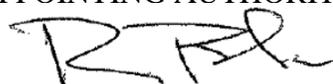


## INFORMATION TECHNOLOGY RESOURCE USAGE

POLICY NUMBER: <p style="text-align: center;">700-01</p>	EFFECTIVE DATE: <p style="text-align: center;">05/04/2015</p>	APPOINTING AUTHORITY APPROVAL: 
REPLACES POLICY DATED: <p style="text-align: center;">04/23/2012</p>	AUTHORITY: Ohio Administrative Policy IT-04, "Use of Internet, E-mail and Other IT Resources " (5/4/2015)	

### 1.0 PURPOSE

The purpose of this policy is to minimize the risks and maximize the benefits of using information technology (IT) resources and to maintain the integrity and stability of computer and network hardware, software, data, and related services within the Department of Administrative Services (DAS). An IT resource is described as computer hardware and software, IT services, telecommunications equipment and services, digital devices such as digital copiers and facsimile machines, supplies, and the Internet. This policy addresses the acceptable use of IT resources in the DAS workplace and/or for DAS business.

### 2.0 SCOPE

This policy applies to IT resources used by employees, contractors, temporary personnel, and other agents of the state for DAS business or used within the DAS work environment. This policy does not apply to external DAS customers.

### 3.0 BACKGROUND

Technology is a critical component of our daily business lives. DAS provides IT resources to employees, contractors, temporary personnel and other agents of the state to support the work and conduct the business of Ohio government. Users of DAS IT resources hold positions of trust both in preserving the security and confidentiality of state information and in safeguarding IT resources. Any potential loss of sensitive data (refer to Section 8.0 for a definition of sensitive data) or IT resource availability can have a significant impact on DAS' ability to fulfill its mission. The requirements outlined in this policy will help users understand DAS' expectations with regard to appropriate use, and consequently will help minimize some of the risks that are inherent with the daily use of state IT resources.

DAS policy 700-01, "Information Technology Resource Usage," complies with the requirements outlined in Ohio Administrative Policy IT-04, "Use of Internet, E-mail and Other IT Resources."

### 4.0 REFERENCES

- 4.1 DAS Policy 100-02, "Employee Handbook: Introduction to HR Policies"
- 4.2 Ohio Administrative Policy IT-04, "Use of Internet, E-mail and Other IT Resources"

### 4.3 Ohio IT Bulletin ITB-2007.02, “Data Encryption and Securing Sensitive Data”

## 5.0 POLICY

The following policy statements outline DAS requirements for the use of state issued IT resources. The policy requirements are intended to clarify the distinction between the acceptable and unacceptable use of IT resources. In addition, the policy defines key privacy and security requirements. It is the expectation of DAS that employees, contractors, temporary personnel, and other agents of the state will comply with all of the components of this policy.

### 5.1 Use of IT Resources

#### 5.1.1 Ownership and Privacy

All data, text, images, or other information created, stored, transmitted, received, or archived using DAS’ IT resources belong to DAS, except for those items whose ownership is protected by law, contract, license agreement, copyright, or other agreement. All data stored or transmitted on a DAS IT resource may be subject to review, investigation and public disclosure.

When using DAS’ IT resources, the user shall have no expectation of privacy. Access and use of the Internet, including communication by e-mail and instant messaging and the content thereof, are not confidential, except in certain limited cases recognized by state or federal law.

DAS reserves the right to monitor, access, and disclose all information generated and actions performed using DAS’ IT resources. Files, messages (including attachments), and logs may be retained and used as evidence in litigation, audits, and investigations. The user is responsible for all activity originating from his or her username/account.

In addition, DAS IT resources are on loan to DAS employees, contractors, temporary personnel, and other agents of the state so that essential job functions may be performed. Upon separation from DAS employment or contract termination, all DAS supplied IT resources, and the associated data shall be returned.

