COMMONWEALTH OF VIRGINIA

IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL (IMSAC)

GUIDANCE DOCUMENT 3
Privacy, Security, and Confidentiality of Identity Information

Table of Contents

1 Publication Version Control

The following table contains a history of revisions to this publication.

Publication Version	Date	Revision Description
1.0	10/24/2017	Initial Draft of Document

2 Reviews

- The initial version of the document was prepared by staff from the Virginia Information Technologies Agency (VITA) for the Secretary of Technology, under the direction from the Identity Management Standards Advisory Council (IMSAC).

- The document will be reviewed in a manner compliant with the Commonwealth of Virginia's Administrative Process Act, § 2.2-4000 et seq.

3 Purpose and Scope

Pursuant to § 2.2-436 and § 2.2-437, *Code of Virginia*, this guidance document was developed by the Identity Management Standards Advisory Council (IMSAC), on behalf of the Secretary of Technology, to establish minimum specifications for identity management of Non-Person Entities, so as to warrant liability protection pursuant to the Electronic Identity Management Act ("the Act"), Chapter 50 of Title 59.1. The guidance document, as defined in § 2.2-4001, was prepared to provide information or guidance of general applicability to the public for interpreting or implementing the Act. The guidance document was not developed as a Commonwealth of Virginia Information Technology Resource Management (ITRM) Policy, Standard, and Guideline, pursuant to § 2.2-2007, and therefore the guidance document is not applicable to executive branch agencies of the Commonwealth of Virginia.

4 Statutory Authority

The following section documents the statutory authority established in the *Code of Virginia* for the development of minimum specifications and standards for the privacy, security, and confidentiality of identity information. References to statutes below and throughout this document shall be to the *Code of Virginia*, unless otherwise specified.

Governing Statutes:

Secretary of Technology
§ 2.2-225. Position established; agencies for which responsible; additional powers
http://law.lis.virginia.gov/vacode/title2.2/chapter2/section2.2-225/

Identity Management Standards Advisory Council
§ 2.2-437. Identity Management Standards Advisory Council
http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-437/

Commonwealth Identity Management Standards
§ 2.2-436. Approval of electronic identity standards
http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-436/

Electronic Identity Management Act
Chapter 50. Electronic Identity Management Act
http://law.lis.virginia.gov/vacode/title59.1/chapter50/

5 Definitions

The terms used in this document comply with definitions in the Public Review version of the National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3), and align with adopted definitions in § 59.1-550, *Code of Virginia* (COV), and the Commonwealth of Virginia's ITRM Glossary (ITRM Glossary). [1]

The definitions may be accessed at:
http://vita.virginia.gov/default.aspx?id=6442475952

[1] NIST SP 800-63-3 may be accessed at https://pages.nist.gov/800-63-3/sp800-63-3.html#sec3 . At the time of the publication of this document, NIST SP 800-63-3 was still under development. However, this document may be updated, as recommended by IMSAC, following the final adoption and publication of NIST SP 800-63-3.
§ 59.1-550, *Code of Virginia*, may be accessed at http://law.lis.virginia.gov/vacode/title59.1/chapter50/section59.1-550/
The Commonwealth's ITRM Glossary may be accessed at
http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/PSG_Sections/COV_ITRM_Glossary.pdf

6 Background

In 2015, Virginia's General Assembly passed the Electronic Identity Management Act (Chapter 50 of Title 59.1, *Code of Virginia*) to address demand in the state's digital economy for secure, privacy enhancing Electronic Authentication and identity management. Growing numbers of "communities of interest" have advocated for stronger, scalable and interoperable identity solutions to increase consumer protection and reduce liability for principal actors in the identity ecosystem – Identity Providers, Credential Service Providers and Relying Parties.

To address the demand contemplated by the Electronic Identity Management Act, the General Assembly also created the Identity Management Standards Advisory Council (IMSAC) to advise the Secretary of Technology on the adoption of identity management standards and the creation of guidance documents, pursuant to §2.2-436. A copy of the IMSAC Charter has been provided in **Appendix 1**.

