Face Verification Service (FVS)
Access Policy
National Facial Biometric Matching Capability
CONTENTS

A. PURPOSE AND SCOPE ......................................................................................................................................1
B. DESCRIPTION OF THE FVS ..........................................................................................................................1
C. ACCESS CRITERIA .............................................................................................................................................2
  1. Legislative Compliance ..............................................................................................................................2
  2. Privacy Impact Assessments ......................................................................................................................2
  3. Interagency Data Sharing Arrangements ....................................................................................................2
  4. Scope of data sharing .................................................................................................................................3
  5. Protection and use of personal information ...............................................................................................3
  6. Management of Nominated Users ............................................................................................................4
  7. Training of Nominated Users ....................................................................................................................4
  8. Auditing and Accountability .......................................................................................................................4
  9. Security Accreditation .................................................................................................................................5
 10. Service MOUs with the Attorney-General’s Department ........................................................................5
 11. Transparency ...........................................................................................................................................5
D. GOVERNANCE FRAMEWORK FOR THE FVS ..............................................................................................6
E. THE ROLE OF THE COORDINATION GROUP .............................................................................................6
F. RESPONSIBILITY OF AGENCIES ....................................................................................................................6
G. THE ROLE OF THE ATTORNEY-GENERAL’S DEPARTMENT ........................................................................7
A. PURPOSE AND SCOPE

This policy sets out the requirements that Agencies must meet in order to gain and maintain access to the Face Verification Service (FVS).

B. DESCRIPTION OF THE FVS

The FVS is one of the Identity Matching Services provided by the National Facial Biometric Matching Capability ('the Capability').

The Capability adopts a 'hub-and-spoke' model which is comprised of a central interoperability hub ('the Hub') that acts as a router or exchange to facilitate information sharing between agencies on a query and response basis. The Capability is a secure, automated and auditable mechanism for the sharing and matching of facial images between government agencies for the purposes of identity fraud prevention, law enforcement, national security, community safety and service delivery, while maintaining strong privacy safeguards.

The FVS enables a facial image or biographic data associated with an individual to be compared, on a one-to-one basis, against an image and/or biographic data held on a specific government record associated with that same individual to help verify that person's identity.

The FVS is able to perform the following functions:

a) **Retrieve Biometric Request ('Retrieve')**: This function will allow a Nominated User of a Requesting Agency (an agency submitting queries via the FVS) to submit an Evidence of Identity (EOI) document type, EOI document number, and biographic details in the request, and return the facial image and biographic details associated with that document from the Data Holding Agency (an agency that is receiving and responding to a query via the FVS);

b) **Verify Match Request ('Match')**: This function will allow a Nominated User of a Requesting Agency to submit an EOI document type, EOI document number, a facial image, and biographic details for matching at a Data Holding Agency, and return a response indicating a match or no match (based on an agreed threshold) with the biometric data at the Data Holding Agency;

c) **Search Subject Request ('Search')**: This function will allow a Nominated User of a Requesting Agency to submit an EOI document type, a facial image and biographic details in the request and return the corresponding facial image and biographic details from the Data Holding Agency to confirm whether these match the person's record. If more than one corresponding record is found, the document with the highest matching image is returned.

Access to the Hub is initially made available to agencies via a web-based user interface (the Portal) that enables users to log in and manually enter search requests.
Over time, the Hub will also be able to receive requests via system-to-system connections with agencies’ existing systems, using industry standard integration technologies such as web services. It is anticipated that the bulk of transactions to the Hub will be from identity document issuing agencies that will be sending identity verification requests from their systems to the Hub using web services (System-to-system connections).

An administration facility for the FVS is provided through the Portal. This facility enables the ability to add, manage (including password reset, access support, and access re-authorisation) and remove Nominated Users who can access the FVS. It provides the ability for Agencies to generate reports, perform audit queries of Nominated User activities and download audit data.

C. ACCESS CRITERIA

Prior to the Attorney-General’s Department (AGD) granting access to the FVS, and in order to maintain that access, Agencies must comply with the following access criteria:

1. **Legislative Compliance**

   Agencies must provide a statement referencing legislation that demonstrates their legal basis for using and/or disclosing identity information via the FVS. This statement should form part of the Interagency Data Sharing Arrangements (IDSA) (see Criterion 3, below).

2. **Privacy Impact Assessments**

   Where an agency’s use of the FVS is not exempt from the relevant Commonwealth, State or Territory privacy laws, the agency must undertake or contribute to a privacy impact assessment (PIA) to account for every information flow that occurs through the FVS, to which the agencies are a party. PIAs must be undertaken prior to the finalisation of the relevant IDSA, and must consider the information sharing processes that are likely to occur under those IDSA. Agencies should refer to the Office of the Australian Information Commissioner’s (OAIC) guidelines in conducting PIAs. PIAs should be conducted independently unless it is not feasible to do so.

