

## USE OF PUBLICLY OWNED IT RESOURCES POLICY

<b>Effective</b>	July 17, 2006
<b>Purpose</b>	To set forth departmental policy to ensure uniformity and consistency in the use and security of ODNR Information Technology Resources
<b>Authority</b>	Statewide Information Technology Policy DAS ITP-B.1, 2, 4, 5, 6 DAS ITP-D.4 DAS ITP-E.8 ORC 2909.04-5, 2913.04, 2921.41
<b>Resource</b>	Office of Information Technology

Computer hardware, software, and software services are publicly owned assets and are intended to be resources utilized by an employee in performing their job duties. Information contained on them is subject to review by department managers. As the user of IT resources, the employee will be held accountable for any misuse of the product.

### Prohibited Uses of IT Resources

Any use of IT resources that is unlawful, could potentially embarrass or harm the state, or has the appearance of impropriety is strictly prohibited and includes, but is not limited to, the following:

1. violating or encouraging the violation of local, state or federal law
2. downloading, duplicating, disseminating or printing of copyrighted materials such as texts, music and graphics
3. operating a business, directly or indirectly, for personal gain
4. accessing or participating in any type of personal ads or services such as dating, matchmaking, companion finding, pen pal or escort services
5. downloading, displaying, transmitting, duplicating, storing, or printing sexually explicit materials
6. downloading, displaying, transmitting, duplicating, storing, or printing material that is offensive, obscene, threatening or harassing
7. organizing, wagering on, participating in or observing any type of gambling event or activity
8. sending unsolicited e-mails or facsimiles in bulk or forwarding electronic chain letters in bulk
9. except for agency approved efforts, soliciting money or support of behalf of charities, religious entities or political causes
10. impeding the state's ability to access, inspect and monitor IT resources. No employee or approved contractor shall encrypt or conceal the contents of any file or electronic communications or set or manipulate a password on any state computer, program, file or electronic communication without proper authorization from the Office of Information Technology
11. personal use of IT resources that disrupts or interferes with state business or incurs an

undue cost to the state

## **Hardware**

Installing, attaching, or physically or wirelessly connecting any kind of hardware device to any state-provided IT resource, including computers or network services, without prior authorization from the Office of Information Technology is strictly prohibited

## **Owner Responsibilities**

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. Responsibility is assigned as follows:

1. The Office of Information Technology is responsible for all IT products and services that have been procured by the Office for agency employees to perform their job duties.
2. The division/office is responsible for all products and services that have been procured by a division/office for employees to perform their job duties.
3. The employee is responsible for all products and services that have been procured by the employee to perform their job duties. In this particular case, the employee shall secure a waiver authorizing the use of the product and/or service signed by the division/office or Department representative and kept in the employee's personnel file. The waiver is intended to protect the employee as well as the division/office or Department.

## **Security and Confidentiality of Data Files and Safeguarding State Assets**

All of the following activities are strictly prohibited:

1. Make or permit unauthorized use of any information in files maintained by the Department/Division/Office.
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.
3. Knowingly include or cause to be included in any record or report a false, inaccurate or misleading entry.
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.
5. Use IT resources to violate or attempt to circumvent confidentiality procedures.
6. Accessing or disseminating confidential information about another person without authorization.
7. Accessing networks, files or systems or an account of another person without proper authorization.
8. Assist another to violate any part of this Code.
- 9.

## Software Use and Duplication

The following points are to be followed to comply with software license agreements:

1. All software will be used in accordance with its license agreement.
2. No user will make any unauthorized copies of any software. Anyone found copying software other than for backup purposes may be subject to disciplinary action.
3. Acquisition and registration of shareware products will be handled in accordance with its license agreement. Shareware software is copyrighted software that is distributed freely through bulletin boards, web pages and online services.
4. Evaluation and Beta test copies of software will be used only for the time period agreed to in accordance with its license agreement.
5. Installing or using software including, but not limited to, instant messaging clients, video games (both stand alone and on-line), peer-to-peer file sharing software, or personally owned software on department-owned IT resources is prohibited unless approved in writing by the Office of Information Technology.
6. 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. With regard to use on wide or local area networks, or on multiple machines, owners shall acquire and use the software in accordance with the license agreement.

## Privacy

Department IT resources belong to the State. Users should be aware that any files or communications made by or through State equipment may be subject to review by the department. The department 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.

## Penalties

Violation this policy may result in disciplinary action or contractual penalties, and may be cause for termination. Additionally, the Ohio Revised Code (ORC) makes certain misuses of IT resources criminal offenses:

- 2909.04 using IT resources to disrupt or impair a government entity
- 2909.05 using IT resources to cause serious physical harm to government property
- 2913.04 accessing IT resources without consent of the owner
- 2921.41 using a public office to commit theft which includes fraud and unauthorized use of government IT resources

Anyone who becomes aware of a violation of these Codes shall report it to his/her supervisor or the violator's supervisor immediately. The Supervisor is responsible for notifying the Office of

Information Technology chief or assistant chief.

## **Glossary**

1. **IT resources:** includes computers, servers, personal digital assistants, printers, copiers, fax machines, plotters, hubs, switches, routers, bridges, wireless access points, network interface cards or firewalls
2. **Owner:** the individual or organization that has legal right of possession or access to a specific 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