NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

New York State Information Technology Policy	**No:** NYS-P20-001
IT Policy: **Digital Identity**	**Updated:** 07/16/2020
	Issued By: NYS Office of Information Technology Services **Owner:** Chief Information Security Office

1.0 Purpose and Benefits

This policy establishes a framework for issuing and managing trusted identity credentials to allow citizens, businesses, and government employees to conduct business online with New York State (NYS). A trusted identity credential is one in which a State Entity (SE) has sufficient confidence that the identity credential represents the person named in it and that the person engaged in the electronic transaction is the person to whom the identity credential was issued.

This policy benefits users of systems and e-Government services by providing a framework that creates and issues NYS electronic identity credentials that can be universally trusted by ensuring alignment with the National Institute of Standards and Technology (NIST) Digital identity guidelines. SEs will be able to participate in shared identity solutions and reduce the need to issue and manage their own electronic identity infrastructure for e-Government services; resulting in reduced costs of providing online services that require user authentication.

2.0 Authority

Section 103(10) of the State Technology Law provides the Office of Information Technology Services (ITS) with the authority to establish statewide technology policies, including technology and security standards. Section 2 of Executive *Order No. 117*, established January 2002, provides the State Chief Information Officer with the authority to oversee, direct and coordinate the establishment of information technology policies, protocols, and standards for State government, including hardware, software, security, and business re-engineering. Details regarding this authority can be found in NYS ITS Policy, *NYS-P08-002 Authority to Establish State Enterprise Information Technology (IT) Policy, Standards and Guidelines*.

3.0 Scope

This policy applies to all SE, defined as "State Government" entities as defined in Executive Order 117, established January 2002, or "State Agencies" as defined in Section 101 of the State Technology Law. This includes employees and all third parties (such as local governments, consultants, vendors, and contractors) that use or access any IT resource for which the SE has administrative responsibility, including systems managed or hosted by third parties on behalf of the SE. While an SE may adopt a different policy, it must include the requirements set forth in this one.

This policy applies to online services provided by a SE which requires user authentication. This includes all systems for which SEs have administrative responsibility including those managed or hosted by other entities.

4.0 Information Statement

This policy requires that SE information owners complete digital identity requirements assessments during system design to determine the appropriate Identity Assurance Level (IAL), Authenticator Assurance Level (AAL), and Federation Assurance Level (FAL) for all information technology (IT) systems that will require user authentication and contain or process SE data. The assessments focus on:

- whether the person seeking to access the system is who they claim to be and the potential impact to the confidentiality and integrity of the data and/or system if that person is not who they claim to be;
- whether the person accessing the service today is the same person who accessed the service using the same authenticator previously; and
- how to convey the results of authentication processes and relevant identity information to other applications.

Completion of the assessments provides a system specific numerical IAL, AAL, and FAL.

Assessments must be documented and kept with other system documentation and must be used to guide system design and functions which impact identity, authentication, and/or federation services.

All digital identity assurance processes will be managed using the NYS-S20-001 Digital Identity Standard.

4.1 Identity Vetting

The system's IAL defines the accepted assurance level a user must have to access the system. The level of certainty in the identity of a user is established through the strength of the evidence and processes used to verify the identity of the individual requesting a trusted identity credential (identity vetting).

Table 1. Identity Assurance Levels[1]

Identity Assurance Level	
IAL1	There is no requirement to link the individual to a specific real-life identity. Any attributes provided in conjunction with the authentication process are self-asserted or should be treated as such.
IAL2	Evidence supports the real-world existence of the claimed identity and verifies that the individual is appropriately associated with this real-world identity. Identity vetting can occur either remotely or in-person in accordance with the NYS-S20-001 Digital Identity Standard. A Credential Service Provider (CSP) can validate the identity assurance level to the Relying Party (RP) without providing identifying information of the individual.
IAL3	Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained representative of the CSP. As with IAL2, a CSP can validate the identity assurance level to the RP without providing identifying information of the individual.

Improper identification of users can result in direct and potentially dire consequences to the SE and individual consumers of NYS services. The SE's information owner must include the SE's information security officer (ISO)/designated security representative in assurance assessments, both to assist with the process and to guide discussion regarding any final determinations. The SE's information owner is ultimately responsible for assigning the appropriate IAL for the system.

Appendix B outlines the process used by a SE to examine the data within its system and identify the risks of improperly validated access or potential data exposure. By understanding these risks, the SE is better able to determine the required IAL and the corresponding authentication technology.

