

**INFORMATION SECURITY AND PRIVACY  
POLICY  
MOBILE COMPUTING**

---

IT POLICY NUMBER: 2100-02

EFFECTIVE DATE: 12/05/2012

APPROVED BY:



Robert Blair, Director  
Department of Administrative Services

**1.0 PURPOSE**

This policy addresses the use, management, and control of portable computing devices and remote access to IT resources owned, managed, or operated by the Department of Administrative Services (DAS).

**2.0 SCOPE**

This policy applies to all managers of DAS business units and IT systems using state-owned or privately-owned equipment to access DAS' IT resources. This policy also applies to remote connections used to access those IT resources.

Some cellular telephones have computing, data communication, or data storage capabilities; their use may also be subject to other DAS or statewide policies relating specifically to cellular telephones.

This policy does not apply to portable computing devices or access methods used by the general public to access government services electronically.

**3.0 BACKGROUND**

The use of portable computing devices and/or remote access to DAS' IT resources increases the potential risk to those resources and makes them more difficult to secure. Several statewide policies address these issues. This policy provides for DAS' compliance with those statewide policies and also specifies more stringent security measures where appropriate.

## 4.0 REFERENCES

- 4.1. **NIST Special Publication 800-53 (Rev 3), Recommended Security Controls for Federal Information Systems and Organizations**, provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government.
- 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 800-53, revision 3 as the framework for information security controls implementation for the state.
- 4.3. **Ohio IT Standard; ITS-SEC-01; Data Encryption and Cryptography**: This state IT standard defines the minimum cryptographic algorithms that are cryptographically strong and are used in security services that protect at-risk or sensitive data.
- 4.4. **Ohio IT Bulletin; ITB-2007.02; Data Encryption and Securing Sensitive Data**: This state IT bulletin provides guidance to agencies as they take steps to protect sensitive data and information.
- 4.5. **DAS Policy; 700-01, IT Resource Usage**: This DAS policy establishes controls on the use of IT resources in accordance with Ohio IT Policy ITP-E.8, "Use of Internet, E-mail and Other IT Resources."
- 4.6. **DAS Procedure; Incident Response**: This DAS procedure defines the steps to follow for DAS' response to any type of critical incident, including security incidents, that affects DAS' applications, systems, networks, infrastructure or capability to deliver services.
- 4.7. **DAS Procedure; Portable Computing Lost & Stolen Device Handling**: This DAS procedure defines the steps to follow if a DAS portable computing device is lost or stolen.
- 4.8. A glossary of terms found in this policy is included in Section **8.0 – Definitions**.

## 5.0 POLICY

DAS is issuing this policy to ensure compliance with related state policies and to protect DAS' IT resources. More detailed security standards and procedures supporting the implementation of this policy will be maintained separately.

### 5.1 Remote Access

- 5.1.1. DAS shall authenticate all remote users. Only pre-approved users shall have access to state systems. At a minimum, a user-ID and password are required. For

data and other system assets identified as requiring secure access, two-factor authentication is required.

- 5.1.2. DAS shall grant permission for remote access following the least-privilege method, giving only the minimum levels of access needed to perform job responsibilities. DAS shall regularly review remote access privileges of all users for compliance with the least-privilege method and take appropriate corrective action when needed.
- 5.1.3. DAS shall revoke access privileges immediately upon notification of the separation or termination of any employee with remote access privileges or immediately upon request by an appropriate authority if an employee is under investigation or placed on Administrative Leave and the revocation has been approved by the Human Resource Administrator.
- 5.1.4. DAS shall regularly review remote access usage logs and suspend or revoke access for inactive users as appropriate.
- 5.1.5. Dial-in access to DAS owned and operated networks or systems shall be strictly controlled through a centralized modem pool.
- 5.1.6. The quantity of dial-in numbers shall be limited to the minimum needed to support the user population. Dial-in access numbers shall be considered confidential and only provided to those individuals with a valid, active dial-in account.
- 5.1.7. Remote access connections from the Internet shall be secured in accordance with DAS security policies.
- 5.1.8. If an agency customer provides DAS with a written copy of its remote access policy, DAS shall ensure that the connection and associated session activity are in compliance with that agency's remote access policy as well as this DAS policy, utilizing the stricter controls in cases of discrepancy.
- 5.1.9. DAS shall ensure that all remote access host servers are securely configured by establishing appropriate standards and procedures for their operation in accordance with guidance provided in the AC family of controls within NIST Special Publication 800-53.
- 5.1.10. Pursuant to Ohio IT Bulletin; ITB-2007.02, "Data Encryption and Securing Sensitive Data" and Ohio IT Standard, ITS-SEC-01, "Data Encryption and Cryptography," passwords that are transmitted shall be encrypted. Data requiring secured access shall be encrypted for transit between remotely accessed systems.

