



# INFORMATION SECURITY AND PRIVACY POLICY SECURITY EDUCATION AND AWARENESS

---

IT POLICY NUMBER: 2100-05

EFFECTIVE DATE: 12/05/2012

APPROVED BY:

A handwritten signature in black ink, appearing to read "Robert Blair", written over a horizontal line.

Robert Blair, Director  
Department of Administrative Services

## 1.0 PURPOSE

Security awareness and education are necessary so that users of Department of Administrative Services (DAS) systems and networks understand their responsibilities with regard to protecting information. This policy provides the requirements for DAS' information technology (IT) security education and awareness program.

## 2.0 SCOPE

The scope of this policy includes all DAS computer and telecommunications systems and the managers of DAS business units and IT systems who use or administer such systems.

## 3.0 BACKGROUND

DAS personnel should understand how and why an IT security program is implemented. Since all personnel will play a critical role in DAS' security profile, inadequate education and awareness programs can lessen DAS' ability to adequately safeguard its IT assets and information. Failure to educate people on how to protect information resources can result in compromise of DAS' sensitive and confidential information. In order for an IT security program to be most effective, personnel should be effectively and routinely informed of deployed IT security measures so that they understand how the measures align with DAS' business objectives and why they exist. An effective IT security program heightens security awareness and establishes individual responsibility.

## 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 800-53, revision 3 (NIST 800-53) as the framework for information security controls implementation for the state.
- 4.2. **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.
- 4.3. **Ohio IT Bulletin ITB-2006.01:** Notifies state agencies that Ohio's public records law exempts certain types of security and infrastructure records from mandatory release to protect critical information regarding agency security practices and vulnerabilities.
- 4.4. **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.
- 4.5. 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.

DAS shall establish an IT security education and awareness program in order to assure that all employees, contractors, temporary workers and agents who use or operate DAS information systems understand and adhere to all security policies. The requirements of this policy include:

- 5.1 Security Awareness. DAS programs, with support from the Office of Information Security and Privacy, shall coordinate and conduct ongoing IT security awareness training for all program personnel. As a minimum, the training shall include:

- 5.1.1 How DAS' IT security policies meet the business objectives of DAS, identifying the system assets that need to be protected.
- 5.1.2 Identification of the most likely threats to the DAS IT environment, such as:
  - Insider abuse and mistakes
  - Viruses and other malicious code
  - Unauthorized access

- Social engineering
- Inadequate password creation, protection and maintenance

5.1.3 An overview of the risk management process used by DAS.

5.1.4 Identification of security responsibilities for all personnel levels including, but not limited to:

- Compliance with all password requirements
- Physical security
- Workstation security
- Portable computing security
- Reporting security events
- Data classification
- Data retention, safeguarding and disposal

5.2 Security Notifications. DAS shall use security notifications for all public and nonpublic systems, including web-based applications. Use of security notifications shall comply with DAS standards for composition of notification and presentation of notification and procedures for legal review.

5.3 General IT Security Education. DAS shall incorporate IT security education as part of the orientation for new employees, contractors, temporary personnel and other agents of the state. Thereafter, education programs shall be offered at a minimum biennially. As a minimum, such education shall include:

5.3.1 A description of the elements of the risk management process as defined by DAS.

5.3.2 A description of DAS IT security policies and the rationale of how they mitigate risk and complement the business objectives of the state.

5.3.3 A review of the applicable laws, regulations, and state policies, including state and individual liabilities.

5.3.4 Communication of the consequences of noncompliance with DAS policies, state IT security policies, related laws, regulations and other policies.

5.4 Technical Education. Technical IT security education shall be administered at a minimum on an annual basis for DAS personnel responsible for implementing secure solutions. Technical education may include as applicable, but not be limited to:

5.4.1 Education and certifications for IT security technologies and practices, such as:

- Firewalls
- Wireless
- Routers
- Switches
- Virtual private networks
- Encryption
- Public key infrastructure
- Technical procedures and methodologies
- Implementing secure solutions at each stage of the software development lifecycle
- Data protection
- Audit logging

5.4.2 Overview of why security notifications are necessary, the types of notifications, and the justification behind employing various types.

