DAVE YOST
OHIO ATTORNEY GENERAL

➢ CONFIDENTIAL PERSONAL INFORMATION ACCESS POLICY

Effective Date: **January 15, 2016**

I. PURPOSE

Confidential personal information has very specific legal requirements regarding its protection. The purpose of this policy is to inform Ohio Attorney General's Office (AGO) employees about their responsibilities regarding the protection of confidential personal information (CPI), outline valid reasons for accessing CPI, and set forth the potential liability should CPI be misused or accessed for unauthorized reasons.

II. SCOPE

This policy applies to all full-time or part-time permanent, temporary, or intermittent employees, (except as otherwise provided in R.C. 1347.04), interns and externs, consultants, and contractors of the AGO who gain access to AGO physical facilities or data or electronic and paper systems that are determined to contain CPI. For guidelines on how to handle access and disclosure of data contained in any of these systems, refer to the AGO Confidentiality/Sensitive Data and Information Use Policy.

III. AUTHORITY

• ORC 1347.01, .04, and .15

• OAC 109-4-01 through 109-4-04

IV. DEFINITIONS

"Personal information" means 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, a name, identifying number, symbol, or other identifier assigned to a person. A few examples include: names, Social Security Numbers, driver's license numbers, state identification numbers, and professional license numbers. Some of this personal information is sensitive and may have additional privacy protection requirements, such as Social Security Numbers (SSN), medical records, bank account information, and educational records.

"Confidential personal information" is personal information maintained in a personal information system that falls within the scope of section 1347.15 of the Revised Code and that the AGO is prohibited from releasing under Ohio's public records law.

"Access," for the purposes of this policy, means the retrieval of confidential personal information from a personal information system using a name or personal identifier so that CPI is viewed, and/or so that CPI is copied or retained outside of the personal information system.

"Data Privacy Point of Contact" ORC 1347.15(B)(7) requires state agencies to designate a data privacy point of contact, who will perform all duties required in ORC 1347(B)(7)and (8), including, but not limited to identifying CPI systems, ensuring privacy impact assessments are completed, and providing consultation on CPI guideline development, and individual requests for CPI.

V. PROVISIONS

A. Generally

1. Many AGO employees are entrusted with sensitive personal information. It is the responsibility of all AGO employees that sensitive information is only seen by those who need it. Sometimes AGO employees are required to share this information with another authorized agency. In such cases, sensitive personal information, such as the SSN, should be encrypted when sent via e-mail. In addition, no sensitive data should be shared via any other cloud service used to transfer files. Only AGO-owned devices should be used to process, store, or view sensitive data.
2. The AGO collects and maintains confidential personal information for a number of authorized purposes, and will maintain an agency-wide inventory of all CPI systems that is updated annually.
3. The requirements employees must follow regarding confidentiality and requests for information can be found in the AGO's Public Relations and Professional Demeanor policy.

B. Identification of CPI Systems within the AGO

1. Information systems in the Bureau of Criminal Identification and Investigation (BCI), the Ohio Peace Officer's Training Academy (OPOTA), the Ohio Organized Crime Investigations Commission (OOCIC), and in AGO sections or units that perform law enforcement and/or prosecutorial functions are exempt from the provisions of ORC 1347. Also exempt are systems that contain routine information that is maintained for the purpose of internal office administration, the use of which would not adversely affect a person. One example is the Online Payroll Application (OPA).
2. Prior to authorizing access to a system, users will be informed by section leadership, and notification upon log on to a system if technically feasible, if an information system contains CPI.
3. Even if a system containing personally identifiable information is seemed to be exempt from the requirements of ORC 1347.15, the AGO is still committed to protecting the personal information held in trust in all of its systems.

C. CPI System Specific Policies

Each section with one or more identified CPI systems will adopt a written set of guidelines specific to each CPI system regarding who can authorize access and proper record-keeping of the system. The Internal Audit Section of the AGO will include examination of section guidelines and compliance with those guidelines in its audits.

D. Employee CPI Training

Each section will ensure that employees of that section receive training about AGO rules and policies regarding access to CPI, as well as system specific guidelines for each system to which employees have access.

E. Valid Reasons for Accessing CPI Systems

1. Employees may only access confidential personal information for a valid reason directly related to the exercise of an AGO power or duty. Each employee is assigned a level of access to AGO information systems that reflects his/her position and work assignments. Access to each system within a section is determined by section leadership and/or agency leadership. Whenever there are changes in an individual's employment situation (transfers/promotions/exits), access levels will be reviewed and updated accordingly.
2. The following functions constitute valid reasons for authorized individuals to access confidential personal information:
    a) Responding to a public records request;
    b) Responding to a request from an individual for the list of CPI the office maintains on that individual;
    c) Administering a constitutional provision or duty;
    d) Administering a statutory provision or duty;
    e) Administering an administrative rule provision or duty;
    f) Complying with any state or federal program requirements;
    g) Processing or payment of claims or grants or otherwise administering a program with individual participants or beneficiaries;
    h) Auditing purposes;
    i) Licensure processes;
    j) Investigation or law enforcement purposes;
    k) Administrative hearings;
    l) Litigation, complying with an order of the court, or subpoena;
    m) Human resource matters (e.g., hiring, promotion, demotion, discharge, salary/compensation issues, leave requests/issues, time reporting approvals/issues);
    n) Complying with an executive order or policy;
    o) Complying with an office policy or a state administrative policy issued by the Department of Administrative Services, the Office of Budget and Management or other similar state agency;

p) Complying with a collective bargaining agreement provision;
q) Supervising the work of another employee; or
r) Providing information technology technical support.

