



## Information Technology Resource Usage

<b>Number:</b> IT-09.07/15	<b>Issuing Division:</b> Office of Information Technology	<b>Effective Date:</b> 20 July 15
<b>Reference/Authority:</b> Ohio Administrative Policy IT-04, "Use of Internet, E-mail and Other IT Resources"	<b>Resource(s):</b>	<b>Supersedes:</b> Comprehensive Information Technology Use

### 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 Agriculture (ODA). 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 ODA workplace and/or for ODA business.

### 2.0 Scope

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

### 3.0 Background

Technology is a critical component of our daily business lives. ODA 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 ODA 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 or IT resource availability can have a significant impact on the ability of this agency to fulfill its mission. The requirements outlined in this policy will help users understand agency 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.

This policy, "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 Definitions

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. The assurance that information is disclosed only to those systems or persons who are intended to receive the information. Areas in which confidentiality may be important include nonpublic customer information, patient records, information about a pending criminal case, or infrastructure specifications. Information systems that must ensure confidentiality will likely deploy techniques such as passwords, and could include encryption.

DAS. Department of Administrative Services.

DAS-OIT. Department of Administrative Service – Office of Information Technology.

Information Technology 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.

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. Collective term for program code or data that is intentionally included in or inserted into an information system for unauthorized purposes without the knowledge of the user. Examples include viruses, logic bombs, Trojan horses and worms.

Management. Management refers to supervisory staff responsible for the completion of activities to fulfill ODA 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.

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

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

ODA-OIT. Department of Agriculture - Office of Information Technology.

ODA-owned. Purchased with ODA funds or otherwise acquired by ODA; property of ODA.

ODA-provided or ODA-supplied. Made available to users by ODA.

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. A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Examples of security incidents are as follows<sup>1</sup>:

- Denial of Service. (e.g., A user sends specially crafted packets to a Web server, causing it to crash.)
- Malicious Code. (e.g., A user introduces a “worm,” a self-replicating program that usually performs malicious actions, to use open file shares to quickly infect several hundred workstations.)
- Unauthorized Access. (e.g., A perpetrator obtains unauthorized administrator-level access to a system and the sensitive data it contains.)
- Inappropriate Usage. (e.g., A user provides illegal copies of software to others through peer-to-peer file sharing services.)

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.

---

<sup>1</sup> Grance, Tim, Kelly Masone, and Karen Scarfone. Computer Security Incident Handling Guide, Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology. March 2008. <<http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf>>.

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™ and LinkedIn™; video sharing sites, and bookmarking sites.

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.

## **5.0 Policy**

The following policy statements outline 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 ODA 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 ODA IT resources belong to ODA, except for those items whose ownership is protected by law, contract, license agreement, copyright, or other agreement. All data stored or transmitted on a ODA IT resource may be subject to review, investigation and public disclosure.

When using ODA 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.

ODA reserves the right to monitor, access, and disclose all information generated and actions performed using ODA 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, ODA IT resources are on loan to ODA employees, contractors, temporary personnel, and other agents of the state so that essential job functions may be performed. Upon separation from ODA employment or contract termination, all ODA 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 or is believed to be stolen or lost, it shall immediately be reported to the Division Chief, to management and to the ODA-OIT Help Desk. (Please find the ODA-OIT Help Desk contact information in Section 8.0 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.

All ODA-owned laptops, desktops, tablet computers, or other electronic devices that authenticate to the ODA Network, must be connected to the network at least once every calendar month in order to receive operating system patches and security updates. Inventory owners of shared devices, to which this requirement applies, are responsible for connecting all shared computers and laptops contained on their inventory in the same timeframe.

### **5.1.3 Personal Use of IT Resources**

ODA 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 ODA business. Management may further restrict personal use of IT resources where appropriate.

An incidental amount of non-work related data may be stored on the local drive of the assigned desktop/laptop computer. If this provision is exercised by the individual employee, it is done at the employees own risk.

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

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

Users of ODA IT resources, to include agency provided wireless access (Agriculture Guest), shall comply with all applicable policies, procedures, and standards related to the security and usage 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.

Sensitive data may not be removed from state premises without the Division Chief and management's authorization. Refer to section 5.2.2 of this policy for requirements regarding the transport of sensitive data.

Computing devices that do not have adequate security controls in place will not be placed on or authenticated to the network. Adequate security controls would include such items as an anti-virus application with current definitions and a supported Operating System.

Except for devices that are inherently mobile, such as laptops, smart phones 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 ODA-OIT Help Desk.