#### 5.1.2 Damaged, Stolen, Lost, or Potentially Compromised IT Resources

If an IT resource is damaged, fails, or is believed to be stolen or lost, it shall immediately be reported to management and to the Customer Service Center. (Please find the Customer Service Center contact information in Section 9.0 of this policy.) In addition, employees, contractors, temporary personnel, and other agents of the state shall also report instances in which they think an IT resource may have been potentially compromised. For instance, a user may suspect that someone gained access to the data on their IT resource, possibly viewing and/or downloading sensitive data (refer to Section 8.0 for a definition of sensitive data) and/or personally identifiable information.

#### 5.1.3 Personal Use of IT Resources

DAS IT resources are provided for business use. However, incidental personal use of IT resources is allowed if the usage does not have an adverse impact on job performance, IT

resources, or DAS business. Management may further restrict personal use of IT resources where appropriate.

The user is responsible for understanding how his/her personal use may impact IT resources as well as DAS business activities, and for complying with all applicable laws, policies, rules, and license agreements. DAS is under no obligation to provide support for the personal use of DAS' IT resources.

#### **5.1.4 System, Network, and Data Security**

Users of DAS IT resources, to include agency provided wireless access, shall comply with all applicable policies, procedures, and standards related to the security of those resources.

Whenever users of desktop or laptop computers leave their work areas, they shall use one or more of the following methods to prevent unauthorized access to their computers, software, and/or data:

- Log off all accounts, including their computer and/or network user account.
- Lock their computers by using an approved password protected screensaver.
- Lock their computers by using operating system level workstation locking.
- Shut their computers down.

All files shall be stored on network file servers to facilitate back-up. Files maintained on the drives of desktop or laptop computers or on other mobile devices will not be centrally backed-up.

Data may not be removed from state premises without management authorization. Refer to section 5.2.2 of this policy for requirements regarding the transport of sensitive data.

Except for devices that are inherently mobile, such as laptops, smartphones and personal digital assistants (PDAs), IT equipment may be physically relocated only with appropriate authorization. Requests to move IT resources shall be made via the Customer Service Center. (Please find the Customer Service Center contact information in Section 9.0 of this policy.) The physical move of the IT resource is to be performed by DAS IT Services staff only.

Disposal of IT resources shall be coordinated by IT Services and accomplished in accordance with Ohio IT policies and DAS policies and procedures.

## **5.2 Unacceptable Use of IT Resources**

Any use of IT resources that disrupts or interferes with DAS business, incurs an undue cost to the State, could potentially embarrass or harm the State, or has the appearance of impropriety is strictly prohibited.

### **5.2.1 Prohibited Use**

Use that is strictly prohibited includes, but is not limited to, the following:

1. Violation of Law. Violating or supporting and encouraging the violation of local, state, or federal law is strictly prohibited.
2. Illegal Copying. Downloading, duplicating, disseminating, printing or otherwise using copyrighted materials, such as software, texts, music and graphics, in violation of copyright laws is strictly prohibited.
3. Operating a Business. Operating a business, directly or indirectly, for personal gain is strictly prohibited.
4. Accessing Personal Services. Accessing or participating in any type of personals advertisements or services, such as or similar to dating services, matchmaking services, companion finding services, pen pal services, escort services, or personal advertisements is strictly prohibited.
5. Accessing Sexually Explicit Material. Downloading, displaying, transmitting, duplicating, storing or printing sexually explicit material is strictly prohibited.
6. Harassment. Downloading, displaying, transmitting, duplicating, storing or printing material that is offensive, obscene, threatening or harassing is strictly prohibited.
7. Gambling or Wagering. Organizing, wagering on, participating in or observing any type of gambling event or activity is strictly prohibited.
8. Impeding Access. Impeding the state's ability to access, inspect and monitor IT resources (e.g., inappropriately encrypting or concealing the contents of files or electronic communications, inappropriately setting or manipulating passwords, physically concealing devices) is strictly prohibited.
9. Tampering with, circumventing or removing security controls. Security controls are put in place to protect IT resources. Employees, contractors, temporary personnel, and other agents of the state are prohibited from removing, tampering with or circumventing these security controls without the express written permission of the DAS IT Services Administrator.
10. Engaging in Unauthorized IT Related Activities. Engaging in IT related activities that are unauthorized and/or outside of one's job duties, and that could result in a security incident is strictly prohibited (e.g., denial of service attacks, attempts to intercept/collect data, introduction of malicious code, network monitoring/scanning).
11. Misrepresentation. Concealing or misrepresenting one's name or affiliation to mask unauthorized, illegal, fraudulent, irresponsible or offensive behavior in electronic communications is strictly prohibited.
12. Accessing or Disseminating Sensitive Data or Personally Identifiable Information. DAS employees, contractors, temporary personnel, and other agents of the state shall not access or disseminate sensitive data (refer to Section 8.0 for a definition of sensitive data) or personally identifiable information without authorization. DAS employees, contractors, temporary personnel, and other agents of the state shall comply with applicable rules and procedures before disclosing or providing access to public information.
13. Passwords. DAS employees, contractors, vendors, and agents with user access privileges to state IT resources shall not disclose their passwords to other parties, including internal staff. DAS employees, contractors, vendors, and agents shall not set or manipulate a password to impede access to any state computer, program, file or electronic communication without proper authorization.
14. Distributing Malicious Code. Distributing malicious code or circumventing malicious code security is strictly prohibited.
15. Peer-to-Peer File Sharing. The personal use of peer-to-peer file sharing from non-state computer systems is prohibited.