4.2 Authentication

A successful authentication provides a level of risk-based assurance that the individual accessing the service today is the same individual that previously accessed the service with that authenticator. The strength of this assurance is described by an AAL.

An AAL will define the appropriate authentication requirements based on the SE's risk tolerance and assessment of the potential harm caused by unauthorized access to SE systems and data.

[1] NIST Special Publication 800-63A Digital Identity Guidelines: Enrollment and Identity Proofing

Table 2. Authenticator Assurance Levels[2]

Authenticator Assurance Level (AAL)	
AAL1	Provides some assurance that the individual authenticating is in control of an authenticator bound to the individual's account. Requires at least single-factor authentication. For example, a person logging in with a username and password (or smart card, biometrics, etc.) would meet this requirement. Successful authentication requires that the individual logging in prove possession and control of the authenticator through a secure authentication protocol as defined in the NYS-S14-007 Encryption Standard.
AAL2	Provides high confidence that the individual authenticating is in control of an authenticator(s) bound to the individual's account. Requires at least two distinct authentication factors (multi-factor). For example, a person logging in with a username and password (i.e., something you know), and an RSA SecurID token (i.e., something you have) would meet this requirement. For additional information on acceptable authentication factors, please see NYS-S14-006 Authentication Tokens Standard.
AAL3	Provides very high confidence that the individual authenticating is in control of an authenticator(s) bound to the individual's account. Authentication at AAL3 is based on proof of possession and control of at least two distinct authenticators using an approved cryptographic protocol. Authentication must use a hardware-based cryptographic authenticator and an authenticator that provides impersonation resistance. The same device may fulfill both requirements. For example, a person logging in with a smart card and a hardware-based RSA SecurID token with PIN would meet this requirement. AAL3 requirements are **extremely** specific and additional information can be found in NYS-S14-006 Authentication Tokens Standard.

Appendix C outlines the process used by a SE to determine the risk of improperly validated access or potential data exposure. By understanding these risks, the SE is better able to determine the required AAL and the corresponding authentication technology.

4.3 Federation and Assertions

Federation refers to the linking of an individual's identity in one system to that same individual's identity in other systems. Federation allows the results of authentication processes and relevant identity information to be shared and trusted across networked applications or systems. Federated identity systems use assertions to accomplish this task. Assertions are declarations from an Identity Provider (IdP) to an RP that contain information about an individual. Even when full identification is necessary, SEs must

[2] NIST Special Publication 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management

only collect the minimum amount of personal information required and must not identify the individual in an assertion.

FAL categories reflect the options SEs can select based on their risk tolerance and the assessment of potential harm caused by an attacker taking control of federated transactions.

Table 3. Federation Assurance Levels[3]

Federation Assurance Level (FAL)	
FAL1	Allows for the system to access an identity assertion from a separately administered identity provider (IdP); the SE system will trust that the third-party system has identified and authenticated the individual to the degree claimed. FAL1 maps to the OpenID Connect Basic Client profile or Security Assertion Markup Language (SAML) Web Single Sign On (SSO) Artifact Binding profile with no additional features.
FAL2	Adds the requirement that the assertion be encrypted using approved cryptography. The SE system, known as the RP, is the only party that can decrypt it. This provides strong assurance over the confidentiality, and therefore privacy, of the assertion. FAL2 additionally requires that the assertion (e.g., the OpenID Connect ID Token or SAML Assertion) be encrypted to a public key representing the RP in question.
FAL3	Requires the individual to present proof of possession of a cryptographic key referenced in the assertion in addition to the assertion artifact itself. The assertion is signed by the IdP and encrypted to the RP using approved cryptography.

Appendix D outlines the process used by a SE to examine the data within its system and identify the risks of improperly validated access or potential data exposure. By understanding these risks, the SE is better able to determine the required federated level of assurance.

5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is expected.

If compliance with this policy is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, SEs shall request an exception through the Chief Information Security Office exception process.

6.0 Definitions of Key Terms

[3] NIST Special Publication 800-63C Digital Identity Guidelines: Federation and Assertions

Except for terms defined in this policy, all terms shall have the meanings found in http://www.its.ny.gov/glossary.

Term	Definition
Authenticator	Something the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity (e.g. token).
Identity Provider (IdP)	The party that manages the individual's primary authentication credentials and issues assertions derived from those credentials. This is commonly the Credential Service Provider (CSP) as defined in the ITS Glossary.

