Access Controls Policy

<table>
<thead>
<tr>
<th>POLICY NUMBER:</th>
<th>EFFECTIVE DATE:</th>
<th>APPOINTING AUTHORITY APPROVAL:</th>
</tr>
</thead>
<tbody>
<tr>
<td>2100-11</td>
<td>10/10/2017</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REPLACES POLICY DATED:</th>
<th>AUTHORITY: Ohio Revised Code Section 125.18</th>
</tr>
</thead>
<tbody>
<tr>
<td>n/a</td>
<td></td>
</tr>
</tbody>
</table>

**1.0 PURPOSE**

This policy addresses access control requirements to ensure that Ohio Department of Administrative Services (DAS)-managed system assets are properly protected against unauthorized access while still meeting the access requirements for all authorized users.

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 user accounts on any DAS-managed system assets. This policy also applies to DAS data owners and service owners.

**3.0 BACKGROUND**

A critical line of defense in information system security is the proper management of access controls across networks, operating systems, applications, and mobile computing and teleworking environments. Strict controls and deliberate procedures will help to prevent unauthorized access, loss, disclosure, destruction, modification or disruption of data or information.

**4.0 REFERENCES**


4.2 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.

4.3 DAS Policy 200-14, Teleworking: DAS Policy 200-14 outlines the requirements for DAS teleworking.

4.4 Ohio Revised Code 1347.15, Access rules for confidential personal information: This section of Ohio Revised Code outlines what needs to be included in the rules...
that each state agency adopts under Chapter 119 of the Revised Code, regulating access to the confidential personal information the agency keeps, whether electronically or on paper.

5.0 POLICY

To adequately protect DAS-managed system assets, access control requirements need to be addressed within network, operating system, application and information, mobile computing and teleworking environments. The appropriate controls also need to be in place for user access management. The access controls for these environments need to be selected not only based upon security requirements, but also business and legal requirements. The following policy sections outline requirements for each of these critical access control components.

5.1 Business, Legal & Security Requirements for Access Control: In consideration of business, legal, and security requirements, the data owner shall drive the authorization process and access to IT resources and information assets.

5.1.1 Access control requirements shall be reviewed at least annually, and the occurrence of each review shall be documented.

5.1.1.1 Access shall be commensurate with the security requirements of the DAS-managed system asset. Access controls shall comply with all relevant federal and state laws, executive orders, directives, policies, regulations, standards, and guidance. For example, the controls implemented for protected health information shall be consistent with the requirements of the Health Insurance Portability and Accountability Act (HIPAA).

5.1.1.2 Identification and authentication controls shall be consistent with the security requirements of the DAS-managed system asset. The controls shall comply with all applicable federal and state laws, executive orders, directives, policies, regulations, standards, and guidance. For more detailed Identification and Authentication requirements, refer to DAS Policy 2100-10, “Identification and Authentication.”

5.2 User Access Management: The objective of user access management is to ensure authorized users, and processes acting on behalf of users, are able to access DAS-managed system assets, while unauthorized users are prevented from access to the same. Each DAS-managed system asset shall have documented system specific procedures and controls that cover all phases in the life cycle of user access.

5.2.1 User Registration: Access to DAS-managed system assets shall follow formal procedures.
5.2.1.1 Specific account types shall be defined (e.g., individual, group/shared, service, guest/anonymous, emergency, and temporary).

5.2.1.1.1 Authorized users shall be assigned group and role membership, and account access authorizations (e.g., privileges) for each account.

5.2.1.2 Accounts shall not be created, activated or deactivated without obtaining the necessary level(s) of authorized approval. This process shall include a documented access request.

5.2.1.3 Account administrators shall be notified when:

5.2.1.3.1 Users are transferred or terminated;

5.2.1.3.2 Individual information system usage or need-to-know requirements change; or

5.2.1.3.3 Accounts, including shared/group, emergency, and temporary, are no longer required.

5.2.1.4 When individuals transfer to DAS from another agency, all previous agency-specific role access to DAS enterprise systems (e.g., Ohio Administrative Knowledge System, Office365, Release and Permit, network file shares, SharePoint, etc.) shall be removed if not already done through the agency off-boarding process.

5.2.1.5 The use of group/shared, service, guest/anonymous, emergency, and temporary accounts shall be permitted only if the use is explicitly authorized and monitored.

5.2.1.5.1 Group identifiers shall be assigned to an owner, who is the primary point of contact for the identifier. Procedures shall be developed to manage and document ownership changes.

5.2.1.5.2 The use of group/shared and guest/anonymous accounts shall not be authorized to access sensitive data.

5.2.1.5.3 When group/shared accounts are permitted, a process shall be established for changing passwords when individuals are removed from the group. In addition, a process shall be established for the individual accountability of members authorized to use the group/shared accounts.
5.2.2 User Account Archiving: In an effort to retain user history and auditability of DAS-managed information systems, user accounts shall not be deleted.

