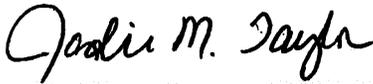


APPOINTING AUTHORITY APPROVAL: 	POLICY NUMBER: ADM007 EFFECTIVE DATE: 04/14/11 REVIEW: 04/22/13
AUTHORITY: R.C.1347.15, O.A.C. Chapter 4121-4 Accessing Confidential Personal Information	APPROVAL DATE: 04/14/11 REVIEW: 04/22/13

I. Purpose:

The Industrial Commission (Commission) is dedicated to developing and implementing information access policies and controls that enhance and ensure the privacy and security of Ohio's citizens who have information stored in the personal information systems maintained by the Commission. The purpose of this Policy is to comply with R.C. 1347.15 and O.A.C. Chapter 4121-4 by regulating access to the confidential personal information (CPI) that the Commission maintains.

II. Applicability:

This Policy applies to all personal information systems maintained by the Commission containing CPI and to all employees of the Commission.

(A) Employees of the Commission shall report all instances of invalid access to CPI of which they have knowledge to his/her supervisor and the Executive Director.

III. Policy:

(A) It is the policy of the Commission that CPI shall be accessed in accordance with R.C.1347.15 and O.A.C. 4121-4-01 – 4121-4-05.

(B) This policy applies to the following Commission personal information systems:

- CAS
- ECM
- ECM Workflow
- ICON
- IC Resource Documents

(1) The remainder of the Commission's personal information systems are exempted from the application of this Policy as the information contained within such systems does not meet the definition of CPI and/or such systems are specifically exempted from the application of O.A.C. 4121-4-02.

(C) This Policy also applies to the CPI contained within the personal information systems of other state agencies and departments to which Commission employees have access in the normal course of their employment duties.

IV. Definitions:

Access: As a noun, the act of copying, viewing or perceiving. As a verb, the retrieval of CPI from a personal information system by name or personal identifier so that CPI is copied, viewed or otherwise perceived.

Computer system: A system that stores, maintains, or retrieves personal information using electronic data processing equipment.

Confidential Personal Information: Personal information that is not a public record for the purposes of R.C. 149.43.

Employee: Each employee of the Commission regardless of whether he or she holds an appointed office or position within the Commission.

Individual: A natural person or the natural person's authorized representative, legal counsel, legal custodian or legal guardian.

Maintains: State or local agency ownership of, control over, responsibility for or accountability for systems and includes, but is not limited to, state or local agency depositing of information with a data processing center for storage, processing, or dissemination. An agency "maintains" all systems of records that are required by law to be kept by the agency.

Personal Information: Any information that describes anything about a person or that indicates actions done by or to a person, or that indicates that a person possesses certain personal characteristics, and that contains, and can be retrieved from a system by name, identifying number, symbol, or other identifier assigned to a person.

Personal Information System: Any system of records that contains all of the following attributes:

- (1) It is a group or collection of records that are kept in an organized manner in either electronic or paper formats.
- (2) It contains "personal information".
- (3) Personal information is retrieved from the system by name or other identifier.
- (4) The agency maintains that system of record.

Research: Methodical investigation into a subject.

Routine: Commonplace, regular, habitual or ordinary.

Valid Business Reason: Reason that reflects an employee's execution of his/her job duties for the Commission.

V. Individual's Request for CPI:

(A) Upon receipt of a signed written request for CPI, the Commission shall verify the identity of the individual making the request and provide the individual with any CPI that does not relate to an on-

going investigation about the individual or is not otherwise excluded from the scope of O.A.C. 4121-4-02 - 4121-4-03.

- (1) If all the requested information relates to an on-going investigation about the individual, the Commission shall inform the individual that it has no CPI that is responsive to their request.

VI. Notice to an Individual of Invalid Access to CPI:

- (A) Upon discovery or notification that an employee of the Commission has accessed an individual's CPI for invalid reasons, the Commission will notify the individual whose CPI was invalidly accessed of the breach of confidentiality within seven state business days.

- (1) If the Commission determines that said notification will delay or impede an investigation regarding the scope of the invalid access, the Commission shall delay this notification for a period necessary to identify the extent of the breach and to restore the integrity of the system.

VII. Valid Reasons for Accessing CPI:

- (A) Employees shall only access CPI for valid business reasons. The following are such reasons:

- (1) Responding to a public records request;
- (2) Responding to a request from an individual for the list of CPI the Commission maintains on that individual;
- (3) Administering a constitutional or statutory provision or duty;
- (4) Administering an administrative rule provision or duty;
- (5) Processing or payment of claims or otherwise administering a program with individual participants or beneficiaries;
- (6) Auditing purposes;
- (7) Eligibility or filing purposes;
- (8) Investigation or law enforcement purposes;
- (9) Administrative hearings;
- (10) Litigation, complying with a court order, or responding to a subpoena;
- (11) Handling human resource matters, including hiring, promotion, demotion, discharge, salary/compensation issues, leave requests/issues and time card issues;
- (12) Complying with an executive order or policy;
- (13) Complying with Commission policy or a state administrative policy issued by the Department of Administrative Services, the Office of Budget and Management or other similar state agencies;
- (14) Complying with a collective bargaining agreement provision; and
- (15) Complying with any state or federal program requirements.

