Ohio | Industrial Commission

COMPUTER USE

APPOINTING AUTHORITY APPROVAL: Jodie M. Taylor	POLICY NUMBER: HR062
	EFFECTIVE DATE: 11/01/07 AMEDNED: 06/14/11 REVIEWED: 04/03/13
AUTHORITY: ADMINISTRATION	APPROVAL DATE: 11/01/07 AMENDED: 06/14/11 REVIEWED: 04/03/13

I. Purpose:

The purpose of this policy is to create a standard within the Industrial Commission to maintain system security, data integrity, and privacy by preventing unauthorized access to data, and misuse of, damage to, or loss of data.

II. Policy:

The use of personal computers, the Internet, email, and online services has the potential to enhance the productivity of IC employees. At the same time, the potential for abuse may exist. This agency, as well as its employees may be held accountable for the use and misuse of these resources. The use of any computer-related resources shall not be in a manner inconsistent with State of Ohio policies, Industrial Commission policies or interfere with the work or mission of the State of Ohio or of the Industrial Commission. It is the responsibility of the Information Technology staff, as well as the individual employee to maintain the integrity and stability of Industrial Commission computer resources. This includes protecting the confidentiality and security of any computer resources assigned to an employee. Employees are responsible for complying with policies, procedures, and standards relating to the information security policy.

III. Applicability:

This policy applies to all employees of the Industrial Commission of Ohio.

IV. Procedures:

A. Acceptable Use

- Use only software that is approved, licensed, and installed by Information Technology staff.
- With the exception of Information Technology staff, allow no one, including self, to install software or alter the configuration of any equipment.
- Purchasing of personal computer software and peripherals is to be approved by Information Technology.
- Coordinate the moving of equipment with Information Technology.
- Report known damage to, or failure of hardware or software to Information Technology.
- Maintain reasonably unpredictable passwords on all accounts requiring passwords. Keep all passwords confidential.

- Refrain from setting any Basic Input Output System (BIOS) password, or placing passwords on individual files without the consent of Information Technology.
- Properly sign-off of the network at the end of each working day unless otherwise directed from Information Technology staff.
- Do not interfere with, or terminate any anti-virus software that may be running on a workstation.
- Employees are not permitted to store files on the local hard drive of a workstation.
- Employees may be held accountable for the loss of agency work product not properly stored.
- Employees are not permitted to intentionally access, create, store, or transmit material considered to be offensive, indecent, obscene, or embarrassing to the agency.
- Access to the Internet from state-owned equipment must comply with all IC computer policies.
- Employees are not permitted to grant family members or other non-employees access to agency computer systems.
- Employees must not otherwise engage in acts contrary to IC policies and purposes.
- Employees must not encrypt or conceal unauthorized use of IT resources. Impeding the State's ability to access, inspect and monitor IT resources is strictly prohibited.
- Any use of State provided IT resources to operate, participate in, or contribute to an online community including but not limited to: Instant messaging (IM), online forums, chat rooms, listservs, blogs, wikis, peer-to-peer file sharing and social networks, is strictly prohibited unless organized or approved by the Industrial Commission.

B. Internet, Email, Online Services Use

Information Technology cannot guarantee the confidentiality of any messages or documents stored on the system. Activity logs will be kept for all Internet and electronic mail traffic. These logs will contain the location, and duration of time spent at location if applicable, of all traffic into and out of the agency. These logs may be periodically reviewed to ensure that available resources are being used in an appropriate manner. In order to protect the stability and security of its computer systems, the Industrial Commission may employ hardware or software systems, which monitor or prohibit the use of certain types of software and/or data from being accessed or utilized on the Industrial Commissions computer system. Electronic files created, sent, received, or stored on agency resources, including personal files and documents, are not considered private. Electronic files may be accessed by designated information technology staff at the direction of the executive director at any time. The State of Ohio reserves the right to view any files and electronic communications on state computers, monitor and log all electronic activities, and report findings to the Office of Human Resources and/or appropriate management staff.

C. Unacceptable Use

Any personal use of IT resources that disrupts or interferes with government business, incurs an undue cost to the State of Ohio or the Industrial Commission, could potentially embarrass or harm the State of Ohio or the Industrial Commission, or has the appearance of impropriety to the State of Ohio or the Industrial Commission is considered unacceptable use and employees may be subject to disciplinary action.

Personal use which is strictly prohibited includes, but is not limited to:

- Violation of Law – Violating or supporting and encouraging the violation of local, state, or federal law is strictly prohibited.
- Illegal Copying – Downloading, duplicating, disseminating, printing, or otherwise using copyrighted materials (i.e. including but not limited to software, texts, music, movies, and graphics, etc.) is strictly prohibited.
- Operating a Business – Operating business using state equipment and/or resources, directly or indirectly, for personal gain is strictly prohibited.
- Accessing Personals Services - Accessing or participating in any type of personals ads or services (i.e. dating services, matchmaking services, companion finding services, pen pal services, escort services, personals ads, etc.) is strictly prohibited.
- Accessing Sexually Explicit Material - Downloading, displaying, transmitting, duplicating, storing, or printing sexually explicit material is strictly prohibited.
- Harassment - Downloading, displaying, transmitting, duplicating, storing, or printing material that is offensive, obscene, threatening, or harassing is strictly prohibited.
- Gambling or Wagering - Organizing, wagering on, participating in or observing any type of gambling event or activity is strictly prohibited.
- Mass Emailing - 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.
- Solicitation - Except for agency-approved efforts, soliciting for money or support on behalf of charities, religious entities or political causes is strictly prohibited.
- Portable Computing Devices - State-owned and state-authorized portable computing devices, removable storage components, and removable computer media must be protected from unauthorized access.
    - Devices must be stored in a secure environment.
    - Devices should not be left unattended without employing adequate safeguards such as cable locks, restricted access environments, or lockable cabinets.
    - When possible, portable computing devices, computer media, and removable components shall remain under visual control while traveling.
    - Safeguards should be taken to avoid unauthorized viewing of sensitive or confidential data in public or common areas.