The Advisory Council recommends to the Secretary of Technology guidance documents relating to (i) nationally recognized technical and data standards regarding the verification and authentication of identity in digital and online transactions; (ii) the minimum specifications and standards that should be included in an Identity Trust Framework, as defined in §59.1-550, so as to warrant liability protection pursuant to the Electronic Identity Management Act (§59.1-550 et seq.); and (iii) any other related data standards or specifications concerning reliance by third parties on identity credentials, as defined in §59.1-550.

Purpose Statement

This guidance document, as defined in § 2.2-4001, was developed by the Identity Management Standards Advisory Council (IMSAC), on behalf of the Secretary of Technology, to provide information or guidance of general applicability to the public for interpreting or implementing the Electronic Identity Management Act. Specifically, the document establishes minimum specifications for the privacy, security, and confidentiality of identity information within a Digital Identity System. The minimum specifications apply core provisions of the Commonwealth of Virginia's Information Security Standard 501 (SEC501) and National Institute of Standards and Technology Special Publication 800-53-4 (NIST SP 800-53-4).

The document assumes that specific business, legal, and technical requirements for NPEs will be established in the Identity Trust Framework for each distinct Digital Identity System, and that these requirements will be designed based on the Electronic Authentication model, Identity Assurance Level (IAL), and Authenticator Assurance Level (AAL) requirements for the system. The document limits its focus to privacy, security, and confidentiality of identity information. Minimum specifications for other components of a Digital Identity System have been defined in separate IMSAC guidance documents in this series, pursuant to §2.2-436 and §2.2-437.

7 Minimum Specifications

National Institute of Standards and Technology Special Publication 800-53-4 (NIST SP 800-53-4) establishes recommended security controls for information systems. This document defines minimum specifications for privacy, security, and confidentiality of identity information within a Digital Identity System. The minimum specifications have been developed based on the core provisions of SEC501 and NIST SP 800-53-4. The minimum specifications also align with the Identity Ecosystem Steering Group's (IDESG) Identity Ecosystem Framework (IDEF) Baseline Functional Requirements (v.1.0) for Privacy and Security, shown in **Appendix 2**.

Classification of Identity Information

Classification of sensitivity defines the steps necessary to classify all identity information according to its sensitivity with respect to the following three criteria:

- Confidentiality: Sensitivity to unauthorized disclosure
- Integrity: Sensitivity to unauthorized modification
- Availability: Sensitivity to outages

Sensitive identity information is any data of which the compromise with respect to confidentiality, integrity, or availability could have a material adverse effect on the organization's interest, the conduct of business, or the individual privacy. Data sensitivity is directly proportional to the materiality of a compromise of the data with respect to these criteria. Organizations should classify identity information by sensitivity according to the most sensitive data stored, processed, or transmitted within the Digital Identity System.

Organization's responsible for a Digital Identity System should:

1. Identify the type of identity information handled within the Digital Identity System.
2. Determine whether the identity information is subject to other regulatory requirements.
3. Determine the potential damages to the organization of a compromise of confidentiality, integrity, or availability of each type of identity information within the Digital Identity System, and classify the sensitivity of the information accordingly.
4. Classify the identity information as sensitive if any type of the data handled within the Digital Identity System has a sensitivity of high on any of the criteria of confidentiality, integrity, or availability.
5. Verify and validate that all identity information has been reviewed and classified as appropriate for sensitivity.
6. Communicate approved identity information classifications to appropriate stakeholders.
7. Require that the organization restrict access to identity information classified as sensitive with respect to confidentiality.
8. Use the information documented in the sensitivity classification as a primary input to the Risk Assessment process (see below).

Risk Assessment

Risk Assessment guidance delineates the steps agencies must take for each set of identity information classified as sensitive to:

- Identify potential threats to a Digital Identity System and its operational environment
- Determine the likelihood that threats will materialize
- Identify and evaluate vulnerabilities
- Determine the loss impact if one or more vulnerabilities are exploited by a potential threat

For each set of identity information within a Digital Identity System classified as sensitive, the responsible organization(s) should:

1. Conduct and document a risk assessment of the Digital Identity System as needed
2. Conduct and document a regular self-assessments and audits to maintain the validity of the risk assessment
3. Prepare a report of each risk assessment that includes, at a minimum, identification of all vulnerabilities discovered during the assessment, and an executive summary, including major findings and risk mitigation recommendations

Security Control Catalog

Security controls documented in these minimum specifications define the baseline security capabilities needed to protect a particular aspect of identity information within a Digital Identity System. The control statement describes specific security-related activities or actions to be carried out by the organization or by the system.

