Standard ID:	SE-IAM-002
Title:	**Identity and Access Management Standard**
Revision Number:	0
Domain:	Security
Discipline:	Identity and Access Management
Effective:	6/14/2022
Reviewed:	6/14/2022
Approved By:	Chief Information Officer
Sponsor:	Chief Security Officer

I. Authority, Applicability and Purpose

A. Authority: Title 29 Chapter 90C Delaware Code, §9004C – General Powers, duties and functions of DTI "2) Create, implement and enforce statewide and agency technology solutions, policies, standards and guidelines, including as recommended by the Technology Investment Council on an ongoing basis and the CIO"

B. Applicability: Applies to all State of Delaware communications and computing resources. DTI is an Executive Branch Agency and has no authority over the customers in Legislative and Judicial Branches, as well as School Districts, and other Federal and Local Government entities that use these resources. However, all users, including these entities, must agree to abide by all policies, standards promulgated by DTI as a condition of funding, access and continued use of these resources.

C. Purpose: Applications containing State data must address the requirements outlined in this document such as authorization, session management and logging.

II. Scope

A. Audience: This standard addresses applications and the requirements that must be met by the developers. This document is not intended for use by non-IT personnel.

B. Areas Covered: This standard covers applications containing State data.

C. Environments: This standard applies to all applications that process, store or display State data.

III. Process

A. Adoption: These standards have been adopted by the Department of Technology and Information (DTI) through the Technology and Architecture Standards Committee (TASC) and are applicable to all Information Technology use throughout the state of Delaware.

B. Revision: Technology is constantly evolving; therefore, the standards will need to be regularly reviewed. It is the intent of the TASC to review this standard annually. The TASC is open to suggestions and comments from knowledgeable individuals within the state, although we ask that they be channeled through your Information Resource Manager (IRM).

C. Contractors: Contractors or other third parties are required to comply with these standards when proposing technology solutions to DTI or other state entities. Failure to do so could result in rejection by the Delaware Technology Investment Council. For further guidance, or to seek review of a component that is not rated below, contact the TASC at dti_tasc@delaware.gov.

D. Implementation responsibility: DTI and/or the organization's technical staff will implement these best practices during the course of normal business activities, including business case review, architectural review, project execution and the design, development, or support of systems.

E. Enforcement: DTI will enforce these best practices during the course of normal business activities, including business case and architectural review of proposed projects and during the design, development, or support of systems. These best practices may also be enforced by others during the course of their normal business activities, including audits and design reviews.

F. Contact us: Any questions or comments should be directed to dti_tasc@delaware.gov.

IV. Declarations

A. Declarations

1. User authorization
   - Must be OAuth/OpenID aware, compliant, and supported
   - Must be System for Cross-domain Identity (SCIM) compliant
   - Must support Role-based access authorization
   - Must follow a Least Privilege User Access model
   - Must demonstrate General Password and Authenticator Requirements
   - Must have credential storage requirements
   - Must have cryptographic Software and Device verifiers
   - Must have Service Authentication and Out of Band Verifiers
   - Must have Look-up Secret Verifiers and Credential Recovery requirements

2. Session Management
   - Custom session management must not store session parameters on the client side, even if encrypted
   - User sessions must be cancelled at the moment a user logs out of the web application
   - Sessions must have a timeout set after a specified period of inactivity
   - Sessions should have a secure flag set to prevent unauthorized viewing of session identifiers
   - Sessions must be invalidated on user log out
   - Session tokens must be sufficiently long and random
   - Session cookies must have appropriately restricted paths
   - Sessions must not permit duplicate concurrent user sessions from different machines
   - User must be able to see and terminate all sessions
   - User must be prompted for session termination on password change
3. All security related activity must be logged such as
   - Authentication
   - Authorization and privilege use
   - Create/Delete/Read/Change/Update
   - Successful and failed application authentication attempts
   - Application startups and shutdown
   - Major application configuration changes
4. Logs with security related activity must contain
   - Timestamp to NTP
   - Event, status, and error codes, event severity where possible
   - Service/command or application name
   - User or system account associated with event; where are service account is used, the true user account must be captured too
   - Connection source and destination
   - Session ID, terminal session ID and user-agent details of browser or tool used
   - Security Logs must not contain sensitive user information like PII (SSN, DOB) Bank Information (CC, Account information)
   - Source and destination IPs, source and destination ports
   - Payload size when possible

- The identity of the user should not be lost while traversing the web service, middleware or when calling the database for data
- Security logs should be separated from transaction logs wherever possible
- Ability to change, modify or delete logs must be restricted
- Systems must collect and retain at least 90 days' worth of logs
- Compliance related systems must collect and maintain 7 years' worth of logs
- Logs older than 90 days can be archived to less expensive storage

5. On a case-by-case basis, applications with validated technical limitations may be authorized by DTI to operate without full compliance.

V. Development and Revision History

Date	Revision
6/14/2022	Rev 0 – Initial version