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Chief Information Security Office
Reference: NYS-P20-001
NYS Office of Information Technology Services
1220 Washington Avenue, Building 5
Albany, NY 12226
Telephone: (518) 242-5200
Email: CISO@its.ny.gov

Statewide technology policies, standards, and guidelines may be found at the following website: http://www.its.ny.gov/tables/technologypolicyindex

8.0 Revision History

This policy shall be reviewed at least once every two years to ensure relevancy.

Date	Description of Change	Reviewer
10/05/2010	Original Policy Release	Thomas Smith, Chief Information Security Officer
09/12/2012	Reformatted and updated to reflect current CIO, agency name, logo and style	Thomas Smith, Chief Information Security Officer
10/18/2013	Full revision	Thomas Smith, Chief Information Security Officer

09/19/2014	Removed references to EIAM service and EIAM Program Office; moved procedures to Appendix B; removed Mitigation Request and Proposal – replaced by exception request form	Deborah A. Snyder, Acting Chief Information Security Officer
02/16/2017	Update of contact information and rebranding	Deborah A. Snyder, Deputy Chief Information Security Officer
07/16/2020	Content updated based on new NIST SP 800-63-3 Digital Identity Guidelines. Renamed policy from Identity Assurance (NYS-P10-006) to Digital Identity (NYS-P20-001).	Karen Sorady, Acting Chief Information Security Officer
05/20/2021	Updated Scope language	Karen Sorady, Acting Chief Information Security Officer

9.0 Related Documents

NYS-P03-002 Information Security Policy

NYS-S20-001 Digital Identity Standard

National Institute of Standards and Technology (NIST) Special Publication 800-63-3, Digital Identity Guidelines

NYS-S14-007 Encryption Standard

NYS-S14-001 Information Security Risk Management Standard

NYS-S14-006 Authentication Tokens Standard

NYS-S14-013 Account Management/Access Control Standard

APPENDIX A: Potential Impacts for each Category of Harm[4]

This section defines the three levels of impact for each category of harm. Each assurance level, IAL, AAL, and FAL (if accepting or asserting a federated identity) shall be evaluated separately.

Note: If an error in the identity system causes no measurable consequences for a category, there is no impact. For assessment purposes a category with no impact is marked with "N/A" or Not Applicable.

Potential impact of inconvenience, distress, or damage to standing or reputation	
Low	At worst, limited, short-term inconvenience, distress, or embarrassment to any party.
Moderate	At worst, serious short-term or limited long-term inconvenience, distress, or damage to the standing or reputation of any party.
High	Severe or serious long-term inconvenience, distress, or damage to the standing or reputation of any party. This is ordinarily reserved for situations with particularly severe effects or which potentially affect many individuals.

Potential impact of financial loss	
Low	At worst, an insignificant or inconsequential financial loss to any party, or at worst, an insignificant or inconsequential SE liability.
Moderate	At worst, a serious financial loss to any party, or a serious SE liability.
High	Severe or catastrophic financial loss to any party, or severe or catastrophic SE liability.

Potential impact of harm to SE programs or public interests	
Low	At worst, a limited adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) mission capability degradation to the extent and duration that the organization can perform its primary functions with noticeably reduced effectiveness, or (ii) minor damage to organizational assets or public interests.

[4] NIST Special Publication 800-63-3 Digital Identity Guidelines, Section 5.3.2 Impacts per Category

Moderate	At worst, a serious adverse effect on organizational operations, assets, or public interests. Examples of serious adverse effects are: (i) significant mission capability degradation to the extent and duration that the organization can perform its primary functions with significantly reduced effectiveness; or (ii) significant damage to organizational assets or public interests.
High	A severe or catastrophic adverse effect on organizational operations, assets, or public interests. Examples of severe or catastrophic effects are: (i) severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions; or (ii) major damage to organizational assets or public interests.

Potential impact of unauthorized release of sensitive information	
Low	At worst, a limited release of PPSI or other sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact as defined in NYS Information Classification Standard.
Moderate	At worst, a release of PPSI or other sensitive information to unauthorized parties resulting in loss of confidentiality with a moderate impact as defined in NYS Information Classification Standard.
High	A release of PPSI or other sensitive information to unauthorized parties resulting in loss of confidentiality with a high impact as defined in NYS Information Classification Standard.