16. Mass E-mailing. Sending unsolicited e-mails or facsimiles in bulk or forwarding electronic chain letters in bulk to recipients inside or outside the state environment is strictly prohibited.
17. DAS Wireless. Privately-owned devices are not authorized to use the DAS wireless access point as an employee (DAS Employee), only state-owned equipment is approved. When using a privately-owned device on the DAS wireless network as a guest (DAS Guest), the employee, contractor, temporary personnel, and other agent of the state shall comply with all applicable policies, procedures, and standards related to the security of those resources.

## **5.2.2 Use Prohibited without Agency Authorization**

Use that is prohibited without proper authorization includes, but is not limited to, the following:

1. Solicitation. Except for agency approved efforts, soliciting for money or support, for example on behalf of charities, religious entities or political causes is strictly prohibited.
2. Unauthorized Installation or Use of Software. Installing or using software without proper agency approval is strictly prohibited. (See also Sections 5.3.2.2 and 5.3.3 of this policy.)
3. Unauthorized Installation or Use of Hardware. Installing, attaching, or connecting devices to DAS systems or networks without proper authorization is strictly prohibited.
4. Data Transport. Sensitive data (refer to Section 8.0 for a definition of sensitive data) is not to be transported from one location to another without management approval and must be transported using a secured, encrypted method provided and approved by DAS IT Services. A request to transport sensitive data should be made using the Customer Service Center. (Please find the Customer Service Center contact information in Section 9.0 of this policy.)
5. Accessing Systems without Authorization. Accessing networks, files or systems or an account of another person without proper authorization is strictly prohibited.
6. Use of Privately-owned e-mail accounts to conduct DAS or State business. Privately-owned e-mail accounts, including private web-based e-mail accounts, shall not be used to conduct DAS business unless specifically authorized, in writing, by management. DAS is under no obligation to provide support for privately-owned e-mail accounts. (See also Section 5.5.1 of this policy.)

## **5.3 Electronic Communications**

### **5.3.1 Professionalism**

DAS employees, contractors, temporary personnel, and other agents of the state shall use professional and appropriate language in all electronic communications. Sending abusive, harassing, threatening, menacing, discriminatory, pornographic, disrespectful, or otherwise offensive or embarrassing electronic communications is prohibited.

### **5.3.2 Electronic Mail (E-mail)**

#### **5.3.2.1 Use of DAS' E-mail System**

The DAS e-mail system is Microsoft Exchange and primarily uses Microsoft Outlook client software. E-mail accounts are provided by the DAS/OIT Exchange Mail Service group.