   Where an agency’s use of the FVS is exempt from the relevant Commonwealth or State and Territory Privacy laws, the agency must develop a privacy statement outlining the legislative, policy and other safeguards that apply to the handling of personal information to be obtained by the FVS. This privacy statement should be provided to the Data Holding Agency and AGD.

3. **Interagency Data Sharing Arrangements**

   Agencies must enter into an IDSA or equivalent with each agency with which it intends to share information via the FVS.

   Where possible, classes of agencies with like functions (such as state and territory police or road authorities) should enter into common, multilateral agreements to promote consistent information sharing and safeguards across jurisdictions.

   The provisions of an IDSA will be negotiated by the agencies involved, but must be informed by a PIA, must include the matters listed below and Access Criteria 4-9:
AGD maintains a template IDSA for use by agencies participating in the FVS that meets the requirements of this Access Policy. Agencies may use AGD’s template or modify their existing information or data sharing arrangements to fulfil all the requirements of this Access Policy.

4. **Scope of data sharing**

The Requesting and Data Holding Agencies should clearly understand the scope of the proposed data sharing under the FVS. For each data source that is to be accessed, Agencies must record in the IDSA:

- the type of identity information provided in response to FVS requests for each function and Data Source
- the characteristics (for example, security clearance (for persons) or accreditation (for systems) and/or training) relating to agreed categories of Nominated Users (Role Types) and access permissions associated with each Role Type
- the maximum number of Nominated Users for each data source and each Role Type
- the method of access to the FVS for each Role Type (e.g. through the Hub Portal, or via a system-to-system connection), and
- the agreed maximum number of transactions, expressed in terms of total estimated transactions annually, and estimated peak transaction rates per month (or other agreed time period).

This information must be provided to AGD in a format that enables implementation of the agreed data sharing via the Interoperability Hub. Any changes to the matters above should be notified to the Data Holding and Requesting Agencies as soon as practicable. Such changes will also require a variation of the IDSA, a copy of which must be provided to AGD.

5. **Protection and use of personal information**

Agencies must record in an IDSA the arrangements for the protection of personal information that will be shared via the FVS, including:

- arrangements for the retention and destruction of any images or other identity information obtained via the FVS, and
- the circumstances where any release of identity information to third parties may occur, if at all.

Requesting Agencies must acknowledge that the FVS is designed to assist, but not replace, existing processes and procedures for verifying a person’s identity and that Requesting Agencies are
responsible for the information they access through the FVS and decisions they make using identity information or results obtained through the FVS.

6. **Management of Nominated Users**

Only Nominated Users may submit queries via the FVS. 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. Any information technology (IT) system that the 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. In both cases, the level of access must be commensurate with the requirements of those functions and activities.

The addition and removal of Nominated Users will occur through the Administration facility. Agencies should record and advise each other of the person who is responsible for managing Nominated Users and ensuring compliance with the requirements of this Access Policy relating to Nominated Users in their agency.

Requesting Agencies must maintain a register of Nominated Users for oversight and auditing purposes. The register must not be made publicly available. Requesting Agencies must reconfirm the basis for each of their Nominated Users to access the FVS every 180 days.

Once a Nominated User no longer requires access to the FVS, agencies must take reasonable steps to advise AGD and ensure that their access to the service is terminated.

7. **Training of Nominated Users**

Nominated Users will undertake training in security awareness and privacy obligations (this may already occur as part of their ongoing employment). To gain access to the FVS, Nominated Users must be trained in how to use the Interoperability Hub and its portal interface, including how to interpret the results of the FVS. Common training materials relating to the Interoperability Hub will be developed and maintained by AGD and made available for these purposes.

8. **Auditing and Accountability**

A Requesting Agency must audit all of its data sharing via the FVS at least once every financial year. These audits should be conducted independently, unless it is not feasible to do so, and should be conducted to the satisfaction of each Data Holding Agency to which the Requesting Agency has conducted transactions. The Requesting Agency should be responsible for its own audit costs.

Requesting Agencies must retain all necessary information to support audits of their use of the FVS. These information holdings should provide the ability to:

- identify the time, purpose and Nominated User associated with each transaction
- track the handling of any identity information provided as part of a transaction response, including whether the Agency stored or destroyed the identity information
- track the handling of any identity information provided as part of a transaction response, including whether and when the Agency stored or destroyed the identity information
- detect anomalous or potentially suspicious transactions or patterns of transactions, and
some of this information may need to be obtained from the Data Holding Agency.

- identify any complaints and review responses to them.

9. **Security Accreditation**

Agencies must ensure that any IT systems that are Nominated Users or otherwise connected to the Hub receive and maintain appropriate security accreditation, in accordance with the requirements of the Australian Government *Protective Security Policy Framework* and *Information Security Manual*.

Agencies must provide ICT Accreditation certificates to each other. Security accreditation must be informed by a Security Risk Management Plan (SRMP) which is regularly updated. The SRMP must be prepared in accordance with the Protective Security Policy Framework, and a copy of the SRMP and ICT Accreditation must be provided to AGD.