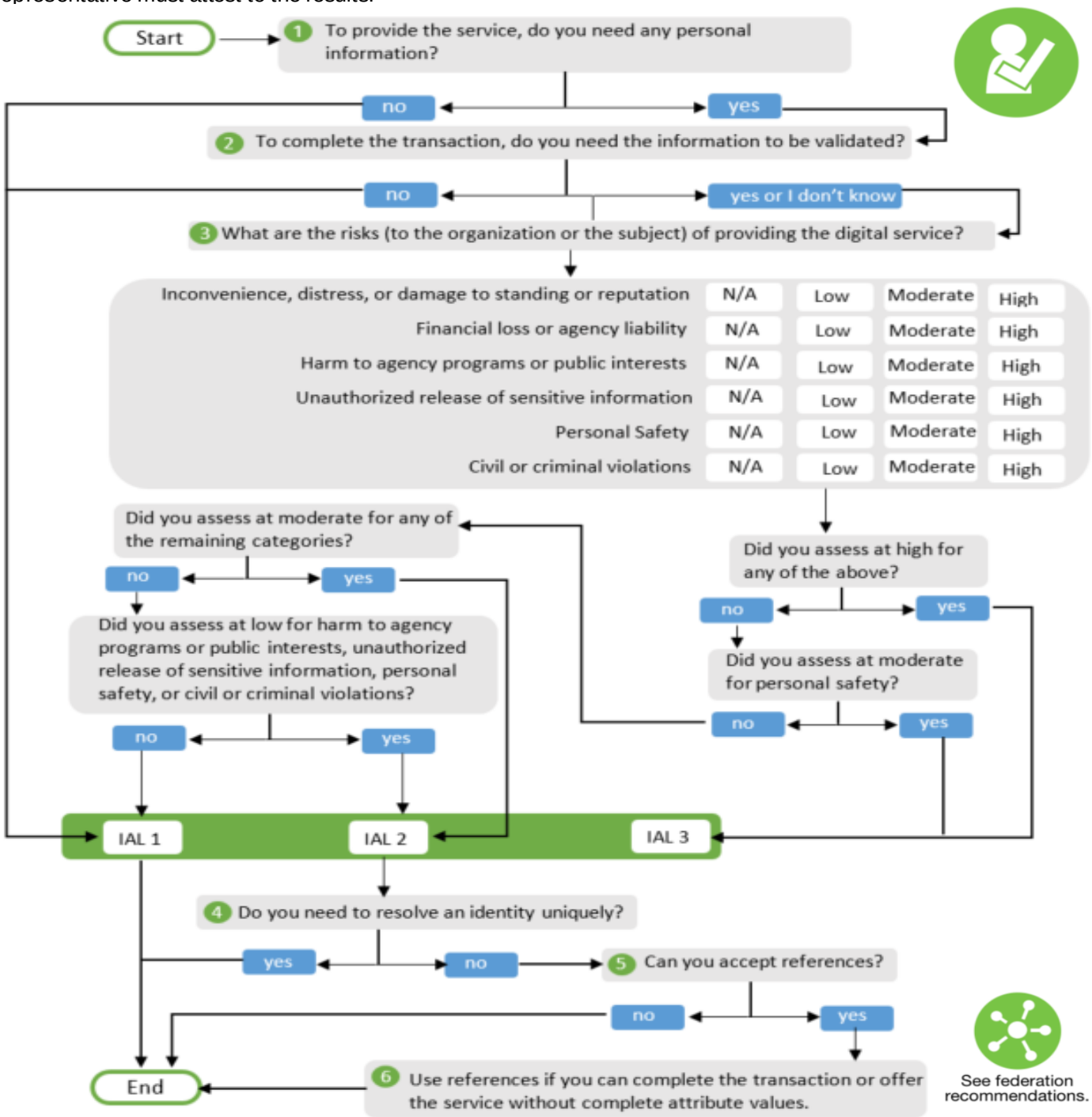
Potential impact to personal safety	
Low	At worst, minor injury not requiring medical treatment.
Moderate	At worst, moderate risk of minor injury or limited risk of injury requiring medical treatment.
High	A risk of serious injury or death.

The potential impact of civil or criminal violations is	
Low	At worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts.
Moderate	At worst, a risk of civil or criminal violations that may be subject to enforcement efforts.
High	A risk of civil or criminal violations that are of special importance to enforcement programs.