5.2.2.1 Organizational user accounts may be archived after 400 days of inactivity.

5.2.2.2 Non-organizational user accounts may be archived after 800 days of inactivity.

5.2.3 Privilege Management: Access control rules shall incorporate the principle of least privilege, which grants the lowest level of access, rights, privileges, and security permissions needed for the performance of authorized tasks.

5.2.3.1 Acceptable access control implementation shall include the allocation of user privileges on a need-to-use, per system, per application basis.

5.2.3.2 Access controls shall support business and legal requirements, including job function and separation of duties.

5.2.3.3 Privileged users shall be assigned two separate accounts. One account shall be used to perform standard or base level functions (e.g., access to email or Internet) and the other shall be used solely to perform administrator or higher access level functions.

5.2.4 Review of User Access Rights: User access levels shall be reviewed by the data owner (or their designee) at least annually, or more frequently as indicated by the results of the information system risk assessment and data classification label requirements. The occurrence of each review shall be documented.

5.3 Network Access Control: Access to internal and external networked systems shall be provided in a controlled manner, and shall be protected through a combination of security controls including segmentation, deployment of firewalls and other security appliances and authentication mechanisms as appropriate (e.g. site-to-site virtual private networks). The security controls shall help to prevent and detect unauthorized access, while providing secure access for authorized users and systems.

5.3.1 Equipment Identification: Whenever possible, connections from specific locations and equipment shall be authenticated using automatic equipment identification.

5.3.2 Remote Diagnostic and Configuration Port Protection: The need for remote access functionality shall be validated prior to enabling any remote diagnostic or configuration capabilities.

5.3.3 Network Segregation: A segmented approach for separating logical network domains shall be adopted.
5.4 **Operating System Access Control:** Access to operating systems shall be restricted to authorized users. Security controls shall be employed to properly authenticate users, provide appropriate access by role (e.g., administrator), log activities and generate notifications of security events.

5.4.1 **Secure Login:** Secure login procedures that minimize the opportunity for unauthorized access shall be adopted (e.g., access restricted to local logins).

5.4.2 **Use of System Utilities:** Access and permissions associated with utility programs, including programs that are capable of overriding system and application controls, shall be strictly controlled (e.g., documented, vetted for security vulnerabilities/malicious code, deleted when no longer needed, etc.) and limited to only authorized users.

5.4.3 **Session Time-Out:** Inactive sessions shall be locked or terminated after a defined period of inactivity. Typically, *session locks* shall be implemented at the operating system or application level and session terminations shall be executed at the network or application level.

5.4.3.1 At a minimum, an information system shall be configured to:

5.4.3.1.1 Prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity or upon receiving a request from a user;

5.4.3.1.2 Conceal information that was previously visible on the display with a publicly viewable image;

5.4.3.1.3 Retain the session lock until the user re-establishes access using pre-defined identification and authentication procedures; and

5.4.3.1.4 Initiate a screen lock after a maximum of 15 minutes of inactivity.

5.4.4 **Connection Time Limitation:** Connection time shall be limited based upon a defined period of inactivity that requires the user to log out (e.g., at the end of the work day).

5.5 **Application and Information Access Control:** Access policies shall be enforced for information and system functions to protect against unauthorized access and to prevent the compromise of systems from which information is shared.

5.5.1 **Information Access Restriction:** Access to information and application systems shall be managed in accordance with state policy.
5.5.1.1 Information systems that require authentication shall display an approved system use notification message or banner before granting a user access to the system. The notification message or banner shall be modeled after the “DAS OISP-Approved Security Notification for IT Systems,” which is available on the DAS Policies Web page. If necessary, the “DAS OISP-Approved Security Notification for IT Systems,” may be customized to meet specific requirements. However, as a minimum, the notification message or banner shall include:

5.5.1.1.1 Content that is consistent with applicable federal and state laws, executive orders, directives, policies, regulations, standards, and guidance;

5.5.1.1.2 A statement that users are accessing a State of Ohio information system;

5.5.1.1.3 A warning that unauthorized use of the information system is prohibited and subject to administrative action, criminal and civil penalties;

5.5.1.1.4 Notification that information system usage may be monitored, recorded, and subject to audit; and

5.5.1.1.5 Notice that the use of the information system indicates consent to monitoring and recording.

5.5.1.2 The notification message or banner shall remain on the screen until the user takes an explicit action to log on to or further access the information system.

5.6 **Mobile Computing and Teleworking:** Security controls shall be implemented to protect against the unique risks introduced by accessing resources from potentially unprotected environments.

5.6.1 **Mobile Computing:** Wireless and remote access methods and controls, including wireless local area network (WLAN) access, shall use only approved and supported remote access methods and enforce required resource controls.