5.4.3 Education for reporting IT security incidents and responding to them in accordance with DAS and statewide policies.

5.4.4 Formal course work in IT security technologies.

5.4.5 Conferences.

5.5 Executive Education. DAS shall administer executive education programs biennially to all executive-level DAS personnel. As a minimum, education programs shall include the following elements, specific to DAS:

5.5.1 State and individual roles, responsibilities and liabilities.

5.5.2 Current risk assessment, management and incident response capabilities.

5.5.3 Current threats.

5.5.4 Current countermeasures.

5.5.5 Deficiencies of applicable resources.

5.5.6 Status of all security incidents.

5.5.7 Impact of security incidents.

5.5.8 Incident response successes and failures.

5.5.9 Division of responsibilities during an IT security incident.

5.5.10 Internal and media communication schedules for an IT security incident.

5.5.11 A description of agency IT security policies and the rationale of how they mitigate risk and complement the business objectives of the state.

5.6 Measures and Records. DAS shall maintain records of IT security education programs and attendance. In addition, metrics, such as participant surveys or test scores, measuring the effectiveness of a program shall be maintained by the Office of Information Security and Privacy and referenced during program design sessions. Pursuant to §149.433 of the Ohio Revised Code, security related records are exempt from public disclosure. Security education and awareness programs shall be reviewed and updated periodically to reflect new trends, threats or identified agency IT security breaches.

5.7 Methods. DAS shall define the appropriate methods used for each type of awareness and education program, such as:

- Posters
- Computer-based training
- Web-based education
- Intranet materials and resources
- Videos
- Newsletters
- Memoranda
- Briefings
- Formal classroom instruction
- On-the-job training
- Conferences
- Security notifications

5.8 Public Records Requests. Elements of this policy involve the creation of records that may not be subject to disclosure under Ohio's public records law. When considering public records requests that are related to security or infrastructure records, refer to Ohio IT Bulletin ITB-2006.01 or §149.433 of the Ohio Revised Code.

## 6.0 PROCEDURES

Standards and procedures shall be developed at various levels within the DAS organization in order to effectively and efficiently implement this policy.

## 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.

**Communications Schedule** - A pre-defined structure that delineates the communications strategy for a given event. Elements include who delivers the communication, which personnel are the intended recipients, the format of the communications, the timeline and a record of the accomplishment of each. Communications schedules are implemented in business continuity and risk management planning or other situations where senior officials must ensure that information is disseminated.

**Identification and Authentication (I&A)** - The verification of the identity of a requesting entity (a person, computer, system or process). Once it is determined who may have access to a system, the identification and authentication process helps to enforce access control to the system by verifying the identity of the entity. Systems may use a variety of techniques or combinations of techniques such as user-ID, password, personal identification number, digital certificates, security tokens or biometrics to enforce I&A depending upon the level of access control required to protect the system.

**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.

**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.

**Nonpublic System** - A state computer and telecommunication system for use by employees, contractors, temporary personnel and other agents of the state. Examples of such systems would include payroll or benefit related systems that do not grant access to the general public.

**OIT** – Office of Information Technology.

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

**Public Record** – Any record defined as public by the Ohio Revised Code.

**Public System** - A state computer or telecommunications system used in whole or in part by individuals such that the use is not based on employment or contractual relationships with the state. Examples of such systems would include online applications that allow users from the general public to execute transactions, request documentation, or view information.

**Risk Assessment** – A process for identifying, analyzing and responding to information technology security risks. Risk assessment attempts to maximize the results of positive events and minimize the results of negative events.

**Security Notifications** - An obvious or apparent statement that describes a limitation on use, a duty, a restriction and possible consequences for illegal or unauthorized access or attempted access to a system.

**Social Engineering** - The manipulation of a person through spying, theft or deception for the purpose of obtaining confidential or security compromising information.

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

**System Assets** – System assets include information, hardware, software, and services required to support the business of DAS and identified during the risk assessment process as assets that require protection.

**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.