AC-1 Access Control Policy and Procedures
Control: The organization:

a. Develops, documents, and disseminates to all organization personnel, contractors, and service providers with a responsibility to implement access controls:
    1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
    2. Procedures to facilitate the implementation of the access control policy and associated access controls
b. Reviews and updates the current:
    1. Access control policy on an annual basis or more frequently if required to address an environmental change
    2. Access control procedures on an annual basis or more frequently if required to address an environmental change

AC-2 Account Management

Control: The organization:

a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: individual, group, system, service, application, guest/anonymous, and temporary
b. Assigns account managers for information system accounts
c. Establishes conditions for group and role membership
d. Specifies authorized users of the information system, group and role membership, and access authorizations and other attributes (as required) for each account
e. Requires approvals by manager or designee for requests to create information system accounts
f. Creates, enables, modifies, disables, and removes information system accounts in accordance with the agency-defined logical access control policy
g. Monitors the use of information system accounts
h. Notifies account managers:
    1. When accounts are no longer required
    2. When users are terminated or transferred
    3. When individual information system usage or need-to-know changes
i. Authorizes access to the information system based on:
    1. A valid access authorization
    2. Intended system usage
    3. Other attributes as required by the organization
j. Reviews accounts for compliance with account management requirements on an annual basis or more frequently if required to address an environmental change
k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group

AC-3 Access Enforcement

Control: The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

AC-4 Information Flow Enforcement

Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on the appropriate organization-defined information flow control policies.

AC-5 Least Privilege

Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

AT-1 Security Awareness and Training Policy and Procedures

Control: The organization:

a. Develops, documents, and disseminates to all information system users (including managers, senior executives, and contractors):
    1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and
b. Reviews and updates the current:
    1. Security awareness and training policy on an annual basis or more frequently if required to address an environmental change; and
    2. Security awareness and training procedures on an annual basis or more frequently if required to address an environmental change.

AT-2 Security Awareness

Control: The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):

a. As part of initial training for new users;
b. When required by information system changes; and
c. Annually or more often as necessary thereafter.

AT-3 Role-Based Security Training

Control: The organization provides role-based security training to personnel with assigned security roles and responsibilities:

a. Before authorizing access to the information system or performing assigned duties;
b. When required by information system changes
c. As practical and necessary thereafter

AT-4 Security Training Records

Control: The organization:

a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training
b. Retains individual training records for period as defined by the organization's records retention policy

AU-1 Audit and Accountability Policy and Procedures

Control: The organization:

(a) Develops, documents, and disseminates to the appropriate organization-defined personnel and roles:
    1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance

2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls

(b) Reviews and updates the current:
1. Audit and accountability policy on an annual basis or more frequently if required to address an environmental change
2. Audit and accountability procedures on an annual basis or more frequently if required to address an environmental change

AU-2 Audit Events

Control: The organization:

a. Determines that the information system is capable of auditing the following events: authentication attempt, authenticated individual, access time, source of access, duration of access, and actions executed
b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events
c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents

PL-1 Security Planning Policy and Procedures

Control: The organization:

a. Develops, documents, and disseminates to the appropriate organization-defined personnel:
   1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
   2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls
b. Reviews and updates the current:
   1. Security planning policy on an annual basis or more frequently if required to address an environmental change
   2. Security planning procedures on an annual basis or more frequently if required to address an environmental change

PL-2 System Security Plan

Control: The organization:

a. Develops a security plan for the information system that:
   1. Is consistent with the organization’s enterprise architecture
   2. Explicitly defines the authorization boundary for the system
   3. Describes the operational context of the information system in terms of missions and business processes
   4. Provides the security categorization of the information system including supporting rationale