- (B) Employees of the Commission shall maintain the confidentiality of CPI acquired while employed by the Commission both during the employment and after employment.

- (1) The Commission shall provide employees written notification of this policy during the exit process.
- (2) Upon separation, the Commission shall notify any state agencies and state departments that have provided access to CPI to IC employees of the separation.

(C) Access to CPI shall be granted at the lowest level necessary for an employee to perform his/her assigned job duties.

(1) The level of access shall be determined by the employee's manager and shall be dependent on the job duties of the employee and any assignments given to the employee.

(D) An employee's access to CPI shall be removed whenever his/her job duties no longer require such access.

VIII. Procedures for Logging Access to CPI:

Each employee covered by this Policy who accesses or directs another employee of the Commission to access CPI from a personal information system shall record that specific access whenever it is directed toward a specifically named individual or a group of specifically named individuals. The access shall be recorded in the appropriate CPI log maintained for each of the Commission's personal information systems as provided in Section III, paragraph (B) and other personal information systems as defined in Section III, paragraph (C) of this Policy.

Access to CPI is not required to be recorded in a CPI log under the following circumstances:

(A) Logging is not required if the access is the result of research performed for official Commission purposes and is not directed toward a specifically named individual or group of specifically named individuals.

(B) Logging is not required if the access is the result of routine office procedures not directed toward a specifically named individual or group of specifically named individuals.

(C) Logging is not required if the access is the result of incidental contact, where the contact is merely a product of the specific access and not the primary reason of the intended access, and not directed toward a specifically named individual or group of specifically named individuals.

(D) Logging is not required if the access is the result of a request of the person whose information is being accessed or their authorized representative. Logging is not required if an individual requests the Commission to take some action on the individual's behalf and, pursuant to that request, the Commission needs to access CPI to accomplish the action.

(1) For example, IC IT Help Desk personnel would not need to log contact with CPI that occurred as a result of attempting to assist an injured worker in resolving an issue.

(2) Claims examiners or Hearing Officers would not need to log contact with CPI that results from reviewing claim files assigned to them for the purpose of hearing preparation and/or hearings.

IX. Compliance:

Employees required or entitled to access CPI are required to receive training. Training will include understanding R.C. 1347.15 and O.A.C. Chapter 4121-4. Those trained will be expected to understand all information related to the responsibility of accessing CPI and also understand the potential consequences for improperly accessing and/or disseminating CPI.

X. Discipline:

Any Commission employee found to have violated this policy may be subject to disciplinary action, up to and including removal.

XI. Logs:

Pursuant to Section VIII of this Policy, which requires that access to CPI be recorded unless otherwise provided under Section VIII, Commission employees shall maintain a log that records each instance of access to CPI from within the Commission's computer systems as provided in Section III, paragraph (B) and other personal information systems as defined in Section III, paragraph (C) of this Policy. The logs shall contain the following information.

- (A) Name of the personal information system from which an individual's CPI is viewed or retrieved;
- (B) The date of the access;
- (C) Name of the state official accessing the CPI; and
- (D) The name of the person whose CPI was accessed.

These logs shall be maintained pursuant to the Commission's Records Retention Policy.

XII. Inquiries:

Any individual who wishes to inquire whether the Commission has CPI about himself or herself should submit such an inquiry in writing. CPI inquiries should be sent to:

Ohio Industrial Commission
Customer Service Section – L1
30 W. Spring St.
Columbus, OH 43215
614-466-6136 (Columbus area)
1-800-521-2691 (toll-free nationwide)
1-800-686-1589 (toll-free TDD)
Fax: 614-728-7004
AskIC@ic.state.oh.us

**Ohio Industrial Commission
Log of Access to Confidential Personal Information**

Name of Person Accessing CPI

Name (or identifier) of person whose CPI was accessed

Name of Personal Information System from which CPI was accessed

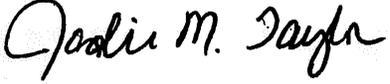
Date & Time

Acknowledgment:

I acknowledge that the information on this log is true and complete and that I have accessed or directed another Commission employee to access CPI that is outside of my job responsibilities.

Signature

Date

APPOINTING AUTHORITY APPROVAL: 	POLICY NUMBER: HR062
	EFFECTIVE DATE: 11/01/07 AMENDMENT: 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

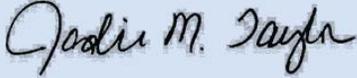
Information Technology cannot guarantee the confidentiality of any messages or documents stored on the system. Activity logs will be kept for all Internet and electronic mail traffic. These logs will contain the location, and duration of time spent at location if applicable, of all traffic into and out 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.

