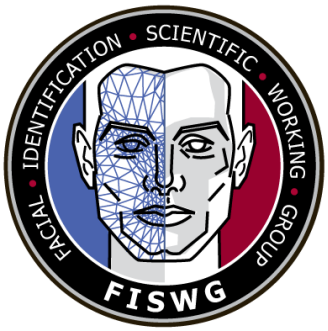

Disclaimer:

As a condition to the use of this document and the information contained herein, the Facial Identification Scientific Working Group (FISWG) requests notification by e-mail before or contemporaneously to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative, or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any foreign country. Such notification shall include: 1) the formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in a formal proceeding, it is requested that FISWG be notified as to its use and the outcome of the proceeding. Notifications should be sent to: chair@fiswg.org

Redistribution Policy:

FISWG grants permission for redistribution and use of all publicly posted documents created by FISWG, provided that the following conditions are met:

Redistributions of documents, or parts of documents, must retain the FISWG cover page containing the disclaimer.

Neither the name of FISWG, nor the names of its contributors, may be used to endorse or promote products derived from its documents.

Any reference or quote from a FISWG document must include the version number (or creation date) of the document and mention if the document is in a draft status.

Principles for Responsible Use of Facial Recognition Technology

1. Scope

1.1 The scope of this document is to provide a set of principles that FRS administrators, developers, integrators, managers, and users can adopt, which will help ensure that facial recognition technology is used in a consistent and responsible manner.

1.2 These principles were written with the understanding that FISWG documents are leveraged across the globe. As such, these principles are written in a way that ensures that they can be adopted regardless of geographical location.

1.3 These principles are based on subject matter that is important to FISWG. As such, these principles may not be all encompassing. Agencies are encouraged to seek additional guiding documentation as needed.

2. Referenced Documents

2.1 Various FISWG documents, which can be found here:

https://www.fiswg.org/documents.html

3. Terminology

3.1 *Definitions:*

3.1.1 *agency*–Within this document, an agency will refer to the organization responsible for the FRS.

3.1.2 *user*–Within this document, a user will utilize or support the FRS.

3.2 *Acronyms:*

3.2.1 *FRS-Facial Recognition System*

4. Purpose

4.1 This document details a set of principles to support agencies using facial recognition technology in a consistent and responsible way.

4.2 The intended audience is:

- Agencies that are interested in facial recognition technology
- Facial recognition technology stakeholders, such as, but not limited to, system owners, users, administrators, developers, and integrators

5. Significance and Use

5.1 FISWG creates documentation to support agencies in their development, deployment, management, and use of facial recognition technology.

5.2 FISWG acknowledges that more supporting and guiding documentation is needed to help agencies use the technology in a responsible manner.

5.3 This document is a summary of key principles that will help ensure that agencies are using the technology in a responsible way.

5.4 This technology is critical for many use cases and is becoming more widespread throughout the world. Adopting these principles will help ensure that the continued use and expansion of this technology is well supported.

6. Principles

6.1 Policy

6.2 Facial recognition technology should be developed, deployed, managed, and used in a way that respects relevant legislation, regulations, policies, and best practices.

6.3 Procedures

6.4 Agencies should develop detailed procedures that dictate how facial recognition technology should be used, including acknowledgement of limitations. Procedures should cover the end-to-end facial recognition process that is specific to the agency.

6.5 Standards Participation

6.6 Agencies should be encouraged to participate in international standards development by joining groups such as FISWG. Participation in these types of groups

gives agencies a voice in the community and allows them to help shape documentation that provides structure and consistency to the use of the technology.

6.7 Risks

6.8 Agencies should have a good understanding of the risks associated with developing, deploying, managing, and using facial recognition technology. Agencies should document, monitor, and manage risks on an ongoing basis. A risk management strategy should include aligning with the principles found in this document.

6.9 Security

6.10 Images and biometric templates should be adequately protected during all stages of the information life cycle: collection, use, disclosure, retention, storage, and disposal. They should be treated with a high level of sensitivity, including appropriate safeguards.

6.11 Training

6.12 Agencies that use facial recognition technology must ensure that system users and administrators are well trained in their designated role.

6.13 Data Quality

6.14 Research demonstrates that data/image quality can impact the performance of facial recognition technology. As such, agencies should be aware of the quality of their

data and should consider monitoring data/image quality on a regular basis to ensure that system performance is maintained at an optimal level.

6.15 Testing

6.16 Agencies should have a thorough understanding of how their respective facial recognition technology/systems perform in general and across demographics that are specific to the agency. Testing should include assessment of system robustness to threats that can compromise integrity. Agencies should reference NIST testing results as benchmark and conduct testing on operationally relevant data through their vendor or in-house research teams.

6.17 Access

6.18 Agencies should ensure that facial recognition system access is only granted to individuals with adequate security clearance, in line with regional or agency-specific security best practices. Access should be monitored and updated on a regular basis, and individuals should only have access to the system functionality relevant to their roles.

6.19 Transparency

6.20 Where permitted by agency policy, agencies should strive to be open and transparent about their use of facial recognition technology. This should include releasing information on how the agency uses the technology and how the agency

aligns with relevant legislation, regulations, policies, and procedures – including the principles specified in this document.

FISWG documents can be found at: www.fiswg.org