
State of Ohio Administrative Policy

IT Security Awareness and Training

No:
Information Technology
IT-15

Effective:
July 21, 2015

Issued By:



Robert Blair, Director

1.0 Purpose

This policy provides information technology (*IT security awareness and training*) requirements for State of Ohio *information system users*, which includes employees, contractors, temporary personnel and other agents of the state. This policy is not intended for the general population that accesses electronic government services or applications.

A glossary of terms found in this policy is located in Appendix A - Definitions. The first occurrence of a defined term is in *bold italics*. In addition, references to National Institute of Standards in Technology (NIST) Special Publication (SP) 800-53 family identifiers and control numbers are provided in parentheses next to requirement headers, where applicable.

2.0 Policy

State agencies shall conduct IT security awareness training in accordance with the requirements outlined in this policy and shall ensure that all information system users adhere to the policy.

2.1 ***Security Awareness Training (AT-2)***: The Department of Administrative Services (DAS) Office of Information Security and Privacy (OISP) shall provide basic information security awareness training for agencies to use to conduct this training.

2.1.1 DAS OISP shall identify and provide a solution for delivering the basic IT security awareness training statewide.

2.1.2 The DAS OISP training shall be updated annually to ensure it remains current, addressing the latest security threats and best practices.

2.1.3 Agencies shall ensure that all information system users complete the DAS OISP basic IT security awareness training.

2.1.3.1 Users shall complete the basic IT security awareness training within two weeks of their initial hire date, annually thereafter; and when required by role or system changes.

2.1.4 Agencies shall determine if it is necessary to augment DAS OISP's basic IT security awareness training due to agency specific requirements or any applicable laws, regulations, or industry codes that require some type of IT security training for the information systems to which personnel have authorized access. Examples of regulations or laws that require additional security training, include:

- Accessing **Confidential Personal Information (CPI)** (Section 1347.15 of the Ohio Revised Code)
- Family Educational Rights and Privacy Act (FERPA)
- IRS Publication 1075
- FBI Criminal Justice Information Services (CJIS) Security Policy
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI-DSS)

2.1.5 As appropriate, each agency shall supplement the basic IT security awareness training with tools that will help communicate local or programmatic information security issues, incidents, and procedures (e.g., "message of the day," posters, special events, e-mail notices).

2.2 **Role-Based Security Training (AT-3):** In addition to basic IT security awareness training, agencies are encouraged to provide role-based security training that focuses on the unique responsibilities for protecting state assets that are inherent in particular job functions. Certain roles may require more targeted training, such as business managers, senior executives, information owners, application developers, systems administrators, database administrators, and desktop support.

2.2.1 Agencies shall identify the job functions that require additional role-based training and then determine the format, content, and frequency of the training. Listed below are a few examples of role-based training:

Business managers and senior executives:

- The safeguarding and use of **personally identifiable information (PII)**
- Executive targeting threats such as social engineering and **spear phishing**
- Identification of suspicious messages and the importance of not opening suspicious e-mails or attachments
- Examples of prominent cyberattacks

Application developers, system administrators and database administrators:

- How to write secure code and use appropriate validation tools

- Proper security testing methods
- How to handle **sensitive data**

Desktop Support:

- **System hardening** techniques
- How to recognize attacks
- Handling systems infected with **malware**

2.2.2 DAS OISP shall help inform and support these efforts through a variety of channels, such as security communications (e.g., current threats, countermeasures, or training opportunities), best practices research and resources, security briefings or conferences.

2.3 **IT Security Awareness and Training Management:** Agencies shall ensure that all information system users meet the training requirements of this policy by identifying, monitoring and managing the overall IT security education effort.

2.3.1 Agencies shall identify all individuals requiring basic IT security awareness and role-based training.

2.4 **Security Training Records (AT-4):** Individual security training records shall be maintained, in accordance with agency record retention requirements, to ensure that basic IT security awareness and role-based training requirements are being fulfilled.

2.5 **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.

