Face Identification Service (FIS) Access Policy

Identity Matching Services

IDENTITY SECURITY

Contents

FACE IDENTIFICATION SERVICE ACCESS POLICY

PART 1 - PURPOSE

1.1 This policy sets out the conditions that Participating Agencies must comply with to gain and maintain access to the Face Identification Service (FIS).

1.2 [This policy has been developed pursuant to section 7H of the *Identity-matching Services Act 20XX* (Cth) (the IMS Act).]

1.3 This policy supports the *Intergovernmental Agreement on Identity Matching Services* (IGA) and the Face Matching Services (FMS) Participation Agreement. If there is an inconsistency between this policy and those agreements [or the IMS Act], those agreements [and/or the IMS Act] prevail to the extent of the inconsistency.

PART 2 - DESCRIPTION OF THE FIS

2.1 The FIS is one of the Face Matching Services provided for by the IGA and governed by the IMS Act.

2.2 The FMS are provided via a 'hub-and-spoke' model, which is comprised of a central interoperability Hub (the Hub). This is a technical system that provides a mechanism for the secure and auditable matching of facial images and associated identification information from different government data sources, in accordance with the FMS Participation Agreement (FMS PA), between Participants.

2.3 The FIS enables a facial image to be compared on a one-to-many basis against images held in government records to help determine the identity of that individual, or to detect instances where an individual holds multiple, potentially fraudulent identities.

2.4 The FIS requires the Requesting Agency to submit a query containing a single facial image, demographic details (such as age range and gender) and query authorisation details (such as purpose, authorising legislation and an internal reference number).

2.5 The response from a Data Holding Agency contains a gallery of the highest matching images, as determined by the facial recognition system used by the Data Holding Agency (based on a pre-configured match threshold). The size of the image gallery is determined by the Data Holding Agency and will not normally exceed 20 images.

2.6 The biographic details associated with the images will only be released to the Requesting Agency once the user selects or shortlists from the gallery image(s) they wish to examine. The number of images that can be shortlisted from a gallery is determined by the Data Holding Agency.

2.7 The Requesting Agency is responsible for reviewing the image gallery to assist in resolving the identity of the person who was the subject of the request.

2.8 Access to the FIS is made available to Participating Agencies via a web-based user interface (the Portal) to the Hub that enables users to log in and manually enter queries.

2.9 An administration facility for the FIS is provided through the Portal. It provides the ability for Participants to generate reports, perform audits of user activities and query audit data.

PART 3 - ACCESS PRINCIPLES

3.1 The following access principles underpin the design and operation of the FIS.

a) Promote privacy and compliance with legal provisions

Provision of the FIS by the Hub Controller requires confidence to be maintained that Participating Agencies are exchanging information consistent with their legal basis for data sharing, and that anticipated impacts on the privacy of individuals are outweighed by the public benefit of the service. This dictates the way in which permitted uses are framed, and how supervision and endorsing requirements, and other access controls, are applied.

b) Protect shielded persons

Continuing provision of the FIS by the Hub Controller is dependent on effective measures being in place to protect persons with legally assumed identities and other shielded persons. This dictates the way in which access controls and authorisation requirements are applied, and audit data is managed.

c) Proportionate functionality

The FIS cannot be used for live facial recognition or real time monitoring of public places, sometimes referred to as 'mass surveillance'. Closed Circuit Television (CCTV) cameras or other types of live video feeds cannot be used as data inputs to the FIS – only single facial images can be included in an FIS query. Likewise, FIS queries must not be made for the dominant purpose of preventing or interfering with lawful advocacy, protest, dissent or industrial action, or identifying an individual merely because the individual is (or was) in a public place.

d) Non-evidentiary system

The FIS is not designed as an evidentiary system and the results of FIS queries must not be relied upon as the sole basis for ascertaining a person's identity in criminal or civil proceedings. Requesting Agencies seeking to use FIS results to help identify a person for evidentiary purposes must confirm the accuracy of the information through other channels or processes. Data Holding Agencies are not responsible for decisions made by a Requesting Agency because of their use of the FIS.

e) Information Sharing

Data Holding Agencies should allow Requesting Agencies to access information via the FIS to the maximum extent permitted by law and in accordance with these principles. The details of the disclosure will be agreed between the Data Holding Agency and the Requesting

