

INTERNET/INTRANET SECURITY AND USE POLICY

Effective	July 17, 2006
Purpose	To set forth departmental policy to ensure the integrity and security of the Department's Internet/Intranet System, and the uniformity and consistency of Internet use on ODNR's IT resources
Authority	Statewide Information Technology Policy DAS ITP-B.6 DAS ITP-E.8
Reference	Use of Publicly Owned Computer Hardware, Software and Software Services Policy
Resource	Office of Information Technology

ODNR employees shall not use the Department's Internet and Intranet servers in such a way as to impair the integrity and security of the systems. Nor shall employees use departmental computer hardware to access the Internet in a manner that interferes with business activities or is in violation of responsibilities outlined below. As the user of department's Internet/Intranet services, the employee will be held accountable for any misuse of these services.

Internet/Intranet Server Use

1. **All materials and applications to be posted to the Department 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 Department Internet and Intranet servers. All materials and applications posted to the Department Internet or Intranet servers must also reside on the development server.
2. **Only authorized DNR staff may post materials and applications to the Department Internet or Intranet servers.** Each division and office shall authorize specific staff members to post materials and applications to the Department 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 Department's web site.

User Responsibilities

1. **Non-business uses of the Internet that interfere with business activities are not permitted.** Internet access is intended for official DNR business purposes. Personal use of the Internet that disrupts or interferes with state business, incurs an undue cost to the state, could potentially embarrass the state or has the appearance of impropriety is strictly prohibited.
2. **Using state IT resources for private business activities, sending chain letters, or soliciting money or support on behalf of charities, religious entities or political**

- causes is prohibited.** IT resources may be used to support department sponsored charitable events. Non-state employees may use state owned PC's that are designated for public use to access ODNR information that benefits a private business.
3. **Internet communications shall not contain offensive, obscene, threatening, harassing or incendiary statements.** Statements that disparage others based on their race, national origin, sex, sexual orientation, age, disability, religious, or political beliefs as well as statements that promote violence or the use of weapons or devices associated with terrorist activities are strictly forbidden.
 4. **Sending, soliciting, viewing or downloading sexually oriented messages or images is strictly forbidden.**
 5. **Sending, soliciting, viewing or downloading messages or images that promote violence or are associated with terrorist activities is strictly forbidden.**
 6. **Disseminating or printing of copyrighted materials (including articles and software) in violation of copyright laws is prohibited.**
 7. **Users shall not provide unauthorized access to confidential information via the Internet.** All use of the Internet must be done in compliance with the rules and regulations that apply to such information. All reasonable means shall be employed to prevent the inadvertent dissemination of another person's private and/or confidential information via the Internet.
 8. **Use of another's account or signature line by a user is prohibited.** This includes all activities on the Internet (e.g., electronic mail or bulletin board system).
 9. **Concealing or misrepresenting one's name or affiliation to mask unauthorized, fraudulent, irresponsible or offensive behavior in electronic communications is prohibited.**
 10. **Users are prohibited from disabling anti-virus software or disseminating malicious code and are required to check all files downloaded from the Internet for malicious code (e.g., a virus), and shall report any incidents to the Office of Information Technology.** Users are required to utilize anti-virus software to check all files for code that could harm department equipment or systems by downloading them to disk. Users must report any malicious code detected to the OIT Support Desk (265-7082).
 11. **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 , listservs is prohibited. Using an ODNR e-mail address on personal communications in online communities is prohibited.** Users can request approval to participate in these forms of communication if required for official business by contacting the Office of Information Technology.
 12. **Accessing or participating in any type of personal ads or services such as dating, matchmaking, companion finding, pen pal or escort services is prohibited.**
 13. **Organizing, wagering on, participating in or observing any type of gambling event or activity is prohibited.**
 14. **Sending unsolicited e-mails or facsimiles in bulk or forwarding electronic chain letters in bulk is prohibited.**
 15. **Accessing Internet Service Providers for any purposes using the Department's network Internet connection is prohibited.** Users are not permitted to access personal e-mail accounts e.g., Hotmail.com, using a networked PC.

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. **Internet:** A worldwide system of computer networks; a network of networks in which users at a computer can get information form another computer. The Internet is generally considered to be public, untrusted, and outside the boundary of the state of Ohio enterprise network.
2. **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.
3. **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
4. **Malicious Code:** Collective term for program code or data that is intentionally included in or inserted into an information system for unauthorized purposed, without the knowledge of the user. Examples include viruses, logic bombs, Trojan horses and worms.