1.0 PURPOSE

The purpose of this policy is to provide multifactor authentication (MFA) requirements to Ohio Department of Administrative Services (DAS) technical teams that will allow for the consistent implementation of MFA across DAS-managed system assets.

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 all DAS-managed system assets that require MFA. This policy outlines the minimum acceptable criteria governing MFA implementations.

3.0 BACKGROUND

The MFA policy describes the conditions necessary to challenge a user for stronger authentication than single-factor authentication (e.g., User ID and password) or two-step authentication. Typically, this is due to 1) the sensitive nature of the application, (e.g. contains sensitive or personally identifiable information) or 2) a privileged user performing administrative functions.

MFA includes two or more of the following conditions:

- Something you know (password)
- Something you have (soft token, hard token, smart cards, etc.)
- Something you are (biometrics)

MFA is typically implemented with a user ID, password and a hard or soft token for organizational users.

Two-step authentication, which should not be confused with MFA, is typically implemented with a user ID, password, and a personal identification number (PIN) for non-organizational users. It usually requires the user to supply additional contact information for the PIN during the registration process. PINs can be delivered by:

- Email
- Phone Callback
- Short Message Service (SMS) Text
4.0 REFERENCES

4.1 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.

4.2 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 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations: NIST SP 800-53 provides guidelines for selecting and specifying security controls for federal government information systems.

4.4 DAS IT 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 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.).

4.6 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.).

4.7 IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies: Provides guidance to ensure the policies, practices, controls, and safeguards employed by recipient agencies, agents, or contractors adequately protect the confidentiality of federal tax information.

5.0 POLICY

DAS system and service owners shall work with DAS business owners to conduct risk assessments and data classification exercises on DAS-managed system assets in accordance with Ohio Administrative Policy IT-13, “Data Classification,” and DAS Policy 2100-08, “Risk Assessment.” MFA shall be applied to systems based on the outcome of those assessments and in accordance with the requirements of this policy. The policy sections below detail when MFA is required or optional.
5.1 **Required MFA for DAS-managed System Assets (for Organizational Users):** The use of MFA shall be required for organizational users under the following conditions:

5.1.1 When User IDs are assigned privileged access

5.1.2 When *remote access* is granted

5.2 **MFA for DAS-managed System Assets (for Organizational Users):** MFA shall be used as a mitigating control and is recommended for organizational users when indicated by the results of a risk assessment. The following conditions are examples of higher-risk scenarios where MFA should be considered:

5.2.1 When the information system contains *sensitive data*, such as federal tax information (FTI), personally identifiable information (PII), and protected health information (PHI).

5.2.2 When high-risk factors, such as the following, are involved:

- Internet Protocol (IP) Reputation – restrict access from untrusted IP addresses.
- Geolocation – only allow access from certain geographic locations.
- Transaction-based – only when certain high-risk transactions (e.g., financial or administrative) are attempted.

5.3 **Two-Step Authentication (for Non-Organizational Users):** Two-step authentication shall not be used in place of MFA. However, the use of two-step authentication is acceptable for non-organizational users as a mitigating control when risk assessment results indicate that there is a need for authentication stronger than single-factor.

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 system or service owners are unlikely to be completely aligned to the MFA 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 MFA 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 MFA requirements outlined in this policy.

7.3 If for some reason a DAS IT system manager or service owner feels that it is not technically feasible to implement the MFA requirements outlined in this policy, an exception request shall be submitted in accordance with Section 6.0.

8.0 DEFINITIONS

**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.

**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 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 (PII)** - “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 system and application functions that ordinary users are not authorized to perform.\(^3\)

**Remote Access** - Access to an organizational information system by a user (or an information system acting on behalf of a user) communicating through an external network (e.g., the Internet). \(^4\)

**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.

**Two-step Authentication** - Two-step Authentication provides an additional layer of security over single-factor authentication (providing something the user knows such as a user ID and password). It requires the user to also provide something they have, which is typically a personal identification number (PIN). Most commonly, the user supplies additional contact information for the PIN during the registration process. The PIN can be delivered by email, phone callback, or short message service (SMS) text. Two-step authentication is generally used with non-organizational users.

**User ID** - Unique symbol or character string used by an information system to identify a specific user.\(^5\)

### 9.0 INQUIRIES

Direct inquiries about this policy to:

Office of Information Security & Privacy
Office of Information Technology
Ohio Department of Administrative Services

\(^3\) Ibid.

\(^4\) Ibid.

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/Administrative-Support/Employees-Services/DAS-Policies

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 of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/22/2017</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.