Agency in accordance with the Face Matching Services Participation Agreement (PA) and the Face Matching Services Participant Access Arrangement (PAA).

f) Risk-Based Access Controls

The FIS has a range of access controls which are based on a risk-management approach that balances ***privacy*** and ***security*** safeguards, with ***usability*** and ***timeliness*** of the service for its users, so that the benefits of facial matching may be realised. These include, for example, a requirement that all FIS requests are endorsed by a senior manager, controlled access to biographic information, and limiting use of the FIS to certain permitted activities.

g) Approved Agencies

Access to the FIS is restricted to agencies with law enforcement or national security related functions [as per section 8A(1) of the IMS Act]. While a Requesting Agency may be listed in the IMS Act, each Data Holding Agency retains discretion as to whether to approve a Participant Access Arrangement of a Requesting Agency.

h) Permitted Purposes

Participating Agencies may only access the FIS for certain permitted activities which relate to an identity or community protection activity. These permitted activities are set out in Section 6 of the IMS Act and are replicated in Part 4 of this policy. Individual Data Holding Agencies may choose to limit their provision of the FIS to a subset of these activities.

i) Approved FIS Users

Within agencies approved to access the FIS, access must be limited to specific Approved FIS Users appointed either by the head of the Requesting Agency or their delegate. Approved FIS Users are persons who: perform specialist investigative, intelligence, incident response, forensic, or protective security functions warranting use of the service; meet minimum security clearance requirements; and are sufficiently trained in facial comparison and other relevant areas to ensure privacy-respecting, efficient and effective use of the capabilities within the system.

j) Endorsing Officers

FIS requests made by Approved FIS Users must be endorsed by the head of the Requesting Agency, or their delegate who is the holder of management office or position. The seniority of the Endorsing Officer reflects the importance placed on FIS requests and the responsibility of the Requesting Agency to ensure that requests are only submitted for a permitted activity.

k) Controlled Access to Biographic Information

The FIS is designed to limit access to biographic information, such as the name and date of birth, of persons who are not the subject of the query. To help maintain the anonymity of these individuals, biographic information will only be made available after the FIS user shortlists an image from the return gallery.

l) Controlled Download and Export of returned images

Data Holding Agencies maintain the right to impose conditions under which Requesting Agencies may download, export or copy images returned in responses to an FIS query. Images must not be exported or copied by means other than the approved download function. The Requesting Agency will be responsible and will be held accountable for securely managing any images downloaded through the FIS.

m) Auditing to ensure compliance and enable risk management

Transaction information will be captured by the Hub to support audits of Requesting Agencies for compliance purposes.

PART 4 - PERMITTED ACTIVITIES

4.1 Participants may only access the FIS for one or more of the following identity or community protection activities:

a) Preventing and Detecting Identity Fraud

The prevention and detection of identity fraud (including use of stolen or fraudulently obtained government identification documents or identification information from such documents).

b) Law Enforcement activities

(i) The prevention, detection, investigation and prosecution of an offence against a law of the Commonwealth, or of a State and/or Territory, including:

a. murder (however described);

b. kidnapping (however described);

c. an act or acts of terrorism;

d. other serious offences punishable by not less than three years or for life imprisonment, including but not limited to:

i. Offences causing harm to person

ii. Harassment and other offences against the person

iii. Theft and related offences

iv. Non-Identity Fraud and Financial Crime

v. Illicit drug offences

vi. Prohibited and regulated weapons and explosives offences

vii. Property damage and environmental pollution

viii. People Smuggling and People Trafficking

ix. Riot and Affray.

(ii) Starting, conducting, or deciding whether to start or continue, proceedings under the *Proceeds of Crime Act 2002* or a corresponding law within the meaning of that Act.

Note: The scope of the law enforcement activity does not limit the ability of states and territories to share identity information between Participants within the same jurisdiction. This will be managed through the PAAs.

c) National Security activities
Conducting investigations or gathering intelligence relevant to Australia's national security, (within the meaning of the *National Security Information (Criminal and Civil Proceedings) Act 2004*).

d) Protective Security activities
Activities to promote the security of agency assets, facilities or personnel associated with government, including but not limited to:

(i) protecting a shielded person or someone else associated with such a person ; or

(ii) checking the security or criminal background of a person with access to such an asset or facility.

e) Community Safety
Activities to identify an individual:

(i) who has suffered, or is reasonably believed to be at risk of suffering, physical harm, including an individual who:

a. has been reported as missing, or

b. has died or is reasonably believed to have died, or

c. is affected, or is reasonably believed have been affected, by disaster, or

(ii) who is reasonably believed to be involved with a significant risk to public health or safety.