Policies, procedures, and standards applicable to the use of the Exchange Mail Service are published on the [DAS/OIT Exchange Email Service Site](#). The user of a DAS e-mail account shall abide by these policies, procedures, and standards as a condition of receiving access to the DAS e-mail system. Other statewide or DAS policies may also apply. Compliance is the user's responsibility.

DAS employees, contractors, temporary personnel, and other agents of the state shall avoid the appearance of impropriety and avoid the appearance of leveraging the stature of the State in the use of their assigned state e-mail address. State e-mail addresses shall not be used for personal communications in public forums such as or similar to listservs, discussion boards, discussion threads, online forums, or blogs.

#### **5.3.2.2 Use of Personal, Consumer-Grade E-mail Systems**

Downloading, installing, and/or using personal, consumer-grade e-mail client software to conduct DAS business via the public Internet or for personal use involving DAS' IT resources is prohibited. If there is a business need for e-mail usage, the potential user shall request access to DAS' e-mail system. When authorized by management, using an external e-mail account for transmission/connectivity testing purposes is an exception to this provision.

Access to personal e-mail directly via an Internet browser interface for personal use in the DAS workplace may be allowed if the usage does not have an adverse impact on job performance or IT resources. The user is responsible for understanding how the personal e-mail system they are using functions and for compliance with this policy.

Private web-based e-mail accounts shall not be used to conduct DAS business. In certain management approved circumstances, use of a private web-based e-mail account for DAS business may be acceptable. An example of such type of use may be to access information regarding professional association benefits (i.e. registered architects, licensed attorneys, etc.)

#### **5.3.3 Instant Messaging (IM) and Text Messaging**

Downloading, installing, and/or using personal, consumer-grade instant messaging (IM) client software is strictly prohibited. Only DAS supported IM solutions are permitted.

IM and text messaging shall not be used to conduct official DAS business. In order to ensure that DAS is able to preserve public records, IM and text messaging shall not be used to record an official act of government. In addition, DAS employees, contractors, temporary personnel, and other agents of the state must follow any applicable state policies, procedures, and standards.

Personal use of DAS supported IM and text messaging is permitted as long as the usage does not have an adverse impact on job performance or IT resources.

### 5.3.4 Social Media

Personal use of social media platforms (e.g., Facebook™, Twitter™, YouTube™, LinkedIn™) is permitted as long as the usage does not have an adverse impact on job performance or IT resources. Excessive personal use of social media platforms during work hours may result in discipline or termination. Personal use, either while at work (e.g., during break or lunch periods) or outside of work, shall be conducted in such a manner that a reader would not think that the employee, contractor, temporary personnel, or other agent of the state is speaking for or on behalf of DAS or the State of Ohio.

Employees, contractors, temporary personnel, and other agents of the state shall not include references or pointers to their personal social media accounts in official DAS or State of Ohio communications without express management authorization. (e.g., providing social media account pointers within personal state e-mail signature lines.)

Employees, contractors, temporary personnel, and other agents of the state are prohibited from creating or designing a social media channel that may appear to represent DAS or the State of Ohio without authorization from the DAS Division Deputy Director and the DAS Office of Communications and External Relations.

While engaged in personal or official state use, do not discuss information related to DAS or Ohio that is not already considered public information. The discussion of sensitive or personally identifiable information is strictly prohibited. This applies even in circumstances where passwords or other privacy controls are implemented. In addition, all of the requirements regarding prohibited and appropriate use outlined within this policy and Ohio Administrative Policy IT-04, "Use of Internet, E-mail and Other IT Resources," also apply to authorized social media use.

Use of such sites must be in compliance with relevant portions of DAS workplace policies, including its harassment, discrimination, confidentiality, and workplace violence policies, as well as with state ethics laws, federal copyright law, and other applicable policies, laws, and regulations. Some of these policies, for example DAS' sexual harassment policy and the ethics rules, could apply to employees, contractors, temporary personnel, and other agents of the state actions performed outside of normal working hours at third party sites. DAS employee policies are available online:

<http://www.das.ohio.gov/Divisions/AdministrativeSupport/EmployeeServices/DASPolicies.aspx>.