5. Describes the operational environment for the information system and relationships with or connections to other information systems
6. Provides an overview of the security requirements for the system
7. Identifies any relevant overlays, if applicable
8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions
9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation

b. Distributes copies of the security plan and communicates subsequent changes to the plan to the appropriate organization-defined personnel
c. Reviews the security plan for the information system on an annual basis or more frequently if required to address an environmental change
d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments
e. Protects the security plan from unauthorized disclosure and modification

RA-1 Risk Assessment Policy and Procedures

Control: The organization:

a. Develops, documents, and disseminates to the appropriate organization-defined personnel:
   1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
   2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls
b. Reviews and updates the current:
   1. Risk assessment policy on an annual basis or more frequently if required to address an environmental change
   2. Risk assessment procedures on an annual basis or more frequently if required to address an environmental change

RA-2 Security Categorization

Control: The organization:

a. Categorizes information and the information system in accordance with applicable laws and regulations
b. Documents the security categorization results (including supporting rationale) in the security plan for the information system
c. Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative

RA-3 Risk Assessment

Control: The organization:

a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
b. Documents risk assessment results in a Risk Assessment Report;
c. Reviews risk assessment results on an annual basis or more frequently if required to address an environmental change;
d. Disseminates risk assessment results to the appropriate organization-defined personnel; and
e. Updates the risk assessment on an annual basis or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

SI-1 System and Information Integrity Policy and Procedures

Control: The organization:

a. Develops, documents, and disseminates to the appropriate organization-defined personnel:
    1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
    2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls
b. Reviews and updates the current:
    1. System and information integrity policy on an annual basis or more frequently if required to address an environmental change
    2. System and information integrity procedures on an annual basis or more frequently if required to address an environmental change

SI-2 Information System Monitoring

Control: The organization:

a. Monitors the information system to detect:
    1. Attacks and indicators of potential attacks in accordance with organization-defined monitoring objectives
    2. Unauthorized local, network, and remote connections
b. Identifies unauthorized use of the information system through organization-defined techniques and methods
c. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion

Appendix 1. IMSAC Charter

COMMONWEALTH OF VIRGINIA
IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL
CHARTER

Advisory Council Responsibilities (§ 2.2-437.A; § 2.2-436.A)

The Identity Management Standards Advisory Council (the Advisory Council) advises the Secretary of Technology on the adoption of identity management standards and the creation of guidance documents pursuant to § 2.2-436.

The Advisory Council recommends to the Secretary of Technology guidance documents relating to (i) nationally recognized technical and data standards regarding the verification and authentication of identity in digital and online transactions; (ii) the minimum specifications and standards that should be included in an Identity Trust Framework, as defined in § 59.1-550, so as to warrant liability protection pursuant to the Electronic Identity Management Act (§ 59.1-550 et seq.); and (iii) any other related data standards or specifications concerning reliance by third parties on identity credentials, as defined in § 59.1-550.

Membership and Governance Structure (§ 2.2-437.B)

The Advisory Council's membership and governance structure is as follows:

1. The Advisory Council consists of seven members, to be appointed by the Governor, with expertise in electronic identity management and information technology. Members include a representative of the Department of Motor Vehicles, a representative of the Virginia Information Technologies Agency, and five representatives of the business community with appropriate experience and expertise. In addition to the seven appointed members, the Chief Information Officer of the Commonwealth, or his designee, may also serve as an ex officio member of the Advisory Council.

2. The Advisory Council designates one of its members as chairman.

3. Members appointed to the Advisory Council serve four-year terms, subject to the pleasure of the Governor, and may be reappointed.

4. Members serve without compensation but may be reimbursed for all reasonable and necessary expenses incurred in the performance of their duties as provided in § 2.2-2825.

5. Staff to the Advisory Council is provided by the Office of the Secretary of Technology.

The formation, membership and governance structure for the Advisory Council has been codified pursuant to § 2.2-437.A, § 2.2-437.B, as cited above in this charter.

