Protecting Confidential and Personal Information

Purpose

The Commission takes seriously the protection of personally identifiable information. This policy provides the requirements for protecting the privacy of people who have personal information in our databases, electronic and paper files and other records. This policy covers all Commission employees even after they leave employment with the Commission. It also covers contractors who gain access to physical facilities or data or computer systems. This policy lays out basic Commission expectations for handing all types of personal information, and it provides important additional handling requirements for sensitive and confidential personal information.

Employees of the Commission shall not discuss the Commission's business with anyone who does not work for the Commission, **including but not limited to permit holders and/or attorneys** and shall never discuss business transactions with anyone who does not have a direct association with the transaction. Even casual remarks can be misinterpreted and repeated.

The Commission speaks through its orders. Employees shall not provide information to anyone, including but not limited to permit holders and/or attorneys, concerning actions taken by the Commission until the order involving that matter has been released, generally by mailing/serving the order to the permit holder and/or the permit holder's attorney.

No employee is permitted to remove or make copies of any Commission records, reports or documents without prior management approval.

The following Commission rules are incorporated into this policy and shall be reviewed by employees annually:

- 4301:1-2-01 Definitions.
- 4301:1-2-02 Procedures for accessing confidential personal information.
- 4301:1-2-03 Valid reasons for accessing confidential personal information.
- 4301:1-2-04 Confidentiality statutes.
- 4301:1-2-05 Restricting and logging access to confidential personal information in computerized personal information systems.

What is Personal Information and What Is Sensitive Personal Information?

For the purposes of this policy, "personally identifiable information" is information that can be used directly or with other information to identify a particular individual, and it includes names and identifying numbers or symbols, and personal information. "Personal information" is defined by Ohio Revised Code 1347.01 and means any information that describes anything about an identifiable 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, a name, identifying number, symbol, or other identifier assigned to a person. Some examples of personally identifiable information are as follows:

- Names
- Social Security numbers
- Resumes
- Correspondence
- Addresses
- Phone numbers
- Driver's license numbers
- State identification numbers
- Professional license numbers
- Financial account information
- Medical and health information
- Physical characteristics and other biometric information
- Tax information
- Education information
- Individuals' job classifications and salary information
- Performance evaluations
- Employment application forms
- Timesheets
- Miscellaneous personnel information

"Sensitive personal information" includes personal information that the Commission has discretion not to release under public records law, and it includes "confidential personal information," which the Commission is restricted or prohibited from releasing under Ohio's public records law. Examples of "sensitive personal information" that the Commission keeps may include the following:

- Social Security numbers
- A person's financial account numbers and information
- Beneficiary information
- Tax information
- Employee voluntary withholdings
- Passwords
- Employee home addresses and phone numbers
- Security challenge questions and answers
- Medical and health information
- Driver's license numbers
- State ID card numbers (as issued by the Ohio Bureau of Motor Vehicles)
- Confidential personal information (see below)

"Confidential personal information" is personal information that falls within the scope of Section 1347.15 of the ORC and that the Commission is prohibited from releasing under Ohio's public records law, such as Social Security numbers or medical information. Confidential personal information may be maintained in the following personal information systems only:

- Legal files (paper files)

Policy

Commission employees and contractors as outlined above must follow these rules on handling all personal information and handling sensitive personal information whenever they know or have reason to know that the information is personally identifiable information or sensitive personal information respectively.

A. Handling All Personal Information

i. Use personally identifiable information only for official, lawful purposes.

ii. Do not access systems with personally identifiable information or sensitive or confidential personal information – whether electronic or paper – if you have not been authorized to do so. Contact your supervisor if you need access.

iii. Enter personal information accurately. Make a good faith effort to correctly enter data. Never intentionally enter false data.

iv. Take reasonable precautions to protect personal information from unauthorized modification, destruction, use or disclosure.

v. Whenever individual requests information that the office maintains about that individual, employees and contractors shall follow the office's procedures concerning requests to inspect personally identifiable information.

vi. Only collect personally identifiable information when you have been authorized to do so by the proper supervisor in the Commission. Do not create a new electronic or paper system of records organized so that personal information is retrieved by name or other identifier of a person unless you have the Commission's authorization and follow the Commission's privacy and security requirements.

vii. Destroy sensitive or confidential personal information securely in accordance with records retention schedules and following appropriate data destruction procedures for particular system or records.

viii. Do not initiate any disciplinary or other punitive action against any individual who reports evidence of unauthorized use of personal information.

ix. The Commission monitors its information, systems, other IT assets, employees and contractors for compliance with this policy. Therefore, employees and contractors have no expectation of privacy when they use state information, systems and IT assets.