## 5.4 Cloud Storage Solutions

### 5.4.1 Restrictions on Use of Cloud Storage Solutions

Microsoft OneDrive for Business and SharePoint Online are the DAS approved solutions for storing and sharing documents in a cloud environment. The following restrictions apply to the use of the DAS Microsoft OneDrive for Business and SharePoint Online solutions:

1. Data Storage: Only data related to state business shall be stored on the DAS Microsoft OneDrive for Business and SharePoint Online solutions. Personal data shall not be stored on the DAS Microsoft OneDrive for Business and SharePoint Online solutions.
2. Sensitive Data Storage: Sensitive data shall not be stored in Microsoft OneDrive for Business. Sensitive data storage is permitted in SharePoint Online if rights management and data encryption is implemented. Data encryption shall be in alignment with the requirements outlined in Ohio IT Bulletin ITB-2007.02, “Data Encryption and Securing Sensitive Data.” (Refer to Section 8.0 for a definition of sensitive data.)
3. Use of Other Cloud Storage Solutions: The use of any other cloud storage solutions for state business is strictly prohibited unless organized or approved by DAS.

## **5.5 Public Records and eDiscovery**

### **5.5.1 Public Records and Record Retention**

Employees, contractors, temporary personnel, and other agents of the state shall understand that records created as a result of the use of state-provided IT resources may be subject to disclosure under Ohio’s public records law and must be retained in accordance with state and agency record retention schedules.

The nature of the data or information determines if it is a public record, not the account, device, or method used to create, transmit or store the record.

Management shall review public records and records retention requirements with each newly hired permanent or temporary DAS employee and with vendors, contractors, and other agents of DAS prior to allowing them to access DAS IT resources.

### **5.5.2 eDiscovery**

Any records created using DAS IT resources may also be subject to eDiscovery. “Discovery” refers to the process of complying with legal obligations to produce relevant documents and information to opposing counsel in the course of civil litigation or to prosecutors or government investigators in criminal or regulatory proceedings. “eDiscovery” refers to the production of files or other data held in an electronic form.<sup>1</sup>

## **6.0 PROCEDURES**

This policy shall be distributed to each newly hired DAS employee during orientation, in conjunction with other applicable policies and procedures, and 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 DAS IT resources.

---

<sup>1</sup> Jamie Popkin, “E-Discovery for IT Professionals: An Exceptional Process that Requires Unique Core Competencies,” Gartner Research Note, 17 February 2011 (Stamford, CT: Gartner, Inc., 2011).

Management shall include this policy when reviewing the DAS Agency-wide Safety/Security Action Plan (ASAP) with employees.

## 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.

It is the responsibility of the user of IT resources to ascertain, understand, and comply with the laws, rules, policies, procedures, standards, and license agreements applicable to their use of those resources.

### 7.1 Consequences of Violation of Policy

Violation of this policy by any user of IT resources may result in loss of access to those resources.

Any DAS employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. In addition, employees may be subject to civil action or criminal prosecution as a result of inappropriate use or misuse of IT resources.

Any contractor, vendor, or other agent of the state performing work for or on behalf of DAS found to have violated this policy may be subject to consequences specified in the contract or other agreement governing their engagement by DAS, up to and including termination of the contract. In addition, contractors may be subject to civil action or criminal prosecution as a result of inappropriate use or misuse of IT resources.

## 8.0 DEFINITIONS

**Availability** - Ensuring timely and reliable access to and use of information.<sup>2</sup>

**Blog** - Web-based content consisting primarily of periodic articles or essays listed with the latest entry and visitor comments at the top. Blog topics can range from personal diaries to political issues, media programs and industry analysis. Blogs are also known as “Weblogs” or “Web logs.”

**Cloud Storage Solutions** - A solution that allows computer data to be stored remotely, providing users the ability to upload and access data over the Internet from a variety of devices (e.g., computer, tablet, smartphone or other networked device).

