Identification and Authentication Policy

1.0 PURPOSE

The purpose of this policy is to provide identification and authentication (I&A) requirements for Ohio Department of Administrative Services (DAS)-managed system assets. Documented I&A controls are needed to ensure proper user provisioning and de-provisioning.

A glossary of terms found in this policy is located in Section 8.0 Definitions. The first occurrence of a defined term is in bold italics.

2.0 SCOPE

The scope of this policy includes any DAS-managed system asset. This policy also applies to DAS data owners, service owners, and extends to managed service providers.

Public information that is provided via the Internet does not require I&A.

3.0 BACKGROUND

Comprehensive I&A requirements and processes help to ensure the confidentiality, integrity, and availability of information. Sound I&A practices are critical to helping prevent unauthorized access to DAS-managed system assets.

I&A is used to ensure that those persons, applications, servers or network devices attempting to access DAS-managed system assets are in fact who they claim to be. This is most often accomplished by a simple login and password combination. However, applications and services that deal with sensitive data require a higher level of security (e.g., multifactor authentication). The risk assessment process outlined in DAS Policy 2100-08, “Risk Assessment,” will help determine the appropriate level of I&A.

This policy outlines requirements for organizational and non-organizational users. DAS interacts with and provides information and services to a variety of users who have differing needs. From a security perspective, it is essential to know who is accessing DAS-managed system assets and to define I&A requirements for each type.
4.0 REFERENCES

4.1 Ohio IT Standard ITS-SEC-02, Security Controls Framework: This state IT standard specifies the minimum requirements for information security in all agencies and identifies the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 as the framework for information security controls implementation for the state.


4.3 Ohio Administrative Policy IT-13, Data Classification: Ohio Administrative Policy IT-13 provides a data classification methodology to state agencies for the purpose of understanding and managing data and information systems with regard to their level of confidentiality and criticality.

4.4 DAS Policy 2100-08, Risk Assessment: Provides risk assessment requirements for DAS-managed system assets. The requirements address preparing for, conducting, communicating and maintaining a risk assessment.

4.5 DAS Policy 2100-01, Password: Addresses the use, management, and control of passwords used to access DAS-managed system assets.

4.6 DAS IT Standard DAS-ITS-2100-01-A, Password Standard for Organizational Users: Provides password requirements to DAS technical teams that will allow for the consistent implementation of password standards across DAS-managed system assets for internal users (e.g., state employees, contractors, county workers, etc.).

4.7 DAS IT Standard DAS-ITS-2100-01-B, Password Standard for Non-Organizational Users: Provides password requirements to DAS technical teams that will allow for consistent implementation of passwords standards across DAS-managed system assets for external users (e.g., citizens, businesses, etc.).

5.0 POLICY

5.1 Each DAS organizational and non-organizational user shall be assigned a unique identifier and shall be properly authenticated prior to gaining access to DAS-managed system assets.

5.1.1 Organizational User I&A: I&A of organizational user identities (e.g., employees, temporary contract workers, independent contractors and consultants) shall be accomplished through the use of mechanisms such as
passwords, *tokens*, *biometrics*, or multifactor authentication, or some combination thereof as dictated by Ohio IT Standard DAS-ITS-2100-01-A, “Password Standard for Organizational Users,” the results of the risk assessment that is conducted as outlined in DAS Policy ITS-2100-08, “Risk Assessment,” and as indicated by the *data classification labels* that are assigned in accordance with Ohio IT Administrative Policy IT-13, “Data Classification.”

5.1.1.1 Organizational users shall be maintained in a separate namespace or separate directory, container or database from non-organizational users.

5.1.1.2 Multifactor authentication is required for *privileged user* accounts.

5.1.1.3 Local access to internal networks from non-privileged accounts does not require multifactor authentication, but it is preferred.

5.1.1.4 *Replay-resistant authentication mechanisms* for network access to privileged accounts shall be employed based on the *security categorization* of the system.

5.1.2 **Non-Organizational User I&A:** At a minimum, non-organizational users are uniquely identified and authenticated for all accesses to non-public information or systems that contain sensitive data.