B. Handling Sensitive Personal Information

i. **Only access sensitive personal information for a valid reason directly related to the exercise of a Commission power or duty.** Valid reasons include:

- responding to a public records request;
- responding to a request from an individual for the list of personal information the agency maintains on that individual;
- administering a constitutional provision or duty;
- administering a statutory provision or duty;
- administering an administrative rule provision or duty;
- complying with any state or federal program requirements;
- processing or payment of claims or otherwise administering a program with individual participants or beneficiaries;
- auditing purposes;
- carrying out licensure, permit, eligibility, filing, certifications or other similar processes;

- carrying out or assisting with an authorized investigation or law enforcement purposes;
- conducting or preparing for administrative hearings;
- responding to or preparing for litigation, or complying with a court order or subpoena;
- reviewing and responding to constituent inquiries;
- administering human resources, including but not limited to hiring, promotion, demotion, discharge, salary and compensation issues, leave requests and related issues, time card approvals and related issues, and reviewing applicant information;
- administering an information system;
- complying with an executive order or policy; or
- complying with an agency policy or a state administrative policy issued by the Department of Administrative Services/CSA, the Office of Budget and Management or other similar state agency.

ii. **Do not access sensitive personal information**
- for gain or personal profit for yourself or someone else;
- out of simple curiosity or personal interest;
- to commit a crime;
- for retribution, use in a personal conflict, or promotion of a personal point of view; or
- to harass or embarrass, or for any other improper purpose.

iii. **You always have a duty not to disclose sensitive personal information without proper agency authorization.** As you do your work, you may inadvertently or unintentionally come in contact with information that you know or have reason to believe is sensitive personal information. In those circumstances, you have a duty not to disclose that sensitive personal information to anyone except properly authorized persons.

iv. **If you suspect that sensitive personal information has been improperly accessed or disclosed, you shall report the incident to the Executive Director. The Director will contact the DAS Data Privacy Point of Contact at (614) 387-1602**.
- Report quickly and do not disturb evidence.
- Allow the Commission to preserve evidence, eliminate any ongoing risks and make a determination that violations have occurred.
- To ensure that any investigation is not compromised and that an accurate evaluation of the incident is conducted, only the Assistant Director or the Executive Director or their designee(s) may authorize notifications to affected individuals.
- Upon a finding that confidential personal information has been accessed for an invalid reason in violation of a confidentiality statute, Section

1347.15 of the ORC or rules of Administrative Code, the Assistant Director or the Executive Director or their designee(s) will notify affected individuals.

v. The Commission does not collect confidential personal information (CPI). However, in the event the Commission in the future begins collecting CPI, the Commission understands that because CPI requires a higher standard of care, employees accessing a CPI system shall follow the privacy procedure specific to that system.
   - FileMaker Pro (a potential CPI system) (FileMaker Pro is a system that is not set up to collect CPI).

C. Authorizing Access

i. An account with a unique password is created for each employee who has authorized access to a system containing confidential personal information.
ii. When an employee no longer needs access to the system his/her account will be closed terminating access to the system.
iii. The employee's supervisor shall contact the Executive Director when such access is no longer needed.

Violations

A. Any employee who violates this policy is subject to disciplinary action up to and including termination.
B. Any employee who violates an applicable confidentiality statute or rule is subject to criminal charges, civil liability arising out of the employee's actions, employment termination and a prohibition against working for the State of Ohio.
C. Any violation of this policy by a contractor may be considered a material breach of the contract and may subject the contract to termination. Any contractor who violates a confidentiality statute or applicable rule also may be subject to criminal charges and civil liability arising out of the contractor's actions. The vendor may also be subject to vendor debarment.
D. An employee or contractor who complies in good faith with this policy is not subject to discipline under this policy.
E. This policy does not prohibit an employee from accessing information about himself or herself as long as the person has been granted access to the system and uses authorized processes, or makes a request to the Commission for a list of the personal information that the office maintains about the individual.

Questions

For questions regarding this policy, please contact the Executive Director (614-644-9200) or the Commission's Assistant Director (614-466-3132).