

<p style="text-align: center;">STATE OF OHIO</p>  <p style="text-align: center;">DEPARTMENT OF NATURAL RESOURCES</p>	<p>SUBJECT: Appropriate Use of Publicly Owned Information Technology (IT) Systems and Services</p>	<p>PAGE <u>1</u> of <u>8</u> PAGES</p>
	<p>RULE/CODE REFERENCE: ORC §2909.04; ORC §2909.05; ORC §2913.04; ORC §149.43 et seq.; ORC §1347.15, DAS ITP-E.8</p>	<p>POLICY #DNR-OIT-0001</p>
	<p>PURPOSE: To set forth the policy for the appropriate use of Department owned IT systems and services.</p>	<p>SUPERSEDES: Use of Publicly Owned IT Resources Policy 7/17/2006; Internet/Intranet Security Use and Policy 7/17/2006; Appropriate Use Policy; Sensitive Information Policy 9/1/2008</p>
	<p>APPOINTING AUTHORITY: ORC §1501.01 ODNR Director</p>	<p>EFFECTIVE DATE: 10/13/2014</p> <p>REVISION DATE: 10/13/2014</p> <p>APPROVER AND DATE: <i>[Signature]</i> 10.9.14</p>

This policy applies to all Ohio Department of Natural Resources (“ODNR”) employees, and in no way supersedes the negotiated language in the applicable collective bargaining agreements.

I. DEFINITIONS:

TERM	DEFINITION
Client Account	An account issued by OIT with a user name (user-id) and password to access (or authenticate) to the ODNR network.
E-mail Account	An account issued by OIT or the state of Ohio with a user name and password to access an Exchange mailbox.
Law Enforcement Sensitive (LES) Information	Any "confidential" information that may be excepted from release as a public record on the basis that it is a "Confidential Law Enforcement Investigative Record pursuant to application of ORC §149.43(A)(1)(h), (A)(2).
Local User Account	An account that exists on a single PC rather than on the domain (network wide).
IT Resources	IT resources include computer equipment, software, systems, services and the information collected and stored by the Department.
Internet	A worldwide system of computer networks; a network of networks in which users at a computer can get information from another computer. The Internet is generally considered to be public, untrusted, and outside the boundary of the state of Ohio enterprise network.
Intranet	An Intranet is a private network that is contained within an enterprise. In general, an Intranet looks like a private version of the Internet. The main purpose of an Intranet is to share enterprise information and computing resources among employees.
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.

Mobile Device	A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers.
Owner	The individual or organization that has legal right of possession or access to a specific computer equipment, software product and/or service. In the case of ODNR, the owner may be the Department, a Division/Office, or an employee, depending on who procured the product or service.
Portable Storage Device	An information system component that can be inserted into and removed from an information system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain non-volatile memory).
Sensitive / Confidential Personal Information	Sensitive/Confidential personal information means personal information that is not a public record for purposes of section 149.43 of the Ohio Revised Code or "personal information" that consists of any individual's name, including the last name along with the individual's first name or first initial, in combination with and linked to any one or more of the following data elements: Social Security number, driver's license number, state identification card, Financial account numbers, health information, or certain information pertaining to minors. The use of the word "person" in the definition could suggest the inclusion of "legal persons" such as a corporation; however, when examined in the context of Ohio Revised Code section 1347.12, and usual practice, the definition would in fact be limited to "natural persons". An individual's federal tax identification number could also be treated as personal information (ORC 149.45), as it may be their Social Security number.
Unauthorized Access	A person using another's network account for any purpose. This does not include OIT technicians performing maintenance on a user's PC or network account.

II. **POLICY:**

ODNR information technology (IT) resources are publicly owned and intended to be utilized in performing job duties. These resources play an essential role in providing quality service to our internal customers and the citizens of Ohio. This policy will direct users of ODNR IT resources in their appropriate use.