**Confidentiality** - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.<sup>3</sup>

---

<sup>2</sup> “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>>.

<sup>3</sup> *Ibid.*

**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.

**eDiscovery.** “Discovery” refers to the process of complying with legal obligations to produce relevant documents and information to opposing counsel in the course of civil litigation or to prosecutors or government investigators in criminal or regulatory proceedings. “eDiscovery” refers to the production of files or other data held in an electronic form, such as e-mail.<sup>4</sup>

**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 public servants in the course of conducting state government business in support of agency mission and goals.

**Instant Messaging (IM)** – A software tool that allows real-time electronic messaging or chatting. Instant messaging services use “presence awareness,” indicating whether people on one’s list of contacts are currently online and available to chat.

**Integrity** - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.<sup>5</sup>

**Internet** - A worldwide system of computer networks — a network of networks — in which computer users can get information and access services from other computers. The Internet is generally considered to be public, untrusted and outside the boundary of the state of Ohio enterprise network.

**Malicious Code** - Software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an information system. Some examples include a virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.<sup>6</sup>

**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.

---

<sup>4</sup> Jamie Popkin, “E-Discovery for IT Professionals: An Exceptional Process that Requires Unique Core Competencies,” Gartner Research Note, 17 February 2011 (Stamford, CT: Gartner, Inc., 2011).

<sup>5</sup> “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>>.

<sup>6</sup> *Ibid.*

**OIT** – Office of Information Technology.

**Online Forums** - A web application where people post messages on specific topics. Forums are also known as web forums, message boards, discussion boards and discussion groups.

**Peer-to-Peer (P2P) File Sharing** – Directly sharing content like audio, video, data, software or anything in digital format between any two computers connected to the network without the need for a central server.

**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.

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

**Security Incident** – An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies or procedures, or acceptable use policies.<sup>7</sup>

**Sensitive Data** – Sensitive data is any type of computerized data that presents a high or medium 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 medium 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. 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.

**Social Media** – Refers to websites that facilitate user participation, networking, and collaboration through the submission of user generated content. In general, this includes tools such as: blogs, wikis, microblogging sites, social networking sites, such as Facebook<sup>TM</sup> and LinkedIn<sup>TM</sup>; video sharing sites, and bookmarking sites.

---

<sup>7</sup> “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>>.

**Social Networks** - Web sites promoting a “circle of friends” or “virtual communities” where participants are connected based on various social commonalities such as familial bonds, hobbies or dating interests.

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

**Text Messaging (Texting)** - Text messaging is used for messages that are very brief, containing very few characters. The term is usually applied to messaging that takes place between two or more mobile devices.

**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.

**Wiki** - A Web application that allows one user to add content and any other user to edit the content. The popular software used to implement this type of Web collaboration is known as “Wiki.” A well-known implementation is Wikipedia, an online encyclopedia.

## 9.0 INQUIRIES

Direct inquiries about this policy to:

IT Services  
Office of Information Technology  
Ohio Department of Administrative Services  
30 E. Broad St., 29<sup>th</sup> Floor  
Columbus, Ohio 43215

Telephone: 614 387 1602

For damaged, stolen, lost or potentially compromised IT resources, please immediately contact:

Customer Service Center  
Office of Information Technology  
Ohio Department of Administrative Services

Telephone: 614 644 6860 or 877 644 6860  
E-mail: [csc@ohio.gov](mailto:csc@ohio.gov)  
Website: <https://stateofohio.service-now.com/>

## 10.0 REVISION HISTORY

Date	Description
7/7/2008	New policy to reconcile DAS policy dated 8/21/06 and OIT policy dated 6/29/07
04/23/2012	Revised to reflect changes in technology and policy direction.

05/04/2015	Added requirements for the use of cloud storage solutions and eDiscovery as well as modified the public records and record retention section. Made minor modifications to align terminology with statewide policy.
------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**11.0 ATTACHMENTS**

None.