requirements

(a) Requesting Agencies must ensure that they only appoint OPOLS Reviewers who have a reasonable need to access information obtained through the OPOLS to perform their functions and activities with the Agency.

(b) Requesting Agencies must reconfirm the basis of access for each of their OPOLS Reviewers at ninety calendar day intervals.

(c) If an OPOLS Reviewer of a Requesting Agency no longer requires access to OPOLS, the Requesting Agency must terminate that OPOLS Reviewer's access to OPOLS as soon as reasonably possible.

SIGNING PAGE

Executed as a **deed**.

SIGNED, **SEALED and DELIVERED** for and on behalf of **The Commonwealth of Australia as represented by the Department of Home Affairs** by:

_____
Signature of authorised signatory

_____
Name of authorised signatory

In the presence of:

_____
Signature of witness

_____
Name of witness

SIGNED, **SEALED and DELIVERED** for and on behalf of **the Crown in Right of the State of Victoria as represented by the Roads Corporation (VicRoads)** by its representative

_____
Signature of authorised signatory

_____
Name of authorised signatory

In the presence of:

_____
Signature of witness

_____
Name of witness

SCHEDULE 1 DEED OF ACCESSION

FACE MATCHING SERVICES PARTICIPATION AGREEMENT

DEED OF ACCESSION

[Insert entity name]

(**New Participant**)

FACE MATCHING SERVICES
PARTICIPATION AGREEMENT

Date:

By [new party's legal name] (ABN [insert]) of [address] (**New Participant**)

In favour of the parties to the Participation Agreement from time to time.

RECITALS

A. The Framework Administrator has invited the New Participant to become a Participant for the purposes of the Participation Agreement.

B. This deed poll is supplemental to the Participation Agreement dated [date of agreement] between [insert original parties] as amended and acceded to from time to time (**Participation Agreement**).

C. The New Participant agrees to become a party to the Participation Agreement and to be bound by the terms and conditions of the Participation Agreement as a Participant.

OPERATIVE PART

1 **DEFINITIONS AND INTERPRETATION**

Unless the context otherwise requires:

(a) terms defined in the Participation Agreement have the same meaning when used in this deed; and

(b) the interpretation provisions in the Participation Agreement apply to the interpretation of this deed.

2 **NEW PARTICIPANT**

The New Participant confirms that:

(a) it has been given a copy of the Participation Agreement; and

(b) it will be a Participant under the Participation Agreement in its Relevant Capacity.

3 **COVENANT**

The New Participant covenants and agrees with the parties to the Participation Agreement (whether or original or by accession) that the New Participant will observe, perform and be bound by the provisions of the Participation Agreement as fully and in the same manner as if it were a party to the Participation Agreement, with the intent and to the effect that the New Participant will be deemed to be a Participant as from the date of this deed.

4 **NOTICES**

The notice details of the New Participant are as follows:

[*Notice details to be supplemented / amended as required.*]

[Participant name]	[Insert addressee full legal name]
	[Insert address]
	[Insert address]
	[Insert email]
	[Insert facsimile]

5 **COSTS**

The New Participant is responsible for all legal and other costs and expenses of and incidental to the preparation and execution of this deed and any stamp duty payable in connection with this deed.

6 **CONSIDERATION**

This deed is entered into in consideration of the parties to the Participation Agreement incurring obligations and giving rights and other valuable consideration.

7 **REPRESENTATIVES OF THE SAME LEGAL ENTITY**

(a) To the extent the New Participant is the same legal entity as one or more other Participants, the provisions of this deed and the Participation Agreement, as between those parties representing the same legal entity, take effect as a memorandum of understanding and are not legally binding.

(b) This clause 7 does not affect the binding nature of this deed and the Participation Agreement as between Participants that are distinct legal entities.

8 **GOVERNING LAW**

This deed is governed by the laws in force from time to time in the Australian Capital Territory.

EXECUTED as a deed poll.

[*Appropriate signature block for acceding party to be inserted.*]

SCHEDULE 2 NOTICE DETAILS

[Drafting note: notice details to be provided for each Participant. Additional names and contact details to be added / removed as required.]

The Commonwealth:	Commonwealth of Australia as represented by the Department of Home Affairs
	6 Chan Street Belconnen ACT 2617 Australia
	[Insert email]
	[Insert facsimile]
[Participant name]	[Insert addressee full legal name]
	[Insert address]
	[Insert address]
	[Insert email]
	[Insert facsimile]