1. **Information Security**

Every employee must take an active role in keeping our information secure and protecting ODNR equipment, services and sensitive information in their possession from loss, theft, damage and unauthorized use. Employees shall not:

1.1 Partake in or permit any unauthorized use of electronic information maintained by the

ODNR;

- 1.2 Seek to benefit personally or permit others to benefit personally by any information which has come to the employee by virtue of a work assignment or work environment;
- 1.3 Knowingly include or cause to be included in any record or report a false, inaccurate or misleading entry;
- 1.4 Remove or cause to be removed copies of any official record or report from any file from the office where it is kept except in the performance of an employee's duties;
- 1.5 Access or disseminate confidential personal information without authorization (see also the ODNR Sensitive Information Policy);
- 1.6 Access networks, files or systems or an account of another person without proper authorization.

2. Sensitive Information

The ODNR has a duty to protect sensitive information (ORC 1347). The proper storage, use and security of sensitive information is important to foster public confidence in the agency as well as protect ODNR employees and our customers. This is true regardless of the format or media on which the information is contained (e.g. paper, electronic, etc.). Therefore, ODNR employees shall comply with the following provisions:

- 2.1 Use of Sensitive/Confidential Personal Information or Law Enforcement Sensitive (LES) Information for other than approved official state business is prohibited. The determination whether certain information is LES is frequently fact-specific, therefore consultation with Department Legal Counsel in making such determinations is advised.
- 2.2 All Sensitive/Confidential Personal Information and the systems, media, devices and electronic transmissions containing that information must be classified, labeled and secured.
- 2.3 Law Enforcement Sensitive (LES) information shall not be transmitted to any non-governmental email account or posted on a non-governmental File Transfer Protocol (FTP) site.
- 2.4 Access to Sensitive/Confidential Personal Information without prior authorization from the Division/Office Information Owner is prohibited.
- 2.5 Electronic Personal Information Systems containing Sensitive/Confidential Personal Information must use a password or other authentication measure to restrict access to electronic Sensitive/Confidential Personal Information.
- 2.6 Allowing unauthorized personnel access to Sensitive/Confidential Personal Information or Law Enforcement Sensitive (LES) Information is prohibited.
- 2.7 Sensitive/Confidential Personal Information shall not be stored on portable storage devices without written approval from the director or his designee. OIT shall consult with Divisions/Offices on security techniques and practices. If the Division/Office receives an approval, the Sensitive/Confidential Personal Information must be stored on an OIT approved encrypted device. The encryption shall be in conformance with Ohio State IT Standard ITS-SEC-01, "Data Encryption and Cryptography." This data should only be stored when it is business critical and removed as soon as possible after the information is no longer required for business purposes.

- 2.8 Sensitive/Confidential Personal Information or Law Enforcement Sensitive (LES) Information shall not be stored on non-ODNR owned personal computers. The Office of Information Technology may outsource the collection, storage or analysis of Sensitive/Confidential Personal Information when the appropriate administrative, technical and physical safeguards are assured.
- 2.9 Law Enforcement Sensitive (LES) Information does not require a Director's signature to be copied to a mobile storage device. However, Law Enforcement Sensitive (LES) Information must be removed/deleted from the device as soon as possible after the information is no longer required for Law Enforcement purposes.
- 2.10 Any lost or stolen departmental mobile storage device must be reported to the Office of Information Technology immediately upon discovery. The PC Liaison of the division or office that owns the missing device must investigate to determine whether Sensitive/Confidential Personal Information was stored on it and, if necessary, follow established procedure to ensure notification to the affected individual(s) of the possible information release within 48 hours of the discovery.
- 2.11 Any records made available to the public under Ohio Revised Code §149.43 or ORC §149.45 must have Sensitive/Confidential Personal Information redacted or truncated as described in the ODNR Redaction Procedure.

3. Public Records

The ODNR has a duty to preserve public records according to the retention schedule and make them available for inspection (ORC §149.43). Electronic public records shall be stored on OIT file and database servers.

4. Privacy

- 4.1 The ODNR respects the privacy of its employees; however, the equipment and services are provided solely to facilitate ODNR business. Users shall have no reasonable expectation of privacy in their use of ODNR resources. Users should be aware that any files or communications made by or passing through state equipment is subject to review by the ODNR. The ODNR may examine, monitor, search or disclose the contents of the files, including but not limited to e-mails, log files, data files, websites or calendars, at its discretion at any time.
- 4.2 Do use proper decorum when communicating. The contents of files, messages and logs may be public records under ORC §149.43 and subject to disclosure to the media or public upon request.
- 4.3 Employees shall not encrypt or conceal the contents of any file or electronic communications nor set or manipulate a password on any state computer, program, file or electronic communication without proper authorization from OIT.