Requests relating to 'other serious offences'

4.2 The permitted activity of law enforcement outlines the categories of offences for which it is anticipated that most FIS queries will be conducted. This is not intended to exclude FIS queries for other types of offences, if they meet or exceed the minimum penalty threshold.

Requests to identify witnesses to a crime

4.3 FIS queries may only be conducted to identify a witness to a criminal offence where:

a) the offence is an offence punishable by not less than three years or for life imprisonment (as per Part 4 above); and

b) the person who is subject of the query is 18 years of age or older.

Requests for community safety activities

4.4 The activity of community safety recognises that there may be circumstances which warrant use of the FIS to help prevent harm to an individual or the broader community, but which do not involve serious offences.

4.5 FIS queries conducted for the activity of community safety must not be requested for the dominant purpose of identifying individuals merely because they were in a public place, or preventing or interfering with lawful advocacy, protest, dissent or industrial action

4.6 If there are reasonable grounds to suspect that an offence that is punishable by not less than three years imprisonment has been committed, or is likely to be committed imminently, in connection to such activities, and where it is reasonably necessary to use the FIS, the query should be conducted using the general law enforcement purpose, specifying the category of offence involved.

Requests returning larger image galleries

4.7 To manage privacy and security risks associated with potential misuse of the FIS, responses to FIS queries are normally limited to a maximum of the 20 highest matching images.

4.8 In limited circumstances, where the Approved FIS User has access privileges to do so and authorisation for the query has been provided, they may receive an additional number of those records with images that exceed the matching threshold. However, this would need to be agreed with the Data Holding Agencies and reflected in the PAA.

4.9 Data Holding Agencies may restrict the provision of larger image galleries to queries conducted for certain permitted purposes, or to certain categories of criminal offences within the general law enforcement purpose.

Requests involving persons under the age of 18 years

4.10 FIS queries where the Approved FIS User suspects the subject of the FIS query is under 18 may only be conducted where:

a) the query relates to a victim in relation to any of the permitted purposes in Part 4, or to a person who is otherwise at risk of harm, or has suffered harm; or

b) the query relates to a person of interest in relation to:

(i) an offence under the general law enforcement purpose, other than terrorism offences, in which case images of persons aged 14 years or over may be returned, or

(ii) a terrorism offence or national security investigation, in which case images of persons aged 10 years or over may be returned.

4.11 Agencies must ensure they have adequate safeguards and policies in place that will address any risks associated with matching the images of minors.

PART 5 - APPROVAL OF ACCESS AND ENDORSEMENT OF REQUESTS

Approving Officers and Approved FIS Users

5.1 An Approved FIS User must be nominated as a suitable person to make an FIS request by an Approving Officer. An Approving Officer must be:

(i) the head (however described) of the Participating Agency; or

(ii) a person who:

a. holds a management office, position or rank within a Participant's organisation that is either;

i. in the case of a Participant that is a police agency, is a rank equivalent to or higher than 'Inspector' or an unsworn position that is required to perform a supervisory role pursuant to current respective police force oversight arrangements; or

ii. in the case of all other Participants, a position equivalent to, or higher than, 'Executive Level 2' as defined in the *Public Service Classification Rules 2000* (Cth); or

iii. an appropriate management office, position or rank approved in writing by the Hub Controller;

b. has been authorised, by notice in writing to the Hub Controller, by the head (however described) of the Participant to approve users to submit FIS Queries on behalf of the Participant; and

c. is senior to the person making the request.

5.2 Approving Officers cannot approve their own access to the FIS.

Endorsing Officers

5.3 All FIS requests submitted by an Approved FIS User must be endorsed by an Endorsing Officer.

5.4 An Endorsing Officer must be:

(i) the head (however described) of the Participating Agency; or

(ii) a person who:

a. holds a management office, position or rank within a Participant's organisation that is either;

i. in the case of a Participant that is a police agency, is a rank equivalent to or higher than 'Inspector' or an unsworn position that is required to perform a supervisory role pursuant to current respective police force oversight arrangements; or

ii. in the case of all other Participants, a position equivalent to, or higher than, 'Executive Level 2' as defined in the *Public Service Classification Rules 2000* (Cth); or

iii. an appropriate management office, position or rank approved in writing by the Hub Controller;

b. has been authorised, by notice in writing to the Hub Controller, by the head (however described) of the Participant to endorse FIS Queries to be submitted on behalf of the Participant; and

c. is senior to the person making the request.