APPOINTING AUTHORITY APPROVAL: 	POLICY NUMBER: IT002 EFFECTIVE DATE: 01/10/12 REVIEWED: 04/03/13
AUTHORITY: ADMINISTRATION, OHIO REVISED CODE SECTIONS 2909.04; 2909.05; 2913.04; 2921.41. STATE OF OHIO INFORMATION TECHNOLOGY POLICY ITP-E.8	APPROVAL DATE: 01/10/12 REVIEWED: 04/03/13

I. Purpose:

This policy establishes controls on the use of Industrial Commission of Ohio (IC) and state provided information technology (IT) resources to ensure that they are appropriately used for the purposes for which they were acquired.

II. Policy:

IC employees' access to the Internet shall be limited and can be further restricted or revoked at the agency's discretion at any time. Employees should only visit sites associated with official activities; in pursuit of information for official business; or those sites associated with other governmental agencies. However, the IC recognizes that it may be necessary for an employee to occasionally access the Internet while at work for personal use. The number and duration of such incidental personal uses shall be kept to a minimum. Incidental personal use is limited to an employee's lunch hour or authorized breaks whenever possible. Incidental personal use of the Internet must not result in direct costs to the agency or interfere with work performance. Employees shall be held accountable for their use of the Internet.

Employees shall have no reasonable expectation of privacy in conjunction with their use of state-provided IT resources. Contents of state computers may be subject to review, investigation and public disclosure. 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. The IC, under the direction of the Executive Director and 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 appropriate supervisors and authorities.

III. Applicability:

This policy applies to all IC employees.

IV. Definitions:

- A. **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."

- B. Chat Room: An online forum where people can broadcast messages to people connected to the same forum in real time. Sometimes, these forums support audio and video communications, allowing people to converse and to see each other.
- C. 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.
- D. Instant Messaging: 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. Examples of instant messaging services include, but are not limited to, AOL Instant Messenger, Yahoo! Messenger and MSN Messenger.
- E. 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, not to be trusted and outside the boundary of the State of Ohio enterprise network.
- F. IT 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.
- G. 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.
- H. Online Forum: A Web application where people post messages on specific topics. Forums are also known as Web forums, message boards, discussion boards and discussion groups.
- I. 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.
- J. 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. Examples include, but are not limited to, eHarmony, Facebook, Friendster, LinkedIn, Match.com, MySpace, Twitter, Plaxo and Yahoo!Groups.
- K. 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.

V. Procedures:

Employees must take reasonable precautions when accessing the Internet to prevent breaches to the security of confidential information and the possibility of contamination to IC systems via viruses or spyware. Employees shall refrain from opening executable files downloaded from the Internet. In the event or suspicion that malicious code has been received, the employee shall report the activity to the IC IT Help Desk immediately.

VI. Unacceptable Personal Use:

Any use of IT resources, including incidental personal use, that disrupts or interferes with government business, incurs an undue cost to the state, could potentially embarrass or harm the state, or has the appearance of impropriety is **strictly prohibited**. Use that is strictly prohibited includes, but is not limited to:

- A. Violation of Law: Violating or supporting and encouraging the violation of local, state or federal law.
- B. Illegal Copying: Downloading, duplicating, disseminating, printing or otherwise using copyrighted materials, such as software, texts, music and graphics, in violation of copyright laws.
- C. Operating a Business: Operating a business, directly or indirectly, for personal gain.
- D. Accessing Personals Services: Accessing or participating in any type of personals ads or services, such as or similar to dating services, matchmaking services, companion finding services, pen pal services, escort services, or personals ads.
- E. Accessing Sexually Explicit Material: Downloading, displaying, transmitting, duplicating, storing or printing sexually explicit material.
- F. Harassment: Downloading, displaying, transmitting, duplicating, storing or printing material that is offensive, obscene, threatening, bullying or harassing.
- G. Gambling or Wagering: Organizing, wagering on, participating in or observing any type of gambling event or activity.
- H. Solicitation: Except for agency-approved efforts, soliciting for money or support on behalf of charities, religious entities or political causes.
- I. Participation in Online Communities: Any 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, instant messaging, blogs, wikis, peer-to-peer file sharing, and social networks, unless organized or approved by the agency. If an individual is approved to participate in any of these forms of communication as part of state business, that person shall complete IC approved security education and awareness requirements for proper use before participating. The content of the education and awareness requirements shall include methods to avoid inadvertent

disclosure of sensitive information and practices to avoid that could harm the security of state computer systems and networks.

- J. Unauthorized Installation or Use of Software: Installing or using unlicensed software or using software including, but not limited to, instant messaging clients and peer-to-peer file sharing software, unapproved web browsing software, or personally owned software, without proper IC approval.
- K. Misrepresentation: Concealing or misrepresenting one's name or affiliation to mask unauthorized, fraudulent, irresponsible or offensive behavior in electronic communications.

VII. Disciplinary Actions:

Violation of this policy may result in disciplinary action under IC policy HR007 Disciplinary Guidelines up to and including removal. In addition, employees may be subject to a 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.