The statutory authority and requirements for public notice and comment periods for guidance documents have been established pursuant to § 2.2-437.C, as follows:

C. Proposed guidance documents and general opportunity for oral or written submittals as to those guidance documents shall be posted on the Virginia Regulatory Town Hall and published in the Virginia Register of Regulations as a general notice following the processes and procedures set forth in subsection B of § 2.2-4031 of the Virginia Administrative Process Act (§ 2.2-4000 et seq.). The Advisory Council shall allow at least 30 days for the submission of written comments following the posting and publication and shall hold at least one meeting dedicated to the receipt of oral comment no less than 15 days after the posting and publication. The Advisory Council shall also develop methods for the identification and notification of interested parties and specific means of seeking input from interested persons and groups. The Advisory Council shall send a copy of such notices, comments, and other background material relative to the development of the recommended guidance documents to the Joint Commission on Administrative Rules.

This charter was adopted by the Advisory Council at its meeting on December 7, 2015. For the minutes of the meeting and related IMSAC documents, visit: https://vita.virginia.gov/About/default.aspx?id=6442474173

Appendix 2. IDESG Identity Ecosystem Framework (IDEF) Baseline Functional Requirements (v.1.0) for Privacy and Security

PRIVACY-1. DATA MINIMIZATION

Entities MUST limit the collection, use, transmission and storage of personal information to the minimum necessary to fulfill that transaction's purpose and related legal requirements. Entities providing claims or attributes MUST NOT provide any more personal information than what is requested. Where feasible, IDENTITY-PROVIDERS MUST provide technical mechanisms to accommodate information requests of variable granularity, to support data minimization.

PRIVACY-2. PURPOSE LIMITATION

Entities MUST limit the use of personal information that is collected, used, transmitted, or stored to the specified purposes of that transaction. Persistent records of contracts, assurances, consent, or legal authority MUST be established by entities collecting, generating, using, transmitting, or storing personal information, so that the information, consistently is used in the same manner originally specified and permitted.

PRIVACY-3. ATTRIBUTE MINIMIZATION

Entities requesting attributes MUST evaluate the need to collect specific attributes in a transaction, as opposed to claims regarding those attributes. Wherever feasible, entities MUST collect, generate, use, transmit, and store claims about USERS rather than attributes. Wherever feasible, attributes MUST be transmitted as claims, and transmitted credentials and identities MUST be bound to claims instead of actual attribute values.

PRIVACY-4. CREDENTIAL LIMITATION

Entities MUST NOT request USERS' credentials unless necessary for the transaction and then only as appropriate to the risk associated with the transaction or to the risks to the parties associated with the transaction.

PRIVACY-5. DATA AGGREGATION RISK

Entities MUST assess the privacy risk of aggregating personal information, in systems and processes where it is collected, generated, used, transmitted, or stored, and wherever feasible, MUST design and operate their systems and processes to minimize that risk. Entities MUST assess and limit linkages of personal information across multiple transactions without the USER's explicit consent.

PRIVACY-6. USAGE NOTICE

Entities MUST provide concise, meaningful, and timely communication to USERS describing how they collect, generate, use, transmit, and store personal information.

PRIVACY-7. USER DATA CONTROL

Entities MUST provide appropriate mechanisms to enable USERS to access, correct, and delete personal information.

PRIVACY-8. THIRD-PARTY LIMITATIONS

Wherever USERS make choices regarding the treatment of their personal information, those choices MUST be communicated effectively by that entity to any THIRD-PARTIES to which it transmits the personal information.

PRIVACY-9. USER NOTICE OF CHANGES

Entities MUST, upon any material changes to a service or process that affects the prior or ongoing collection, generation, use, transmission, or storage of USERS' personal information, notify those USERS, and provide them with compensating controls designed to mitigate privacy risks that may arise from those changes, which may include seeking express affirmative consent of USERS in accordance with relevant law or regulation.

PRIVACY-10. USER OPTION TO DECLINE

USERS MUST have the opportunity to decline Registration; decline credential provisioning; decline the presentation of their credentials; and decline release of their attributes or claims.

PRIVACY-11. OPTIONAL INFORMATION

Entities MUST clearly indicate to USERS what personal information is mandatory and what information is optional prior to the transaction.

PRIVACY-12. ANONYMITY

Wherever feasible, entities MUST utilize identity systems and processes that enable transactions that are anonymous, anonymous with validated attributes, pseudonymous, or where appropriate, uniquely identified. Where applicable to such transactions, entities employing service providers or intermediaries MUST mitigate the risk of those THIRD-PARTIES collecting USER personal information. Organizations MUST request individuals' credentials only when necessary for the transaction and then only as appropriate to the risk associated with the transaction or only as appropriate to the risks to the parties associated with the transaction.