F. Handling All Personally Identifiable Information

AGO employees shall use personally identifiable information only for official, lawful purposes. The following are additional requirements that AGO employees must follow in handling all personally identifiable information:

1. Use personally identifiable information only for official, lawful purposes.
2. Do not access systems with personally identifiable information – whether electronic or paper – if you have not been authorized to do so. Contact your supervisor if you think you need access.
3. Enter personally identifiable information accurately. Make a good faith effort to correctly enter data. Never intentionally enter false data.
4. Take reasonable precautions to protect personally identifiable information from unauthorized modification, destruction, use or disclosure.
5. Whenever an individual requests information that the AGO maintains about that individual, employees and contractors shall follow the guidelines in Section H of this policy.
6. Only collect personally identifiable information when you have been authorized to do so by section leadership and/or agency leadership through the ITS governance process. Do not create an electronic or paper system of record with confidential personally identifiable information unless you have AGO authorization per AGO standard operating procedures, following AGO mandated privacy and security requirements maintained by Information Technology Services.
7. Destroy personally identifiable information securely in accordance with records retention schedules and following the AGO data destruction procedures for particular systems or records.
8. Employees and contractors shall have no expectation of privacy when they use state information, systems and IT assets, in accordance with the AGO Technology Policy.

G. Log Management

Many newer AGO electronic personal information systems that contain CPI will include a mechanism for logging individual employee access. These logs will be maintained by the Information Technology Services section. For systems that contain CPI that do not include such a mechanism, a standard log will be maintained by the section with system oversight responsibilities, to manually document authorized access to the system. Logs will be retained in accordance with record retention schedules. Standard logs should contain the name of the CPI System, date/time accessed, employee name accessing CPI, manager name requesting access to CPI, identification of the person whose CPI was accessed, and acknowledgement that access was by an authorized user for valid purposes. However, access to CPI need not be logged if:

- The access occurs as a result of a request of the person whose information is being accessed.
- The access to CPI is not targeted to a specifically named individual or a group of specifically named individuals.
- The access occurs as a result of research performed for official AGO purposes and/or incidental contact and does not target a specific individual or individuals.
- The access is to CPI stored in a paper-based system.

H. Responding to an Individual's Request for CPI

When an individual requests that an employee provide all confidential personal information about the individual that is in the possession of the section and/or the AGO generally, the employee shall immediately notify the section chief of the request. The section chief shall then notify the AGO-Privacy Point of Contact (AGO-PPC) of the request so that all sources of CPI shall be researched. The individual requesting the information shall be provided a written response from the AGO-PPC within a reasonable amount of time.

VI. PROHIBITIONS

A. Misuse of CPI

Accessing information for any purpose other than as delineated in this policy is strictly prohibited. Misuse of confidential personal information may include, but is not limited to:

1. Intentionally entering inaccurate or incomplete personal information that may result in harm;
2. Intentionally supplying personal information that is false, or that the person has reason to know is false;
3. Intentionally using or disclosing the personal information in a manner prohibited by law;
4. Intentionally denying to an affected individual the right to inspect and dispute the personal information at a time when inspection or correction might have prevented harm;
5. Knowingly accessing confidential personal information in a manner that violates AGO rules regarding access to confidential personal information.

B. Reporting Unauthorized Access or Misuse of CPI

Any employee who is aware of unauthorized access to a specific individual(s) confidential personal information or misuse of CPI has a duty to report the incident(s) to any one of these individuals:

1. the employee's immediate supervisor,
2. the employee's section chief,
3. the Director of Human Resources,
4. the Chief Operating Officer.

The incident report should indicate the following:

1. the information that was accessed or misused,
2. the nature of the misuse of CPI,
3. the circumstances under which the information was accessed or misused,

4. how the individual learned of the unauthorized access or misuse and any documentation, and/or
5. additional information supporting the allegation of unauthorized access or other misuse.

The recipient of the incident report will inform the Director of Human Resources. The Director of Human Resources will make an initial determination regarding whether or not there was misuse, or in cases of suspected unauthorized access, if the access was authorized or inadvertent. If there is a finding of misuse of CPI, action will be taken in accordance with ORC 1347.15 and this policy.

C. Retaliation and False Allegations

No person reporting unauthorized access shall be retaliated against. However, making a false or bad faith allegation of unauthorized access may lead to discipline.

VII. PENALTIES

Violations of the Ohio Revised Code 1347.15 or this policy may result in discipline up to and including removal, civil liability and penalties, criminal prosecution, and/or prohibition of employment with the State of Ohio for the employee's lifetime.

VIII. CONTACT

The Chief Data Officer is the AGO Data Privacy Point of Contact and is available for consultation or questions regarding the provisions of this policy. This policy supersedes any previously issued directive or policy and will remain effective until cancelled or superseded.