Guidelines ID:	SE-IAM-003
Title:	**Identity and Access Management Guideline**
Revision Number:	1
Domain:	Security
Discipline:	Identity and Access Management
Effective:	6/14/2022
Reviewed:	10/17/2023
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 Local Education Agencies, 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: This guideline describes many of the features that are provided by the State Identity Management service.

II. Scope

A. Audience: This guideline addresses how applications and user will interact with several of the features of the State's Identity Management service

B. Areas Covered: This guideline covers a variety of areas such as strong password, multi-factor authentication, identity proofing, lifecycle management and additional areas.

C. Environments: This guideline addresses all the environments in use by consuming applications and systems.

III. Process

A. Adoption: These guidelines 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 guidelines 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 guidelines when proposing technology solutions to DTI or other state entities. Failure to do so could result in rejection of the proposed technology solution. 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 guidelines 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 guidelines 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. Definitions

1. Multi-factor authentication – It consists of a combination of two or more authentication methods. The State of Delaware currently uses RSA Keys. Multi-factor Authentication is to be reserved for those instances where strong passwords do not provide adequate security.
2. Pass phrases – They are strings of words and characters typed to authenticate into a network as opposed to a password of usually 6 – 12 characters. Pass Phrases can be much longer, up to 100 characters or more.
3. Resource Account – It is a user account created to facilitate non-interactive authentication. Examples include Windows service accounts, Exchange resource accounts and accounts created exclusively for inter-device or inter-process communication.
4. Service Account – It is a user account that is created explicitly to provide a security context for services running on a Windows machine.

.

V. Guidelines

A. **Simplified Logons** – Provide an easy logon experience.

1. Identity Authentication for State Internal Communications and Computing Resources
    i. Employee and contractor identities for accessing state internal and back-end applications, systems and networks must be authenticated with the computing tenant called **ID.Delaware.gov**
2. Constituent; Residents and Visitors Identity Authentication for Public-Facing Digital Government Resources
    i. Constituent, resident and visitor identities for accessing state digital government services and applications must be authenticated, authorized and accounted for through the computing tenant called **My.Delaware.gov**

B. **Strong Passwords** – Meet or exceed the defined criteria for strong passwords.

1. All passwords used to access State of Delaware data must adhere to the following characteristics for strong passwords:
    i. Passwords must be at least ten characters long. The security of a password rises exponentially with the number of characters used in the password. Pass Phrases are recommended.
    ii. Passwords/phrases cannot contain whole or significant parts of the username, first name or last name of the user.
    iii. Active Directory (not K12) passwords (used for email, used for logging into Windows, etc) on the State network must be at least 10 characters long.
    iv. A password must not be repeated/reused within 8 resets.
    v. Passwords should not be a common word or name.
    vi. All personnel must treat passwords and other access credentials as confidential and should protect them from disclosure. Refer to the Standards and Policies and notably to the State of Delaware Information Security Policy for further insight.
2. Human/User accounts - These passwords must contain characters from at least three (3) of the following four (4) classes from the Acceptable Password Characters table below:

ACCEPTABLE PASSWORD CHARACTERS	
DESCRIPTION	**EXAMPLES**
English upper-case letters	A, B, C, ... Z
English lower-case letters	a, b, c, ... z
English (Arabic) numerals	0, 1, 2, ... 9
English Non-alphanumeric ("special characters")	#,$,%,& such as punctuation symbols etc.

3. Service/Resource Accounts - Passwords used to access State of Delaware data must adhere to the following characteristics for strong passwords:
    i. Passwords must be at least 32 characters long or the maximum number of characters available.
    ii. Passwords must contain characters from at least three (3) of the following four (4) classes from the Acceptable Password Characters table shown above.

    A different service/resource account must be used for different services.

    A named person must be designated as the owner of each service/resource account.

C. Self-Service Account Management – Provide a self-service capability.

1. State identity services must enable users to manage certain elements of their identity. This can include email address and phone number.
    i. Solution must support password reset and or changes to existing identities.
    ii. Solution must support notifications on account lockouts and enable self-service account unlock.
    iii. Solution must clearly present password complexity requirements and restrictions during creation, change, or updates.

D. Multi-factor Authentication (MFA) – Provide several methods to authenticate.

1. Adaptive multi-factor authentication is required for all applications, systems, and network access.
2. Adaptive multi-factor authentication must take into consideration the risk associated with login sessions to trigger additional validation. Suspicious activity must be reported to the account owner and the administrators of the solution.
3. Risk assessment considerations that should trigger reporting and MFA validation:

i. Geo-related information, such as unusual source country or region

ii. Bot-related or non-human connectivity activity

E. **Suspicious Activity** – Report unusual activities.

1. Suspicious activity must be reported to the account owner and the administrators of the solution. These include:
    i. Login from unknown asset
    ii. Login from unexpected location
    iii. Change of password
    iv. Change or addition of multi-factor authentication options

F. **Lifecycle Management** - The State's identity and access management system must track an employee or contract from position appointment, through position changes to eventual retirement or separation from state government services.

1. The State Chief Security Officer may recommend enhanced username schemas to mitigate authentication attacks where necessary. For instance, User IDs may be recommended to follow the naming schema below:
    i. User IDs must be unique across all branches of government and K12
2. The solution must allow new employees and contractors to be provided a digital identity to authenticate to state systems, applications, networks, and data
3. The State technology teams with oversight from the Chief Security Officer should periodically review user access rights to make sure that access is still required for assigned functions.
4. The State's identity and access management solution should ensure there is a clear separation of duties (SoD) process in place to:
    i. ensure granted access does not lead to conflict of interest combination, and
    ii. actively prohibit access levels that can lead to such situations.
5. The solution must enable the expedited and automated (where possible) removal of access for separating employees and contractors.
6. The State's identity lifecycle management solution must enable the identity proofing of new hires, using an approved identity proofing option, before access is provisioned within any internal directory store.

G. **Identity Proofing** – Utilize a service to verify identity.

1. The state partners with the approved identity proofing vendors below:
    i. Government ID Proofing - Onfido
    ii. Knowledge-based ID Proofing - Lexis/Nexis
2. Limited options for Manual identity proofing services will be offered through designated state service centers.

H. **Legacy identity and access management solutions** – Address legacy solutions.

1. Initiate plans and activities to transition to the State's Identity Management service and away from legacy solutions such as:
    i. ACF2
    ii. Oracle IAM
    iii. Microsoft ADFS

I. **User Authentication** – Provide adaptive multi-factor authentication.

1. Must utilize Claim-based authentication.
2. Must support Federation with other third-party identity providers.
3. Must be SAML2.0/OAuth/OpenID aware, compliant and supported.
4. Must demonstrate Multi-Factor Authentication (MFA).
5. Must utilize the state enterprise identity directory stores.
6. Use of Microsoft Active Directory for direct authentication or authorization is deprecated.

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

VI. Development and Revision History

Date	Revision
6/14/2022	Rev 0 – Initial version
10/17/2023	Rev 1 – Added SAML2.0 awareness and removed User ID naming scheme