P.11

Policy Name

Identity and Access Management Policy

1. Purpose

The purpose of this Policy is to establish the framework by which the State of Indiana manages the identity, authentication, and authorization of users and state information systems for ensuring the confidentiality, integrity, and availability of data and systems.

2. Scope

The Statewide IT Policies and Standards ("POLICIES") apply to all IOT-supported entities ("Entities"), their employees, their contractors, their consultants, and their vendors. Unless otherwise specified, all of the POLICIES apply equally to physical and electronic assets and resources assigned to an individual, on-premises physical assets, on-premises virtual assets, on-premises cloud assets, assets provided by cloud service providers, products and/or services that use cloud computing, all data stored or processed by the above assets in electronic, paper, or any other form, and everything else that supports the functioning of State government ("State Enterprise").

3. Policy

3.1 User Access and Account Management

a. An approved identity and access management ("IAM") platform must be used as the mechanism to manage resource permissions and the user account lifecycle.
b. IOT and Entities must assign a unique identifier for each user account, information asset, service, and workflow.
c. IOT and Entities will manage identity-management tools and centralized identity providers in a manner to prevent a user account from repudiating an action. This will include a cadenced review of user accounts.
d. User access activity must be logged and monitored to ensure the appropriate use of resources and to provide a record in the event of a malicious act.
e. Usernames and passwords will only be permitted and assigned to users who are authorized to use specific systems and domains.
f. IOT and Entities will use separation of duties in the creation and management of user accounts.
g. The State Personnel Department ("SPD") manages the authoritative source of truth for the identity of individuals employed by the State of Indiana. For other individuals working in the State Enterprise, IOT manages the authoritative source of truth for identity.
h. IOT must have identity-proofing processes in place. For further information, see the Access Management Standard.

3.2 Authentication and Password Requirements

a. IOT and Entities must use industry standard authentication methods, including multifactor authentication ("MFA"), where possible.
b. Failed authentication attempts must be limited to a defined number of total failed attempts and investigated by the appropriate team.
c. All authentication methods should be consistent with the determined authenticator assurance levels ("AAL"). This will include mandatory protections for preventing adversary-in-the-middle attacks, consistent privacy controls, and adherence to requirements for record retention. Changes in assurance level may require reauthentication.
d. MFA tools must use approved authenticator options, such as software tokens, hardware tokens, and biometrics.
e. The use of short message service ("SMS") authentication is prohibited, unless other forms of authentication are not technically feasible.
f. Account passwords must follow industry standards and state guidance regarding password change frequency, complexity, and reuse. These requirements must align with the Password and Authentication Standard.
g. Users must be prompted for periodic reauthentication after session expiration or determined levels of inactivity.

h. IOT must manage an information system for authentication. That system should manage the creation, revision, and termination of credentials. IOT and Entities must integrate information systems:
    i. With the IOT-managed single sign-on ("SSO"), and
    ii. Using the technologies that IOT designates for this purpose.

IOT and Entities should authenticate pursuant to U.S. National Institute of Standards and Technology ("NIST") Special Publication 800-53. An Exception Request is required for any information system that does not authenticate through SSO.

3.3 Access Provisioning

a. User creation, access provisioning, and changes to access must be managed through a documented process. IOT and Entities are responsible for maintaining standard operating procedures related to management of the identity lifecycle.
b. A mechanism for submitting details on access changes, including purpose and business justification, must exist. This lifecycle must be tracked and documented in the appropriate ticketing system or identity platform.
c. Access entitlements should only be granted on a need-to-use basis and follow the principle of least privilege.
d. Role-based access control ("RBAC") guidelines should be in place so that individuals in specific roles have an allocated set of applications and access permissions based on role. An individual must have an assigned set of permissions consistent with role and job function.
e. IAM must include prompt changes in access when an individual changes roles.
f. Segregation of duties should be implemented to prevent users from performing inappropriate escalated functions.
g. Provisioning of additional levels of authorizations or new access requests must have proper management approval prior to provisioning.
h. Where applicable, Entities are responsible for managing the identity lifecycle and the associated authorizations of their users.
i. Remote access privileges must only be granted to individuals who meet defined requirements. Remote access must be secured and assigned in accordance with the Remote Access Policy.

3.4 Access Removal

a. Upon an individual leaving an Entity, transferring between Entities, or having a leave of absence greater than three months, IOT and an Entity shall deprovision and disable all the accounts related to that individual. This paragraph does not apply to SPD's authoritative source of truth for Identity.
b. IOT and Entity managers are responsible for submitting a formal notification to remove access from an individual who no longer requires access.
c. Access must be removed within 24 hours of an individual's termination.
d. A vendor, a prospective vendor, and any other seeking to do business with the State must review and comply with this policy. At IOT's written request, a third party must provide written assurance of compliance.

3.5 Access Review and Management

a. All requests regarding user IDs, passwords, and credentials should be communicated through approved support processes. IOT and Entity managers should perform a periodic review of workforce user access to determine if access is still required.
b. If a workforce manager identifies that an individual no longer requires access, the associated manager must complete the necessary paperwork as soon as possible to terminate access.

4. Exceptions

Exception Requests will be addressed through the process designated by IOT.

5. Ultimate Authority

The Chief Information Officer is the ultimate authority for decisions made pursuant to the POLICIES, including Exception Requests.

6. Roles and Responsibilities

State agencies vary tremendously. Some State agencies have Chief Information Officers, while others may have no dedicated IT employees. Because of that variance, the Statewide IT Policies and Standards do not refer to a specific job title as being responsible for compliance. Instead,

the intent is for the responsibilities to rest with the agency head or the highest-ranking employee responsible for IT, unless stated otherwise regarding a specific duty.

7. Statutory Purposes

The statutory purposes of IOT include “establish the standards for the technology infrastructure of the state” and “provide for the technology and procedures for the state to do business with the greatest security possible,” Ind. Code § 4-13.1-2-1(1) and (5). IOT has an obligation to “develop and maintain policies, procedures, and guidelines for the effective and secure use of information technology in state government,” Ind. Code § 4-13.1-2-2(a)(11).

8. Industry Standards

The Statewide IT Policies and Standards are based on the following:

Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, U.S. National Institute of Standards and Technology, Special Publication 800-37 Rev. 2. https://csrc.nist.gov/pubs/sp/800/37/r2/final

Security and Privacy Controls for Information Systems and Organizations, U.S. National Institute of Standards and Technology, Special Publication 800-53 Rev. 5. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Critical Security Controls v.8.1, Center for Internet Security. https://www.cisecurity.org/controls

9. Federal Audit

The federal government audits the IT practices of several Entities. Where necessary, those Entities may create agency-specific policies to supplement the Statewide IT Policies and Standards. Those agencies include the Bureau of Motor Vehicles, Department of Child Services, Department of Revenue, Department of Workforce Development, Family and Social Services Administration, Indiana Office of Technology, and the Indiana State Police.