5.1.2.1 Authentication of non-organizational user identities shall be accomplished through the use of passwords, tokens, biometrics, or multifactor authentication, or some combination thereof as dictated by Ohio IT Standard DAS-ITS-2100-01-B, “Password Standard for Non-Organizational Users,” the results of the risk assessment and the assigned data classification labels.

5.1.2.2 For non-organizational users, different classes of users shall be maintained in a separate namespace or separate directory, container or database (e.g., citizen/public and business entities shall be maintained separately).

5.2 **Use of Group Identifiers and Authenticators:** Individuals authorized to use group identifiers or authenticators (e.g., shared accounts or tokens used by multiple individuals to gain privileged access) are required to use them in a manner that provides detailed accountability.

5.2.1 At a minimum, each use of a group identifier or authenticator shall be logged capturing the time, date, individual, and group identifier or authenticator used. Logging can be accomplished through automated or manual means as dictated by system capability.
5.2.2 Group identifiers shall be tested prior to implementation and training shall be provided to users.

5.3 **Device Identification:** Where required, as dictated by the results of the risk assessment, devices (e.g. workstations, laptops, tablets, smartphones, Voice over Internet Protocol (VoIP) phones and network hardware) shall be uniquely identified before establishing a connection to internal resources.

5.4 **Identifier Management:** Identifiers shall be managed for organizational users and devices, and non-organizational users.

5.4.1 A procedure shall be established to assign user identifiers and device identifiers to the intended party and device respectively.

5.4.2 The DAS Enterprise Identity Management group shall be responsible for authorizing and assigning user and device identifiers.

5.4.3 User identifiers shall not be reused.

5.5 **Authenticator Management:** The DAS Enterprise Identity Management Group shall manage authenticators for organizational and non-organizational users and devices.

5.5.1 DAS shall develop procedures that address initial authenticator distribution, revocation, protection from unauthorized disclosure and modification, and lost/compromised or damaged authenticators.

5.5.1.1 As part of the initial authenticator distribution process (e.g., the initial password), the identity of the individual and/or device receiving the authenticator shall be verified prior to distribution. Identifiers and authenticators shall be transmitted to users separately and securely. (e.g., using separate, encrypted emails).

5.5.1.2 Initial authenticators shall be randomly generated for each user and require change upon initial login.

5.5.1.3 Devices shall be configured to safeguard authenticators where the information system allows.

5.5.2 The reuse of authenticators shall follow the requirements outlined in Ohio IT Standard DAS-ITS-2100-01-A, “Password Standard for Organizational Users” and DAS-ITS-2100-01-B, “Password Standard for Non-Organizational Users.”

5.6 **Authenticator Feedback:** During the authentication process, authentication information feedback shall be obscured (e.g., display asterisks when a user types in a password). This requirement will help protect information from possible exploitation.
or use by unauthorized individuals. The means for obscuring the authenticator feedback shall be selected in accordance with the results of a risk assessment.

6.0 PROCEDURES

6.1 Exception Process: To request an exception to one or more of the requirements outlined in this policy, please complete an IT Security Exception Request form.

6.1.1 The form is located within the IT Enterprise Services Portal under the “Services & Products” category.

6.1.2 If you have any questions, please contact DAS OISP (refer to Section 9.0 Inquiries for contact information).

7.0 COMPLIANCE

As of the effective date of this policy, some DAS entities are unlikely to be completely aligned to the I&A requirements outlined in the policy. A general implementation framework for the requirements of this policy includes:

7.1 All existing DAS-managed system assets shall comply with the I&A requirements within one year from the effective date of the policy.

7.2 All planned and future DAS information system development initiatives, shall immediately comply with the I&A requirements outlined in this policy.

8.0 DEFINITIONS

Authentication - Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.¹

Authenticator - The means used to confirm the identity of a user, process, or device (e.g., user password or token).²

Availability – Ensuring timely and reliable access to and use of information.³

Biometrics - A measurable physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics.⁴

² Ibid.
³ Ibid.
Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.  