APPENDIX B – Identity Assurance Level (IAL) Assessment Process

Determine Identity Assurance Level[5]

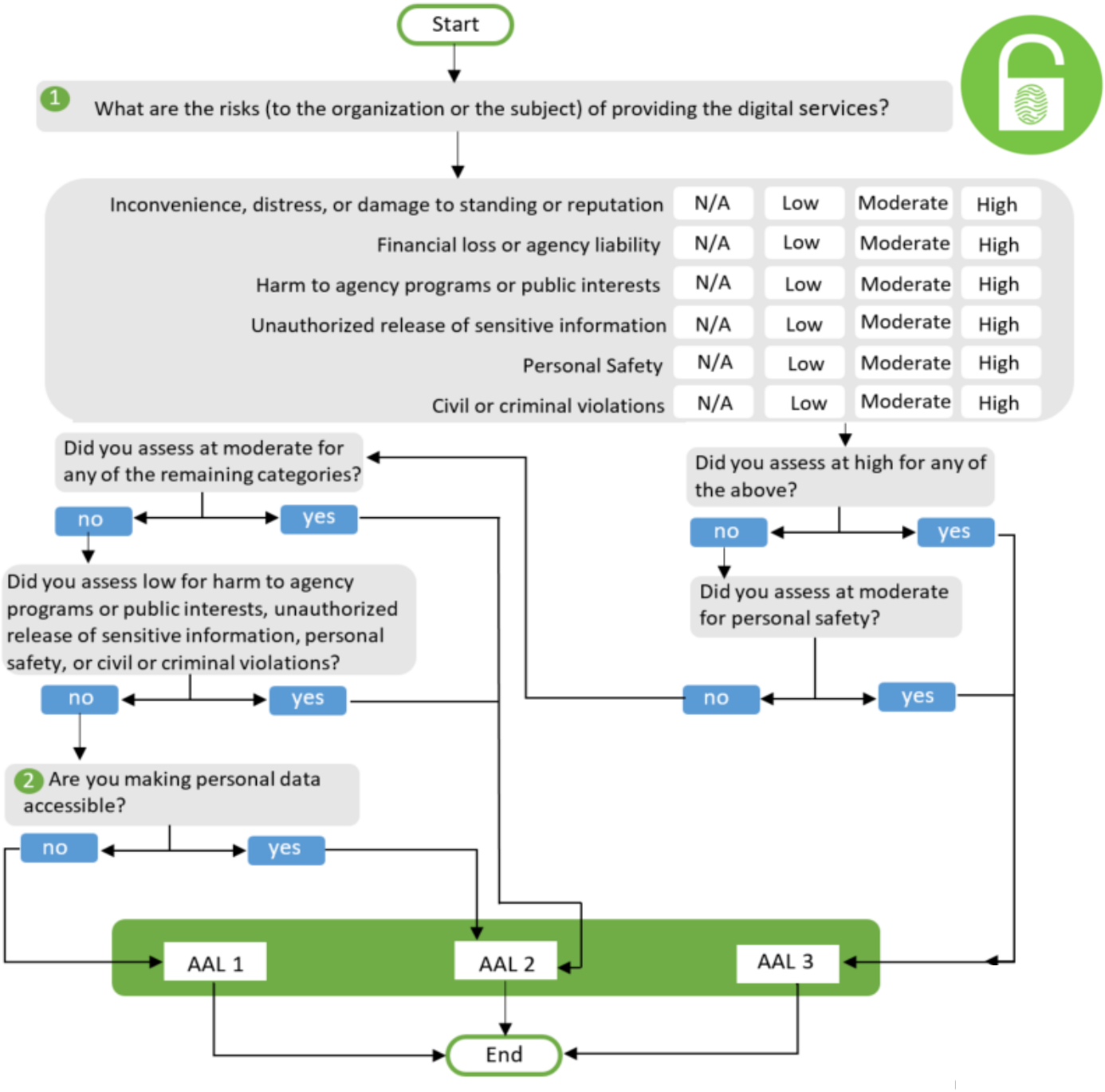
The following IAL decision tree outlines the process for assigning a system-specific identity assurance level. A final IAL designation must be reviewed, and the responsible Information Owner and security representative must attest to the results.



APPENDIX C – Authenticator Assurance Level (AAL) Assessment Process

Determine Authenticator Assurance Level[6]

The following AAL decision tree outlines the process for assigning a system-specific authenticator assurance level. A final AAL designation must be reviewed, and the responsible Information Owner and security representative must attest to the results.