5.5 It is the responsibility of Endorsing Officers to be satisfied that the FIS requests that they endorse are:

(i) made for the purposes of:
   a. the identity or community protection activity stated in the request; and
   b. the performance of the Requesting Agency's functions; and

(ii) is not made for the dominant purpose of:
   a. preventing or interfering with lawful advocacy, protest, dissent or industrial action; or
   b. identifying an individual merely because the individual is or was in a public place.

5.6 Where an Endorsing Officer is also an Approved FIS User, they cannot endorse their own request.

5.7 Endorsing Officers are responsible for acting to address any unauthorised use by the Approved FIS Users under their supervision.

5.8 Endorsing Officers are provided with access to a summary of the queries conducted by Approved FIS Users under their supervision. The Endorsing Officer (or their delegate) is responsible for reviewing this information, on a routine basis, to ensure compliance with these requirements.

PART 6 - ACCESS CRITERIA

6.1 Prior to the Hub Controller granting access to the FIS and to maintain access to the FIS, agencies must comply with the following access criteria:

FMS Participation Agreement and Participant Access Arrangements

6.2 Agencies must enter into the common FMS Participation Agreement (PA) to become Participants in the FIS.

6.3 Participants must also complete a Participant Access Arrangement (PAA) which forms part of the PA. Each Participant's PAA outlines the specific types of information to be made available or accessed via the FIS. Contents of the Participant Access Arrangement will be subject to negotiation between the relevant Participants and the Hub Controller, and must be consistent with this Access Policy.

6.4 The Hub Controller maintains a template PAA for use by Participants that meets the requirements of this Access Policy. The Hub Controller must also maintain a register of all completed PAAs.

6.5 The Hub Controller also maintains the FMS Catalogue, which provides precise details of the information each Data Holding Agency agrees to provide through its PAA, and the level of service that the Hub Controller agrees to provide the Participants.

Legislative Authority

6.6 Participants must provide a statement referencing the legislation that provides their legal basis for collecting, using and disclosing personal information via the FIS. This statement should form part of the Participant's PAA.

Privacy Impact Assessments

6.7 Each Requesting Agency must undertake or contribute to a privacy impact assessment (PIA) conducted in accordance with the Office of the Australian Information Commissioner's Guide to Undertaking Privacy Impact Assessments.

6.8 A PIA is 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. It will identify any impacts on the privacy of individuals, and make recommendations for managing, minimising or eliminating any impacts identified.

6.9 The PIA must map the information flows that occur through the Participant's use of the FIS. PIAs must be undertaken prior to the finalisation of the PAA and must consider the information sharing processes that are likely to occur under the PAA. Participants 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.

6.10 The PIA requirement in paragraph 6.7 does not apply where a Requesting Agency's use of the FIS is exempt from the relevant Commonwealth or State and Territory privacy laws. These agencies must develop a privacy statement outlining the legislative, policy and other safeguards that apply to the handling of personal information to be obtained using the FIS. This privacy statement should be provided to the Data Holding Agency and the Hub Controller.

Scope of data sharing

6.11 Participants should clearly understand the scope of the proposed data sharing via the FIS. For each data source that is to be accessed, Participants must record in their PAA the details of information to be shared as recorded in the FMS Catalogue including:

a) the type of information provided in response to FIS requests for each function and data source, including:

   (i) the number of images that may be returned in responses to standard requests (up to a maximum of 20); and

   (ii) the maximum number of images that may be shortlisted, to disclose biographic details, when reviewing image galleries.

b) the permitted activity (under Part 4) for which FIS requests can be submitted

c) the characteristics (for example, security clearance and/or training) relating to agreed categories of Approved FIS Users (Role Types) and access permissions associated with each Role Type

d) the maximum number of Approved FIS Users for each data source and each Role Type (Requesting Agencies PAA only)

e) 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) (Requesting Agencies PAA only);

f) the application of authorisation requirements, including:

(i) the Role Types, if any, to have access privileges to receive larger galleries and/or download images.