5.6.1.1 It is prohibited to allow offshore access to state computer systems via virtual private networks.

5.6.1.2 Users shall sign all applicable Mobile Device Acknowledgement and/or Remote Access User Acknowledgements prior to being given access to mobile computing resources.
5.6.2 **Teleworking**: If users have approval to engage in teleworking in accordance with DAS Policy 200-14, “Teleworking,” procedures shall be in place to mitigate and address the added risks associated with teleworking and remote access to resources. Users shall be required to adhere to state and agency policies, standards, and contracts while accessing resources via a teleworking environment.

### 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](http://example.com) 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 access control requirements outlined in the policy. A general implementation framework for the requirements of this policy includes:

7.1 The access controls for existing sensitive or business critical DAS-managed system assets shall be implemented within six months from the effective date of the policy.

7.2 All planned and future DAS-managed system asset development initiatives or system asset procurements, shall immediately comply with the access controls outlined in this policy.

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

### 8.0 DEFINITIONS

**Access Control** - Process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities.\(^1\)

**Account Administrator** – For the purposes of this policy, this is an individual who can create, activate or deactivate system accounts as well as assign access privileges or permissions to users.

---

Authentication - Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.²

Authorization - A grant to a requesting entity (computer, system, person or process) for access to a protected system and its resources. Not all entities will have access to all state information. Authorization requirements can be implemented using techniques such as access control lists, file and resource permissions, and digital certificates.

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 Label - 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.³

Data Owner - The data owner is responsible for the identification and classification of information, in consultation with Legal Counsel, and shall address the assignment of data classification labels, data compilation, data classification coordination, data classification compliance and data access. The role of a data owner and his/her associated responsibilities are addressed in detail within Ohio Administrative Policy IT-13, “Data Classification.”

Firewall - A device or program that controls the flow of network traffic between networks or hosts that employ differing security postures.⁴

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.⁵


**Information** - Data processed into a form that has meaning and value to the recipient to support an action or decision. “Information” is often used interchangeably with “data” in common usage and in this policy.

**Information Assets** - Data that is created, processed and used by the business. The information may be stored in paper copies as well as electronic files (e.g., hard drives, USB flash memory devices, CD's, DVD's, back-up tapes etc.).

**Information Technology (IT) Resources** - Any information technology resource, such as computer hardware and software, IT services, telecommunications equipment and services, digital devices such as digital copiers and facsimile machines, supplies and the Internet, made available to employees, contractors, temporary personnel and other agents of the state in the course of conducting state government business in support of agency mission and goals.

**Least Privilege** - The security objective of granting users only those accesses they need to perform their official duties.  

**Mobile Computing** - Refers to a variety of mobile devices (e.g., laptop, tablet or smartphone) that allow users to access data and information from anywhere and at any time.

**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** - “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.  

**Remote Diagnostic** - Provide the ability to assess the overall integrity and efficiency of a system network from a remote location. The remote diagnostic can also identify issues that are inhibiting the efficiency of the equipment, and sometimes even resolve those issues during the running of the diagnostics. The diagnostic process utilizes wired or wireless communication to conduct the remote analysis.

**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.

**Screen Lock** - An information system session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen. A screen lock requires authentication to access the data. Screen locks can be activated manually or in response to rules.

**Segmentation** - Dividing a computer network into sub-networks, each being a network segment or network layer. Network segmentation boosts performance and improves security.

**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.

---

**Service Owner** - A service owner is responsible for the delivery (design, performance, integration), continual improvement and management of assigned IT services.

**Session Lock** - A temporary action taken by an information system to lock a connection to an application or system in a window or screen after a defined time period of inactivity or upon a request by the user until the user reestablishes access using established identification and authentication procedures.

**Teleworking** - The ability for an organization’s employees and contractors to perform work from locations other than the organization’s facilities.

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

**Utility Programs** - Utility programs are designed to aid in the management and tuning of operating systems, computer hardware and application software. Utility programs perform a specific task related to the management of computer functions, resources, or files (e.g., password protection, memory management, virus protection, and file compression).

**Wireless Local Area Network (WLAN)** - A group of wireless networking devices within a limited geographic area, such as an office building, that exchange data through radio communications. The security of each WLAN is heavily dependent on how well each WLAN component—including client devices, APs, and wireless switches—is secured throughout the WLAN lifecycle, from initial WLAN design and deployment through ongoing maintenance and monitoring.

### 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

---


---

Service, Support, Solutions for Ohio Government  
The State of Ohio is an Equal Opportunity Employer  
Page 11 of 12
ACCESS CONTROLS POLICY 2100-11

http://das.ohio.gov/Divisions/AdministrativeSupport/EmployeeServices/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>10/10/2017</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 maintenance review.</td>
</tr>
</tbody>
</table>

11.0 ATTACHMENTS

None.