Disposal of IT resources shall be coordinated by ODA-OIT 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 ODA 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:

Violation of Law. Violating or supporting and encouraging the violation of local, state, or federal law.

Inappropriate Usage. Excessive use or abuse of the internet and other computing resources of the agency and of the state.

Illegal Copying. Downloading, duplicating, disseminating, printing or otherwise using copyrighted materials, such as software, texts, music and graphics, in violation of copyright laws.

Operating a Business. Operating a business, directly or indirectly.

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.

Accessing Sexually Explicit Material. Downloading, displaying, transmitting, duplicating, storing or printing sexually explicit material.

Harassment. Downloading, displaying, transmitting, duplicating, storing or printing material that is offensive, obscene, threatening or harassing.

Gambling or Wagering. Organizing, wagering on, participating in or observing any type of gambling event or activity.

Auctions. Participation in any form of an on-line auction (e.g., eBay).

Games. Downloading, accessing, or playing games (i.e., solitaire, FreeCell, hearts), whether on the local hard drive or internet based.

Streaming. Downloading or accessing non-work related media file (i.e., music, movies, radio stations, videos) on state equipment.

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).

Security Controls. Removing, tampering with or circumventing security controls.

Engaging in Unauthorized IT Related Activities. Engaging in IT related activities that are unauthorized and/or outside of one's Position Description and job duties (e.g., denial of service attacks, attempts to intercept/collect data, introduction of malicious code, network monitoring/scanning).

Misrepresentation. Concealing or misrepresenting one's name or affiliation to mask unauthorized, illegal, fraudulent, irresponsible or offensive behavior in electronic communications.

Sensitive Data and/or Personally Identifiable Information. Accessing or Disseminating sensitive data or personally identifiable information without authorization.

Passwords. Disclosing user account passwords to parties external to ODA, or to ODA co-workers and/or supervisors. Setting or manipulating a password to impede access to any state computer, program, file or electronic communication without proper authorization.

Malicious Code. Distributing malicious code or circumventing malicious code security.

Peer-to-Peer File Sharing. The personal use of peer-to-peer file sharing from non-state computer systems.

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. This prohibition does not apply to work related correspondence transmitted by an authorized user of the ODA Mass Emailer System.

System Damage and Degradation. Deliberately attempting to or intentionally damaging or degrading computer and computer system performance or capability.

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

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

Solicitation. Except for agency approved efforts, soliciting for money or support, for example on behalf of charities, religious entities or political causes.

Unauthorized Installation or Use of Software. Installing or using software without proper agency approval. ODA-OIT provides each end-user with pre-approved software on state-approved IT resources. The installation and use of any additional software requires authorization from the Chief Information Officer or his/her designee. Personally owned software and/or unlicensed software will not be authorized.

Unauthorized Installation or Use of Hardware. Installing, attaching, or connecting network devices to ODA systems or networks without proper authorization. ODA-OIT provides each end-user with pre-approved hardware and state-approved IT resources. The installation and use of any additional network hardware requires authorization from the Chief Information Officer or his/her designee.

Data Transport. Transporting sensitive data (refer to Section 4.0 for definition) from one location to another without management approval and not using a secured, encrypted method provided and approved by ODA-OIT. A request to transport sensitive data should be made using the ODA-OIT Help Desk Ticketing System.

Connections. Bridging connections, Internet connection sharing, and from allowing remote control connections (e.g., Remote Desktop, TeamViewer, UltraVNC) to ODA IT resources. ODA-OIT may establish remote control sessions for troubleshooting and help desk ticket resolution. Exceptions may also be approved for Industrial Control Systems and related functions necessary for the HVAC and security needs of the campus. Users may share their desktop during presentations employing Skype for Business™ and other approved presentation applications if remote control is not passed to another party.

Accessing Systems without Authorization. Accessing networks, files or systems or an account of another person without proper authorization.

Privately-owned E-mail Accounts. Use of privately-owned e-mail accounts, including private web-based e-mail accounts, to conduct ODA or state business unless specifically authorized, in writing, by the Division Chief and by management. The Chief Legal Counsel is to be notified of any such approvals. ODA is under no obligation to provide support for privately-owned e-mail accounts.

Online Community. Use of state-provided IT resources to operate, participate in, or contribute to an online community including, but not limited to, online forums, chat rooms, blogs, wikis, peer-to-peer file-sharing, externally-provided listservs, and social networks, unless organized or approved by the ODA Director or Chief Information Officer.