10. **Service MOUs with the Attorney-General’s Department**

Agencies participating in the FVS must enter into a memorandum of understanding (MOU) with AGD in relation to the services through the Interoperability Hub. Service MOUs will outline the level of service that AGD agrees to provide to the Agency, and the terms and conditions on which that service will be provided. Contents of the Schedules to the Service MOUs will be subject to negotiation between the agencies and AGD and must be consistent with this Access Policy.

Where an agency participates in both the FVS and FIS, AGD will seek to enter into a single consolidated Service MOU.

11. **Transparency**

Agencies must ensure that information relating to their participation in the FVS is made publicly available. This should include publication of PIAs, IDSAs and statements of legislative compliance.

This should include the publication of PIAs and details of legislative compliance and may also include IDSAs where such publishing is practical for agencies. In the event that an Agency does not publish these documents in full for security or other reasons, they should be published or made available upon request to the greatest extent possible. AGD maintains a public register listing the above documents and provides a link on its website to where Agencies have published documents or their descriptions.

Where an agency is not subject to Commonwealth, state or territory freedom of information laws, they are exempt from the requirement to publish documents under this Access Policy.

AGD will publish, on an annual basis, information on the usage of the FVS to enable the community to gain a broad understanding of the scope and volume of FVS use across agencies. This information will include:

- the agencies that have been granted access to the FVS; and
- the number of instances that each agency requested information via the FVS.

Any use of the FVS by agencies of the Australian Intelligence Community will not be included in this reporting in order to protect those agencies’ operations.
D. **GOVERNANCE FRAMEWORK FOR THE FVS**

Ministerial responsibility for the Capability, including the FVS, is intended to rest with the Law Crime and Community Safety Council (LCCSC). The National Identity Security Coordination Group (the Coordination Group) is intended to be the officials-level body accountable to the LCCSC for the efficient and effective delivery and management of the FVS. Until the NISCG has assumed its biometric governance responsibilities, the Programme Advisory Committee (PAC) fulfils the intended functions of the Coordination Group.

The Coordination Group will put in place advisory and consultation mechanisms to ensure its considerations are appropriately informed by the views of relevant stakeholder organisations.

This Access Policy has been informed by an initial, independent privacy impact assessment on the design and governance of the Hub, commissioned by AGD.

E. **THE ROLE OF THE COORDINATION GROUP**

As the body accountable to the LCCSC for the effective management of the Capability, the Coordination Group is responsible for developing policy and procedures to support the operation of the FVS. It is also responsible for monitoring Agencies’ compliance with these policies and for taking appropriate action to address any non-compliance.

The Coordination Group monitors and reviews the operation of this policy and any supporting guidelines or procedures, updating them as required to help ensure that information sharing via the FVS continues to meet the objectives of all participants.

F. **RESPONSIBILITY OF AGENCIES**

Agencies sharing information via the FVS have the primary responsibility for ensuring that their participation in the service is conducted in accordance with this Access Policy.

It is the responsibility of the Agencies sharing information via the FVS to ensure that their PIAs, and IDSAs (or equivalent) fulfil the Access Criteria. Agencies are also responsible for developing business systems and processes to implement Access Criteria 6-9, including for identifying and promptly addressing any suspected or actual non-compliance.

Agencies are responsible for ensuring that any IDSAs they enter into with another agency is consistent with the Access Policy, that they take steps to address any audit or compliance issues and ensure they have adequate privacy safeguards in place for the use of FVS.

It is the responsibility of agencies sharing information via the FVS to ensure they provide the agency with which they have entered into a data sharing agreement, any information that is necessary for them to fulfil the Access Criteria.
G. THE ROLE OF THE ATTORNEY-GENERAL’S DEPARTMENT

As the overall lead agency for development and implementation of the Capability, AGD manages the Hub which supports the FVS and provides Secretariat support to the Coordination Group.

In this capacity AGD is responsible for:

a. reviewing IDSAs entered into by participating agencies in order to be satisfied that they are consistent with this Access Policy and making recommendations to the Coordination Group as required;

b. reviewing audit and compliance reports to identify the potential need for compliance action, making recommendations to the Coordination Group as required; and

c. making recommendations to the Coordination Group for changes to this Access Policy to ensure the effective governance and operation of the FVS.

AGD is not responsible for endorsing the content of PIAs or for negotiating IDSAs between participating agencies.

AGD retains discretion not to provide an agency with access to the FVS, or to suspend or terminate its access to the FVS. AGD can suspend or terminate an Agency if requested to do so by the Coordination Group (or the PAC in the interim), a Data Holding Agency, or if it considers on reasonable grounds that an Agency has, or may adversely affect, the security, privacy, reputation, stability or integrity of the FVS or the operations of a Data Holding Agency.

This discretion is exercised in accordance with any procedures developed and maintained by the Coordination Group (or the PAC in the interim). For example, this discretion may be exercised upon receipt of a complaint from a privacy regulator or oversight body, upon a request from an Agency from which information is provided, or based on adverse findings from audits conducted in accordance with this Access Policy.