6.12 This information must be provided to the Hub Controller in a format that enables implementation of the agreed data sharing via the 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 an update to the PAA and/or FMS Catalogue, a copy of which must be retained by the Hub Controller.

Protection and use of personal information

6.13 Participants must have in place arrangements for the protection of personal information that will be shared via the FIS, including:

a) arrangements for the retention and destruction of any images or other identity information obtained via the FIS, and

b) the circumstances where any disclosure of identification information received through a match request may occur, if at all.

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

Management of Approved FIS Users and Endorsing Officers

6.15 Only Approved FIS Users may submit queries via the FIS. Requesting Agencies must ensure that they only appoint as Approved FIS Users employees who have a specialist investigative, intelligence, incident response, forensic, or operational security function and who have a reasonable need to access the FIS to perform their functions and activities with the agency. The level of FIS access must be commensurate with the requirements of their functions and activities.

6.16 Approved FIS Users must have an appropriate security clearance of:

a) for Australian Government personnel, Baseline clearance or higher; or

b) for state and territory personnel an equivalent clearance consistent with the Australian Government Personnel Security Protocol of the Australian Government Protective Security Policy Framework, Baseline clearance requirements, as approved by the Governing Body.

6.17 Exceptions may be made to the security clearance requirements for certain, limited number of staff in Data Holding Agencies providing technical support.

6.18 Endorsing Officers are provided with access to the Portal to assist in fulfilling their obligations under this Access Policy. The addition and removal of access for Endorsing Officers is managed by the Hub Controller, as advised by the head of the Requesting Agency (or their delegate).

6.19 Approved FIS Users will be assigned access to the Portal by the Hub Controller, as advised in writing to the Hub Controller by the head of the Requesting Agency (or their delegate). Once assigned, the addition and removal of FIS access to Approved FIS Users is managed by a dedicated Client Administrator in each Requesting Agency, overseen by a Senior Client Administrator.

6.20 Requesting Agencies must maintain a register of Approved FIS Users and Endorsing Officers for oversight and auditing purposes. Subject to any overriding legislative obligations, the register must not be made publicly available. Requesting Agencies must reconfirm the basis for each of their Approved FIS Users to access the FIS at 90-day intervals and Endorsing Officers to access the FIS at 180 day intervals.

6.21 Once an Approved FIS User or Endorsing Officer no longer requires access to the FIS, Requesting Agencies must take reasonable steps to advise the Hub Controller and ensure that their access to the service is terminated.

Training of Approved FIS Users and Endorsing Officers

6.22 Approved FIS Users and Endorsing Officers must be trained in security awareness and privacy obligations (this may already occur as part of their ongoing employment). To gain access to the FIS, Approved FIS Users and Endorsing Officers must be trained in how to use the Portal, including how to interpret the results of the FIS. Common training materials relating to the Hub are developed and maintained by the Hub Controller and made available for these purposes.

6.23 Approved FIS Users must undergo facial recognition and image comparison training in accordance with the Face Matching Services Training Policy.

6.24 It is the responsibility of the Requesting Agency to ensure:

a) Approved FIS Users are appropriately trained to interpret FIS results and to provide assurances to this effect to the satisfaction of Hub Controller. Where necessary, Data Holding Agencies may specify additional training requirements in PAAs.

b) Endorsing Officers are appropriately trained in the proper execution of their duties.

Auditing and Accountability

6.25 A Requesting Agency must audit all its data sharing via the FIS at least once every financial year. These audits should be conducted by an independent auditor, or a business unit of the Requesting Agency that is functionally separate to any business unit using the service. The audit should be conducted to the satisfaction of each Data Holding Agency that the Requesting Agency has used. The Requesting Agency is responsible for its own audit costs.

6.26 Without limiting the scope of the audit, the audit report should examine the queries relating to the permitted purpose of community safety considering the greater privacy risk and whether authorisation was obtained for those circumstances that required authorisation.

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

a) identify the time, Approved FIS User, purpose, internal reference number, and (where relevant) authorisation associated with each transaction;

    a. this information is available in the audit logs via the Portal;

b) demonstrate compliance with Approved FIS User access requirements;

c) demonstrate compliance with authorisation requirements

d) examine queries relating to the permitted purpose of community safety;

e) track the handling of any identity information provided as part of a transaction response, including whether and when the Participant stored or destroyed the identity information;

f) detect anomalous or potentially suspicious transactions or patterns of transactions;

    a. some of this information may need to be obtained from the Data Holding Agency; and

g) identify any complaints and review responses to them.