### **5.3 Personnel with Computer System Administrative Rights**

Employees or contractors designated with administrative access rights shall not abuse administrative rights or privileges associated with computer systems. Abuse of administrative rights or privileges includes, but is not limited to, the following activity:

- Using system administrative rights to access or read e-mail associated with any user's e-mail account other than his or her own, without that user's permission or the prior written consent from the Chief Information Officer and the Office of Human Resources;
- Copying or transferring databases and files, including e-mail databases, e-mail accounts, or e-mail files, in preparation for unauthorized access to data and communications by anyone;
- Providing administrative rights or privileges to another person for the purpose of obtaining unauthorized access to data files and communications;
- Using administrative rights or privileges to change or disable any security, access control list, active directory, logging, or tracking function within the computer system in order to hide unauthorized access to files and communications.

### **5.4 Electronic Communications**

#### **5.4.1 Professionalism**

ODA 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.

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

The State of Ohio e-mail system is Office365 and primarily uses Microsoft Outlook client software and/or Outlook Web Access. 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.

ODA 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.

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

Incidental 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.

For more information regarding text messaging please refer to the Public Records Policy and to the Social Media Policy.

### **5.4.4 Social Media**

Social media platforms (e.g., Facebook™, Twitter™, YouTube™, Pinterest™) may be authorized and approved for designated ODA Divisions/Sections/Offices and specific employees. Each designated organizational unit will be responsible for account set up, maintenance, evaluation and site content. ODA employees will use approved social media platforms as an Internet-based social networking forum for education, marketing, and promotion of Ohio agribusiness and for fulfilling the agency mission.

Employees, contractors, temporary personnel, and other agents of the state shall not include references or pointers to their personal social media accounts in official ODA or State of Ohio communications without express authorization from the Division Chief and management. (e.g., providing personal social media account pointers within 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 ODA or the State of Ohio without authorization from the ODA Division Assistant/Deputy Director and the ODA Office of Communications.

While engaged in personal or official state use, do not discuss information related to ODA or Ohio that is not already considered public information under state and federal

laws. 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 ODA 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.

## **5.5 Cloud Storage Solutions**

### **5.5.1 Restrictions on Use of Cloud Storage Solutions**

Only state approved cloud storage solutions, Microsoft OneDrive for Business and SharePoint Online, shall be used to store, share and manage information. When using state cloud storage solutions, the following restrictions apply:

**Data Storage:** Only data related to state business shall be stored in state cloud storage solutions. Personal data shall not be stored in state cloud storage solutions.

**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 Administrative Policy IT-14, "Data Encryption and Securing Sensitive Data".

Electronic information required for the conduct of business may be retrieved from non-state approved solutions as agency personnel interact with constituents, vendors, and other known parties.

## **6.0 Procedures**

This policy shall be distributed to each newly hired ODA employee, who will have access to IT resources, during employee orientation, in conjunction with the distribution of other applicable policies and procedures for the particular Division or Office of employment.

Vendors, contractors and temporary employees, who will have access to IT resources, shall receive a copy of this policy and any associated policies of note.

Current and new ODA employees will acknowledge receipt and review of this particular policy through the Electronic Learning Management (ELM) system.

## **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 ODA 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 ODA found to have violated this policy may be subject to consequences specified in the contract or other agreement governing their engagement by ODA, 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.

The Ohio Revised Code (ORC) makes certain misuses of IT resources criminal offenses:

- ORC Section 2909.04 – knowingly using a computer system, network or the Internet to disrupt or impair a government operation.
- ORC Section 2909.05 – causing serious physical harm to property that is owned, leased, or controlled by a government entity.
- ORC Section 2913.04 – accessing without authorization any computer, computer system, or computer network without consent of the owner.
- ORC Section 2921.41 – using a public office to commit theft which includes fraud and unauthorized use of government computer systems.

## **8.0 Inquiries**

Direct inquiries about this policy to:

Ohio Department of Agriculture  
Office of Information Technology  
8995 East Main Street  
Reynoldsburg, Ohio 43068

Telephone: 614.728.6227  
Facsimile: 614.728.6434  
E-mail: IT@agri.ohio.gov

IT Helpdesk Request Form: <http://intranet/ithelp/ITHelp.aspx>

## **9.0 Revision History**

---

<b><i>Date</i></b>	<b><i>Description of Change</i></b>
20 July 15	Version 1.0 – Original Policy
20 July 16	Scheduled Policy Review

---

## **10.0 Attachments**

None.