5. Prohibited Uses of IT Resources

- 5.1 Internet use for any purpose other than official State of Ohio business purposes is prohibited;
- 5.2 Violating or encouraging the violation of local, state or federal law or ODNR policy;
- 5.3 Disseminating, accessing or attempting to access confidential information without authorization;
- 5.4 Disseminating statements that disparage others based on their race, national origin, sex, sexual orientation, age, disability, religious, or political beliefs;

- 5.5 Downloading, duplicating, disseminating or printing of copyrighted materials such as texts, software, music and graphics in violation of copyright laws;
- 5.6 Operating a business, directly or indirectly, for personal gain;
- 5.7 Soliciting, downloading, displaying, transmitting, duplicating, storing, or printing material that is offensive, obscene, sexually explicit, threatening, harassing or incendiary;
- 5.8 Soliciting, transmitting, viewing or downloading messages or images that promote violence or are associated with terrorist activities;
- 5.9 Organizing, wagering on, participating in or observing any type of gambling event or activity, including the state of Ohio lottery;
- 5.10 Sending unsolicited e-mails or facsimiles in bulk or forwarding electronic chain letters individually or in bulk;
- 5.11 Soliciting money or support on behalf of charities, religious entities or political causes, except for agency approved charitable efforts;
- 5.12 Impeding the state's ability to access, inspect or monitor IT resources;
- 5.13 Accessing or participating in any type of personal ads or services such as dating, matchmaking, companion finding, pen pal or escort services;
- 5.14 Accessing Internet Service Providers for any purposes using the ODNR's network Internet connection, including personal e-mail accounts, e.g. Hotmail, Gmail, Yahoo Mail, etc.;
- 5.15 Using another person's account or signature line. This includes all activities on the Internet (e.g., electronic mail, bulletin board system or social media sites);
- 5.16 Concealing or misrepresenting one's name or affiliation to mask unauthorized, fraudulent, irresponsible or offensive behavior in electronic communications;
- 5.17 Unauthorized operation of, participation in, or contribution to an online community including, but not limited to, forums, chat rooms, blogs, wikis, peer-to-peer file sharing, social networks and non-work related mailing lists. Users can request approval to participate in these forms of communication if required for official ODNR business by contacting OIT. (See the ODNR Social Media Policy.);
- 5.18 Banking, shopping, web email (State of Ohio web email is permitted), job hunting (other than official State of Ohio agency job web site), and games.
- 5.19 Using an ODNR e-mail address on personal communications in online communities.

6. User Accounts, Passwords and Workstation Security

- 6.1 All persons working on the ODNR network shall have a client account with an individual user name (user-id) and password or other authentication mechanism that is not shared or posted in any manner. All client accounts on the network must be individually owned and accessed to ensure security and accountability. An e-mail account shall be owned by an individual; no sharing of e-mail accounts is permitted. Users are prohibited from creating local user accounts on their PC. All user accounts, when required, will be created and maintained by OIT.
- 6.2 Users are responsible for all activities that take place with their user ID. Users must choose passwords that are difficult to guess and satisfy the ODNR Password Standard

requirements. Users must immediately change their password if they suspect it is known by someone else.

- 6.3 Every network user is responsible for ensuring their networked computer is secured from unauthorized access when they leave their workstation. When users leave their workstations unattended password protected screensavers (or other locking programs) shall be used to prevent unauthorized access. Alternatively, users may physically secure the device (e.g., lock their office door).

7. Physical Security

Employees are held accountable for all equipment assigned to them, and must safeguard offsite ODNR equipment and data at all times. Devices shall not be left unattended without employing adequate safeguards such as cable locks, restricted access environments or lockable cabinets. State owned mobile devices and other forms of computer hardware shall not be left in plain sight and unattended within personal or state owned vehicles.