- 5.1.11. In accordance with Ohio IT Policy ITP-E.8, "Use of Internet, E-mail and Other IT Resources" and DAS Policy 700-01, "IT Resource Usage," the DAS employee, contractor, vendor, or agent is responsible to ensure that access accounts are not used to violate any DAS and/or state policies, perform illegal activities, or to facilitate any outside business interests and bears responsibility for the consequences if access is misused, unless it can be shown that the activity was the result of theft or fraudulent use by another person. Accessing the Internet for personal use through the DAS/OIT/ISD network via a remote access account is not permitted.

## 5.2 Portable Computing Devices

- 5.2.1. DAS shall establish standards and procedures for the acquisition, registration, use, and support of DAS-owned portable computing devices. Security controls shall be implemented for these devices in accordance with NIST Special Publication 800-53. At a minimum, device users are responsible for assuring that a DAS-owned device is inventoried and identified as a state asset, appropriately secured, and surrendered upon termination of employment. DAS shall also establish standards and procedures for the use, registration, and support of privately-owned devices used to access DAS' IT resources.
- 5.2.2. DAS retains ownership of any portable computing device purchased using DAS funds or otherwise acquired by DAS. DAS-owned and privately-owned devices are subject to DAS and statewide policies concerning access to and use of state IT resources and other state assets. (See Section 4.0 – References above.)
- 5.2.3. DAS requires immediate reporting for lost or stolen portable computing devices, state-owned or privately-owned, authorized for work use with systems or networks owned or managed by DAS. DAS' reporting processes are documented in DAS Procedures: "Incident Response" and "Portable Computing Lost & Stolen Device Handling."
- 5.2.4. If a portable computing device, state-owned or privately-owned, will be used to send or receive electronic mail via a state account, the device must be registered with DAS/OIT/ISD Exchange/Outlook Mail Services. This provision does not apply when the device is used to access e-mail solely via a web interface.
- 5.2.5. If a portable computing device is shared among multiple users, a single log shall be maintained to track the responsible user and the dates and times the device was checked in and out.
- 5.2.6. Users of portable computing devices, DAS-owned or privately-owned, used for state work shall not have any expectation of personal privacy regarding the device, data stored on the device, or state IT resources accessed using the device. Such devices are subject to audit and may be confiscated as evidence in

civil or criminal proceedings. The device user must produce the device and provide access to its contents upon request by DAS or its agents with or without prior notice.

5.2.7. DAS is not liable for the safeguarding or maintenance of non-state data or privately-owned portable computing devices used in support of official state business or while acting as an agent of the state. DAS is under no obligation to provide support for the use of privately-owned devices. If DAS chooses to provide limited support in some cases, standards and procedures will be established to do so.

5.2.8. DAS shall establish standards and procedures regarding the security of portable computing devices in accordance with guidance provided in NIST Special Publication 800-53; whether the devices are DAS-owned or privately-owned but authorized for use with state systems or networks. Issues addressed by the standards or procedures shall include, but are not limited to, the following:

- Physical security of the device
- Preventing unauthorized access to data transmitted, received, or stored using the device
- Device configuration
- Data backups
- Connectivity restrictions
- Data synching
- Software
- Security notifications
- Identification and authentication controls
- Internet connectivity
- Audits

## 6.0 RELATED PROCEDURES

DAS Procedure: Incident Response

DAS Procedure: Portable Computing Lost and Stolen Device Handling

DAS Procedure: Portable Computing Inventory and Audits

Additional standards and procedures shall be developed at various levels within the DAS organization in order to effectively and efficiently implement this policy. (See multiple references to standards and procedures above.)