2.5.1 The form is located within the [IT Enterprise Services Portal](#) under the “Services & Products” category.

2.5.2 If you have any questions, please contact DAS OISP (refer to Section 5.0 Inquiries for contact information).

2.6 **Implementation:** Agencies that do not have IT personnel shall contact the DAS Office of Information Security & Privacy to determine an appropriate approach for compliance.

3.0 Authority

ORC 125.18

4.0 Revision History

Date	Description of Change
07/21/2015	Original policy.
04/10/2018	References to NIST SP 800-53 control families were added to the requirements, where appropriate. A definition of sensitive data was also added. The

	exception request section was removed and procedural guidance was added in its place. The implementation section was modified due to the time elapsed since the publication of the policy on 7/21/15.
11/21/2018	Updated the exception request language to align with the current procedure.
11/21/2019	Scheduled policy review.

5.0 Inquiries

Direct inquiries about DAS OISP IT security training or 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

State of Ohio Administrative Policies may be found online at
www.das.ohio.gov/forStateAgencies/Policies.aspx

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

Appendix A - Definitions

- a. Availability. Ensuring timely and reliable access to and use of information.¹
- b. Basic IT Security Awareness Training. The purpose of this type of training is for the participant to gain a basic understanding of the need for information security and the actions that he/she can take to maintain security and respond to suspected security incidents. This training also increases awareness regarding the importance of operations security.
- c. Confidential Personal Information (CPI). Personal information that falls within the scope of Section 1347.15 of the Ohio Revised Code and that an agency is prohibited from releasing under Ohio's public records law.
- d. Confidentiality. Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.²

¹ "NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations," U.S. Department of Commerce National Institute of Standards and Technology, April, 2013 <<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>>.

² *Ibid.*

- e. Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.³
- f. Integrity. Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.⁴
- g. IT Security Awareness and Training. IT security awareness training is a formal process for educating employees about computer security.
- h. Malware. A program that is inserted into a system, usually covertly, with the intent of compromising the **confidentiality**, **integrity**, or **availability** of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.⁵
- i. 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.
- j. Role-Based Security Training. Role-based training strives to produce relevant and needed security knowledge and skills within the workforce. Role-based security training supports competency development and helps personnel understand and learn how to better perform their specific security role, which ultimately achieves more secure and protected information and systems.
- k. 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

³ *Ibid.*

⁴ *Ibid.*

⁵ Souppaya, Murugiah, Karen Scarfone. "NIST Special Publication 800-83, Revision 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops" U.S. Department of Commerce National Institute of Standards and Technology, July 2013, <<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf>>.

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.

- l. Spear Phishing. Phishing is the act of tricking individuals into disclosing sensitive personal information through deceptive computer-based means.⁶ “Spear” phishing is a highly targeted attack aimed at a specific individual(s).

- m. System Hardening. The process of enhancing the default or basic security layers associated with an application and/or network. The primary purpose of system hardening is to increase the level of system security to dissuade and defeat intrusion or security breach attempts. Hardening concepts may include, but are not limited to, the application of system or application patches, removal of all unnecessary system features or services, shutting down of all unnecessary ports, incident logging, installation of a demilitarized zone (DMZ), packet filtering, cryptography, strong authorization, data encryption, and system/network monitoring and/or auditing.

- n. User. A user is defined as employees, contractors, temporary personnel and other agents of the state who administer and use state computer and telecommunications systems on behalf of the state. For the purposes of this policy, a user is not a member of the general population that accesses electronic government services or applications.

Appendix B - Resources

Document Name
<i>NIST Special Publication 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013:</i> http://csrc.nist.gov/publications/PubsSPs.html
<i>Ohio IT Standard ITS-SEC-02, “Enterprise Security Controls Framework”:</i> http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITStandards.aspx
<i>Center of Internet Security (CIS) Controls:</i> https://www.cisecurity.org/controls/
<i>Multi-State Information Sharing & Analysis Center (MS-ISAC) Resources:</i> http://msisac.cisecurity.org/resources/

⁶ Souppaya, Murugiah, Karen Scarfone. “NIST Special Publication 800-83, Revision 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops” U.S. Department of Commerce National Institute of Standards and Technology, July 2013, <<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf>>.