8. Network Equipment, Software and Operating Systems

- 8.1 Installing, attaching or physically or wirelessly connecting any kind of hardware device to the ODNR internal network, including computers or network services, without prior written authorization from OIT is strictly prohibited.
- 8.2 Access to the ODNR network using employee owned equipment is prohibited unless authorized by the Office of Information Technology.
- 8.3 Users may connect to their state provided e-mail through "Outlook Web Access" from their personal PC or Mobile Device and not be in violation of this policy.
- 8.4 All owners of state provided laptops, desktops, tablet computers, or other electronic devices that authenticate to the ODNR Network, must connect these units to the network at least once every two weeks to receive operating system patches and security updates. Inventory owners of shared devices are responsible for connecting all shared computers and laptops on their inventory in the same timeframe.
- 8.5 ODNR employees and Divisions/Offices shall not install unapproved operating systems or software, including print drivers, on Department systems. Installing or using software including, but not limited to, instant messaging clients, video games (both stand alone and on-line), media including music and video files, peer-to-peer file sharing software, or personally owned software on ODNR-owned IT resources is prohibited unless approved in writing by OIT.
- 8.6 Users are prohibited from bridging connections, Internet connection sharing, and from allowing remote connections (e.g. Remote Desktop) to their PC. Remote connections may be allowed for OIT troubleshooting and with written approval from OIT. Users are prohibited from disabling firewall software or modifying firewall rules to disable firewall functionality.
- 8.7 OIT may modify or suspend system access without warning should such access be deemed to pose a security or operational risk to ODNR resources.

9. Internet/Intranet Server Use

- 9.1 All materials and applications to be posted to the ODNR Internet or Intranet servers will be tested on the web development server before deployment. Web materials and applications must not compromise the performance, integrity and security of the ODNR Internet and Intranet servers. All materials and applications posted to the ODNR Internet or Intranet servers must also reside on the development server.

- 9.2 Only authorized DNR staff may post materials and applications to the ODNR Internet or Intranet servers. Each Division and Office shall authorize specific staff members to post materials and applications to the ODNR Internet or Intranet servers. These people will be responsible and accountable for the content of their Division's web pages and the pages' impact on the ODNR's web site.

10. Software Use and Duplication

- 10.1 All software must be used in accordance with its license agreement.
- 10.2 Shareware products, evaluation and Beta test copies of software must also be handled in accordance with its license agreement, including observing any time period specified.
- 10.3 Users shall not make any unauthorized copies of any software. The responsibility to adhere to federal copyright laws and proper licensing and distribution of the software and/or software services belongs to the "owner" of a specific software product and/or service.
- 10.4 The "owner" shall follow the "one software package/one IT resource" rule when purchasing software. An equivalent number of software packages shall be purchased for every resource upon which it is run.
- 10.5 Responsibility is assigned as follows:
- 10.5.1 OIT is responsible for all ODNR enterprise IT products and services that have been procured by the Office for agency employees to perform their job duties.
- 10.5.2 OIT will install approved non-enterprise software for the Divisions, but the Divisions are responsible for supporting such software.

11. Malicious Code

Users are required to utilize approved, up-to-date anti-virus software to check all files for code that could harm ODNR equipment or systems. Users are prohibited from disabling anti-virus software or disseminating malicious code. Users shall report any incidents of detected or suspected malicious code to the OIT Support Desk immediately at (614) 265-7082.

12. RESPONSIBILITIES:

POSITION OR OFFICE	RESPONSIBILITIES
Office of Human Resources	A. To process violations of the policy according to the disciplinary process and grid.
ODNR Office of Information Technology	A. To annually review department policies for applicability and updates. B. Monitor workforce, ensure compliance, and report violations to Human Resources. C. Proactively communicate questions, concerns and issues to the appropriate contact listed below.
Employee	A. Read and comply with policy. B. Proactively communicate questions, concerns and issues to the appropriate contact listed below. C. Complete all associated policy training in a timely fashion.

13. RESOURCES:

Office of Information Technology

14. CONTACTS:

SUBJECT	OFFICE	TELEPHONE	EMAIL/URL
Policy Violations	Office of Human Resources/Labor Relations	(614) 265-6981	Policy.Coordinator@dnr.state.oh.us
Policy Issues	Office of Information Technology Security	(614) 265-6854	Office of IT Security