At a minimum:

- This policy shall be distributed to each newly hired DAS employee during orientation, in conjunction with other applicable policies, procedures, and standards; the new employee shall sign an acknowledgement of receipt of this policy.

- Vendors, contractors, and temporary employees shall receive a copy of and sign an acknowledgement of receipt of this policy prior to gaining access to IT resources.

## 7.0 COMPLIANCE

It is the responsibility of management to implement and ensure compliance with the laws, rules, policies, procedures, standards, and license agreements applicable to the use of IT resources within their functional areas.

## 8.0 DEFINITIONS

**DAS** – Department of Administrative Services.

**DAS Contractors** – For the purposes of this policy, DAS contractors are defined as contracted staff and vendor technicians.

**DAS Employees** – For the purposes of this policy, DAS employees are defined as all employees and representatives of DAS, whether they are permanent staff or temporary staff.

**DAS-owned** – Purchased with DAS funds or otherwise acquired by DAS; property of DAS.

**DAS-provided** or **DAS-supplied** – Made available to users by DAS.

**Inactive User/Account** – A username or account that has not been used for a predetermined period of time. Time periods vary in length depending upon the IT system, network, or other resource being accessed.

**IT Resources** – Any information technology resources, such as computer hardware and software, IT services, telecommunications equipment and services, networks, digital devices such as digital copiers and facsimile machines, supplies, and the Internet.

**Least-Privilege** - A method that assigns privileges in a system. The objective is to assign only those privileges that are necessary to perform the required functions, and ensure that other privileges are not assigned and cannot be improperly accessed. For example, a normal system user should not be assigned rights to read, write and execute all of a department's files when that user only requires the ability to read a subset of the files to do the assigned job.

**Management** – Management refers to supervisory staff responsible for the completion of activities to fulfill DAS' mission. If Position A is shown as subordinate to Position B on the Table of Organization, then Position B is supervisory in nature for the purposes of this policy.

**OIT** – Office of Information Technology.

**Portable Computing Device** - Computer or device designed for mobile use. Examples include laptops, personal digital assistants and mobile data collection devices.

**Privately-owned** - Purchased with personal or corporate (vendor or contractor) funds; not provided by the state.

**Remote Access** – A service that enables a device to connect to a network or application. The device making the connection is at a location apart from that of the network or application and is not a physical or wireless extension of the Local Area Network.

**Revoked Access** – Revoked accounts require that the user be re-authenticated before access is reactivated.

**State-owned** - Purchased with state funds or otherwise acquired by the state; property of the state of Ohio.

**Suspended Access** – A reset feature may be used to reactivate suspended accounts, e.g., prompting a user to provide an additional piece of information that only he or she would know.

**Two-factor Authentication** - Authentication that incorporates two elements. There are three elements of authentication: “what you know” (for example, a password or PIN), “what you have” (for example, a digital certificate, security token or a smart card), and “what you are” (for example, a biometric). Two-factor authentication is commonly used for access to systems that contain data requiring secured access or information of which disclosure would cause serious disruption or harm. It is also known as “strong authentication,” although strong authentication can have more than two elements.

**Users** - For the purposes of this policy, users are defined as employees, contractors, temporary personnel and other agents of the state who administer or use privately-owned (if authorized) or state-owned IT Resources on behalf of the state.

## 9.0 INQUIRIES

For information regarding this policy, please contact:

Office of Information Security & Privacy  
Office of Information Technology  
Ohio Department of Administrative Services  
30 East Broad Street, Suite 4083  
Columbus, Ohio 43215  
Telephone: 614.644.9391  
Email: [state.isp@oit.ohio.gov](mailto:state.isp@oit.ohio.gov)  
Web: [infosec.ohio.gov](http://infosec.ohio.gov)

Department of Administrative Services policies can be found online at:

<http://das.ohio.gov/Divisions/DirectorsOffice/EmployeeServices/DASpolicies/tabid/463/Default.aspx>

### 10.0 REVISION HISTORY

Date	Description
12/01/2009	New policy for DAS, replaces OIT policy dated 11/02/07
12/05/2012	Policy reissued under Director Robert Blair.

### 11.0 ATTACHMENTS

None.