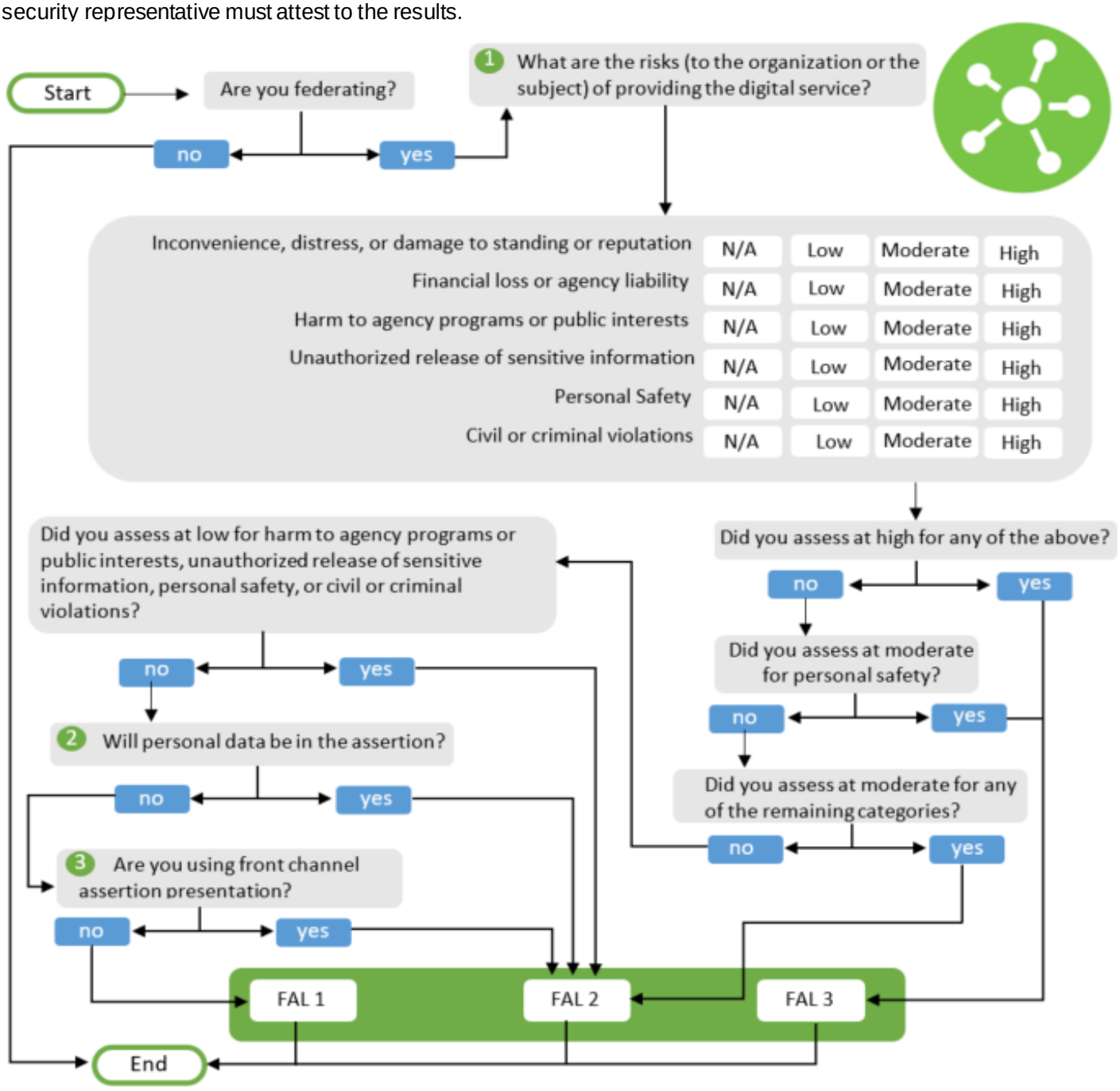


[6] NIST Special Publication 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management

APPENDIX D – Federation Assurance Level (FAL) Assessment Process

Determine Federation Assurance Level (FAL)[7]

The following FAL decision tree outlines the process for assigning a system-specific federation assurance level. A final FAL designation must be reviewed and the responsible Information Owner and designated security representative must attest to the results.



[7] NIST Special Publication 800-63C Digital Identity Guidelines: Federation and Assertions