DAS-managed System Asset - Information, hardware, software and services required to support state business, and identified during the risk assessment process as assets that need to be protected. Primary responsibility for managing these system assets may be assigned to DAS OIT personnel or other outside entities.

Data Classification Labels - Denotes the level of protection based on the confidentiality and criticality requirements of data in accordance with the agency’s risk assessment. Data classification labels enable policy-based standards for securing and handling data and sharing information among organizations. The terms, “data classification label” and “classification label,” are used interchangeably.

Identification - An act or process that presents an identifier to a system so that the system can recognize a system entity (e.g., user, process, or device) and distinguish that entity from all others.

Identifier - A data object – often, a printable, non-blank character string – that definitively represents a specific identity of a system entity, distinguishing that identity from all others.

Integrity – Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Multifactor Authentication - Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

Non-Organizational User - A user who is not an organizational user, which for the purposes of this policy includes public users.

Organizational User - An organizational user is anyone who is an employee of the state, or is otherwise authorized to work on behalf of the State, and who has a need to access.

8 Ibid.
10 Ibid.
11 Ibid.
State of Ohio IT systems and has secured agency authorization for such access. The organizational identifier will help to distinguish the individual during the authentication process. Examples of resources that may fall into this category include full-time employees, part-time employees, seasonal employees, temporary contract workers, independent contractors or consultants, volunteers or unpaid interns. The organizational user identifier category may also include university and federal government resources.

**Personally identifiable information** - “Personally identifiable information” is information that can be used directly or in combination with other information to identify a particular individual. It includes:

- a name, identifying number, symbol, or other identifier assigned to a person,
- any information that describes anything about a person,
- any information that indicates actions done by or to a person,
- any information that indicates that a person possesses certain personal characteristics.

**Privileged User** - A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.12

**Replay-resistant Authentication Mechanisms** - Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.13

**Risk Assessment** - The process of identifying, prioritizing, and estimating risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system.14

**Security Category** - The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.15

---

13 Ibid.
14 Ibid.
Security Categorization - The process of determining the security category for information or an information system.16

Sensitive Data - Sensitive data is any type of computerized data that presents a high or moderate degree of risk if released or disclosed without authorization. There is a high degree of risk when unauthorized release or disclosure is contrary to a legally mandated confidentiality requirement. There may be a moderate risk and potentially a high risk in cases of information for which an agency has discretion under the law to release data, particularly when the release must be made only according to agency policy or procedure. The computerized data may be certain types of personally identifiable information that is also sensitive such as medical information, social security numbers, and financial account numbers. It includes Federal Tax Information under IRS Special Publication 1075, Protected Health Information under the Health Insurance Portability and Accountability Act, and Criminal Justice Information under Federal Bureau of Investigation’s Criminal Justice Information Services (CJIS) Security Policy. The computerized data may also be other types of information not associated with a particular individual such as security and infrastructure records, trade secrets and business bank account information.

Token - Something that the Claimant possesses and controls (typically a key or password) that is used to authenticate the Claimant’s identity.17

User - An individual or (system) process authorized to access an information system.18

9.0 INQUIRIES

Direct inquiries about this policy to:

Office of Information Security & Privacy
Office of Information Technology
Ohio Department of Administrative Services
30 East Broad Street, 19th Floor

1.614.644.9391 | state.isp@das.ohio.gov

DAS Policies may be found online at http://das.ohio.gov/Divisions/AdministrativeSupport/EmployeesServices/DASPolicies.aspx

Additional information regarding the Office of Information Security & Privacy may be found online at InfoSec.Ohio.Gov.

10.0 REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>07/12/2017</td>
<td>Original Policy</td>
</tr>
<tr>
<td>11/26/2018</td>
<td>Updated the exception request language to align with the current procedure.</td>
</tr>
<tr>
<td>11/26/2019</td>
<td>Scheduled policy review.</td>
</tr>
</tbody>
</table>

11.0 ATTACHMENTS

None.