PRIVACY-13. CONTROLS PROPORTIONATE TO RISK

Controls on the processing or use of USERS' personal information MUST be commensurate with the degree of risk of that processing or use. A privacy risk analysis MUST be conducted by entities who conduct digital identity management functions, to establish what risks those functions pose to USERS' privacy.

PRIVACY-14. DATA RETENTION AND DISPOSAL

Entities MUST limit the retention of personal information to the time necessary for providing and administering the functions and services to USERS for which the information was collected, except as otherwise required by law or regulation. When no longer needed, personal information MUST be securely disposed of in a manner aligning with appropriate industry standards and/or legal requirements.

PRIVACY-15. ATTRIBUTE SEGREGATION

Wherever feasible, identifier data MUST be segregated from attribute data.

SECURE-1. SECURITY PRACTICES
Entities MUST apply appropriate and industry-accepted information security STANDARDS, guidelines, and practices to the systems that support their identity functions and services.

SECURE-2. DATA INTEGRITY
Entities MUST implement industry-accepted practices to protect the confidentiality and integrity of identity data—including authentication data and attribute values—during the execution of all digital identity management functions, and across the entire data lifecycle (collection through destruction).

SECURE-3. CREDENTIAL REPRODUCTION
Entities that issue or manage credentials and tokens MUST implement industry-accepted processes to protect against their unauthorized disclosure and reproduction.

SECURE-4. CREDENTIAL PROTECTION
Entities that issue or manage credentials and tokens MUST implement industry-accepted data integrity practices to enable individuals and other entities to verify the source of credential and token data.

SECURE-5. CREDENTIAL ISSUANCE
Entities that issue or manage credentials and tokens MUST do so in a manner designed to assure that they are granted to the appropriate and intended USER(s) only. Where Registration and credential issuance are executed by separate entities, procedures for ensuring accurate exchange of Registration and issuance information that are commensurate with the stated assurance level MUST be included in business agreements and operating policies.

SECURE-6. CREDENTIAL UNIQUENESS
Entities that issue or manage credentials MUST ensure that each account to credential pairing is uniquely identifiable within its namespace for authentication purposes.

SECURE-7. TOKEN CONTROL
Entities that authenticate a USER MUST employ industry-accepted secure authentication protocols to demonstrate the USER's control of a valid token.

SECURE-8. MULTIFACTOR AUTHENTICATION
Entities that authenticate a USER MUST offer authentication mechanisms which augment or are alternatives to a password.

SECURE-9. AUTHENTICATION RISK ASSESSMENT
Entities MUST have a risk assessment process in place for the selection of authentication mechanisms and supporting processes.

SECURE-10. UPTIME

Entities that provide and conduct digital identity management functions MUST have established policies and processes in place to maintain their stated assurances for availability of their services.

SECURE-11. KEY MANAGEMENT

Entities that use cryptographic solutions as part of identity management MUST implement key management policies and processes that are consistent with adopted NIST guidelines or Commonwealth of Virginia SEC501, whichever provides for the most rigorous requirements at the time of the evaluation.

SECURE-12. RECOVERY AND REISSUANCE

Entities that issue credentials and tokens MUST implement methods for reissuance, updating, and recovery of credentials and tokens that preserve the security and assurance of the original Registration and credentialing operations.

SECURE-13. REVOCATION

Entities that issue credentials or tokens MUST have processes and procedures in place to invalidate credentials and tokens.

SECURE-14. SECURITY LOGS

Entities conducting digital identity management functions MUST log their transactions and security events, in a manner that supports system audits and, where necessary, security investigations and regulatory requirements. Timestamp synchronization and detail of logs MUST be appropriate to the level of risk associated with the environment and transactions.

SECURE-15. SECURITY AUDITS

Entities MUST conduct regular audits of their compliance with their own information security policies and procedures, and any additional requirements of law, including a review of their logs, incident reports and credential loss occurrences, and MUST periodically review the effectiveness of their policies and procedures in light of that data.