Security Accreditation

6.28 All Requesting Agencies must conduct a security risk assessment in a format that is approved by their internal information technology security adviser (or equivalent). A copy of the assessment, redacted if necessary, must be provided to the Hub Controller.

Transparency

6.29 Participants must ensure that information relating to their participation in the FIS is made publicly available.

6.30 This should include the publication of PIAs and details of legislative authority and may also include the PA where such publishing is practical for Participants. If a Participant 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. The Hub Controller maintains a public register listing the above documents and provides a link on its website to where Participants have published documents or their descriptions.

Where a Participant is not subject to Commonwealth, state or territory freedom of information laws, they are not required to publish documents under this Access Policy.

6.31 The Hub Controller will publish, on an annual basis, information on the usage of the FIS to enable the community to gain a broad understanding of the scope and volume of FIS use across Agencies. This information will include:

a) the Agencies that have made requests for access to the FIS

b) the number of instances that each Participating Agency requested information via the FIS, and

c) the number of those instances where the Participant received a response containing information in a government identification document, or confirmation of a person's identity.

6.32 Any use of the FIS by the Australian Security Intelligence Organisation and Australian Secret Intelligence Service will be reported separately to protect their operations.

PART 7 - GOVERNANCE FRAMEWORK FOR THE FIS

7.1 In accordance with the IGA, Ministerial responsibility for the FMS (including the FIS) sits with the Ministerial Council for Police and Emergency Management (MCPEM). The National Identity Security Coordination Group (the Coordination Group) is the officials-level body accountable to the MCPEM for the efficient and effective delivery and management of the FIS.

7.2 The Coordination Group is responsible for developing policy and procedures to support the operation of the FIS. It is also responsible for monitoring Participating Agencies' compliance with these policies and for taking appropriate action to address any non-compliance. The Coordination Group has in place advisory and consultation mechanisms to ensure its considerations are appropriately informed by the views of relevant stakeholder organisations.

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

7.4 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 FIS continues to meet the objectives of all participants.

PART 8 - RESPONSIBILITY OF PARTICIPANTS

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

8.2 It is the responsibility of the Participants sharing information via the FIS to ensure that their PIAs and the PAAs fulfil the Access Criteria. Participants are also responsible for developing business systems and processes to implement Access Criteria 6.12-6.27 including for identifying and promptly addressing any suspected or actual non-compliance.

8.3 Participants are responsible for ensuring that their PAAs and details in the FMS Catalogue are 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 FIS.

8.4 It is the responsibility of Participants sharing information via the FIS to ensure they provide the relevant Participant with which they have entered into a Participant Access Arrangement, any information that is necessary for them to fulfil the Access Criteria.

8.5 Participants are also required to provide the Hub Controller with information about security incidents, including data breaches, occurring in connection with their use of the FIS.

PART 9 - THE ROLE OF THE HUB CONTROLLER

9.1 The Hub Controller manages the Hub which supports the FIS and provides Secretariat support to the Coordination Group. In this capacity the Hub Controller is responsible for:

a) reviewing, coordinating and (if necessary) signing the PAAs entered into by Participating Agencies in order to be satisfied that they are consistent with this Access Policy;

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 FIS.

9.2 The Hub Controller is not responsible for endorsing the content of PIAs conducted on behalf Participating Agencies.

9.3 The Hub Controller retains discretion to determine the technical design of the FIS, including the Portal, while ensuring it remains consistent with the Principles and Access Criteria outlined in this policy. In doing so, the Hub Controller will consult closely with relevant Data Holding and Requesting Agencies with a view to reaching consensus agreement where possible.

9.4 The Hub Controller may exercise the discretion not to facilitate or modify or suspend the sharing of information between Participants via the FIS. This discretion is exercised in accordance with the FMS Compliance Policy and the FMS Participation Agreement developed and maintained by the Coordination Group.

9.5 The Hub Controller is obliged to inform the Australian Information Commissioner of breaches of security that are reported to the Hub Controller, including whether it is a data breach that is reasonably likely to result in serious harm to an individual whose identification information is involved in the breach.