STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd.
Dover, Delaware 19904

Doc Ref Number:	SE-IAM-001	**Revision Number:** 1
Document Type:	Enterprise Policy	**Page:** 1 of 5
Policy Title:	Identity and Access Management Policy	

Synopsis:	Management of identity and the authentication of users prior to obtaining access to State information is critical.
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 CIO."
Applicability:	This policy is applicable to all users of the 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 access and continued use of these resources.
Effective:	6/14/2022
Reviewed:	7/18/2022
Approved By:	Chief Information Officer
Sponsor:	Chief Security Officer

TABLE OF CONTENTS

Section **Page**

I.	**POLICY**	2
II.	**DEFINITIONS**	4
III.	**DEVELOPMENT AND REVISION HISTORY**	4
IV.	**APPROVAL SIGNATURE BLOCK**	5
V.	**RELATED POLICIES AND STANDARDS**	5

I. POLICY

EXECUTIVE SUMMARY

Identity is the critical foundational element for the security and protection of state data and information systems. It must uniquely identify, validate, and confirm the user or system accessing state communications and computing resources with non-repudiation. Authenticating users and systems before they gain access to State information and resources has never been more important.

PURPOSE

All state applications, systems, networks, and data access must ensure they are using a State Chief Security Office designated directory store to effectively identify access to state data. This policy defines the requirements for authentication, authorization, and accounting for access to state applications, systems, networks, and data.

POLICY STATEMENT

1. State applications, systems, and networks controlling access to state constituent, employee, or financial data, must be authenticated, authorized, and accounted for through the state designated identity and access management solution.
2. State of Delaware internet facing applications that require the registration of constituent, resident, and/or visitors using their personally identifiable information, or

state applications that collect, store, or use personally identifiable information, must utilize the state designated identity and access management solution.

3. Identities used in the access to state applications, systems, networks, and data must be validated and proofed through a State Chief Security Office approved process or solution that ensures nonrepudiation of all activity.
4. The State identity and access management solution must protect the privacy of constituents', visitors', and residents' private identifiable information (PII). It must ensure they have:
   - The right to be forgotten and, to have their information deleted if they are no longer consuming state resources.
   - The right to know the applications accessing the identity information they have provided.
   - The right to not have their information sold or monetized.
   - The right to initiate the sharing or the transfer of their information to third party vendors.
5. All security-related activity must be logged with the required information (see standard/guideline) and upon request, the logs must be provided.
6. Identity and access management solutions must provide lifecycle management of all employees and contractors from position appointment, through position changes to eventual retirement or separation from State government.
7. Identity and access management solutions must enable the expedited and automated (where possible) removal of access for separating employees and contractors.
8. All Internet-facing applications must be compliant by 12/31/2023. All other state applications must be compliant by 12/31/2024.
9. The following areas are out of scope:
   - Authentication into mobile devices, legacy solutions like mainframes and Internet of Things (IOT) devices.
   - Authentication, authorization, and accounting requirements for ACF2 controlled applications, systems, and infrastructure.

II. DEFINITIONS

ACF2 –a security suite that is often used on mainframes.

Authentication (AuthN) – proving the person is who they say they are.

Authorization (AuthZ) – those things and only those things this authenticated person can do.

Directory store – a location or database of user account information.

Identity Access Management (IAM) – a centrally managed authentication service.

Internet-facing solution – a type of solution with an interface that is accessible to the Internet.

Internet of Things (IoT) devices – hardware devices that have the ability to collect and exchange information over the Internet.

Lifecyle Management – the discipline of ensuring that the information is current and relevant. In the context of this policy, it is confirming that new users are added and users, who are no longer with the State, are removed from the appropriate directory stores.

Mainframe – a large high-speed computer.

Non-repudiation – the process by which the sender must receive confirmation of delivery and the recipient must receive proof of sender's identity.

III. DEVELOPMENT AND REVISION HISTORY

Date	Revision
6/14/2022	Rev 0 – Initial version
7/18/2022	Rev 1 – Added definition section
11/4/2024	Rev 1 - Removed a reference to the Technology Investment Council

IV. APPROVAL SIGNATURE BLOCK

On File	
Name & Title:	**Date**
State Chief Information Officer	

V. RELATED POLICIES AND STANDARDS

Identity and Access Management Standard
Identity and Access Management Guidelines