




POLICY
Ohio Department of Taxation

Policy Description:
Accessing Confidential
Personal Information

Policy No: ODT – CC – 001

Authorities:

Ohio Revised Code 1347.15, 5703.211
Ohio Adm. Code 5703-31-01 through 05

Pages: 10 Pages

Effective Date: February 1, 2011

Divisions With Primary Responsibility:

Office of Chief Counsel
ODT's Designated Privacy Point of Contact

Supersedes: New Policy

1. PURPOSE

Controlling Access to Confidential Personal Information

This policy is issued to provide employees of the Ohio Department of Taxation (ODT) with guidance needed to comply with the provisions of the Ohio Revised Code¹ (RC) and the Ohio Administrative Code² (OAC) relating to access to confidential personal information (CPI). Terms used in this policy have the meanings defined in Ohio Administrative Code 5703-31-01, which appears in the appendix of this policy.

2. POLICY

A. ODT Employees Have Access to Systems on a Need-to-Know Basis

Each ODT employee is assigned a level of access to ODT information systems on a need-to-know basis. The level of access reflects the employee's informational needs, as determined by the employee's job description and assigned duties. The employee's level of access is approved by the employee's supervisor and the business owner of the information system. The level of access will be reviewed every time the employee is transferred or promoted, as well as at the time of the employee's annual access review. When an employee is in a position which does not require access to a particular information system, or when the employee ceases employment with ODT, the employee's access to the system will be removed.

¹ Ohio Revised Code 1347.15 and 5703.211

² Ohio Administrative Code 5703-31-1 through 5703-31-5.

B. Requests for Information

When an individual requests a list of, or copies of, all CPI which ODT maintains on that individual, the request will be forwarded to ODT's Designated Privacy Point of Contact (DPPoC). The DPPoC will do the following:

- Verify the requesting individual's identity to safeguard against improper disclosure.
- Provide the list or copies of information requested to the individual, except information relating to a law enforcement investigation about the individual that is excluded from the scope of Chapter 1347. of the Revised Code.
- If the only information in ODT's possession about the individual relates to a law enforcement investigation about that individual, the DPPoC will inform the individual that there is no CPI in ODT's possession which is responsive to the individual's request.

C. Valid Access of CPI

CPI maintained on ODT's systems may only be accessed by ODT employees for valid business purposes. Such valid purposes include the following:

- Responding to calls and correspondence from taxpayers and their authorized representatives regarding their accounts and updating ODT systems with current information.
- Responding to public records request. Note, however, that an individual's CPI maintained in ODT's systems would never be released to another individual as part of a public records request.
- Responding to a request from an individual for a list of, or copies of, the CPI which ODT maintains on that individual.
- Processing tax returns, including tax payments, and tax refund claims.
- License and permit processes which are part of ODT's authority.
- Complying with state or federal program requirements and/or administering a constitutional, statutory, or administrative rule provision or duty.
- Investigating, auditing, conducting compliance programs or conducting law enforcement activities under ODT's authority.
- Preparing for ODT litigation or complying with an order or subpoena of a court.
- Conducting administrative hearings.
- Complying with an executive order or policy, or an ODT policy, or a policy issued by the Ohio Department of Administrative Services, or the Ohio Office of Budget and Management.
- Complying with a collective bargaining agreement provision.
- Working with the Ohio Attorney General's office or its designee regarding collection and compromise matters.
- Developing, implementing, or supporting ODT's computer systems including interfaces with other agencies.
- Administering programs to discover delinquent or noncompliant taxpayers.
- Performing internal audit functions and investigations.
- Drafting final determinations.

- Assisting other agencies in tax administration and compliance as authorized under Ohio and federal statutes.
- Performing human resource functions, e.g., hiring, promotion, demotion, discharge, compensation issues, leave requests/issues, time card approvals/issues.

D. Invalid / Improper Access of CPI

Examples of invalid / improper access include looking up information regarding relatives, acquaintances, neighbors, celebrities or others for which there is no valid business purpose. In the event an ODT employee is contacted by a relative or acquaintance and asked to look up that person's CPI to resolve a tax issue, the employee should notify his/her supervisor. The supervisor can explain to the requester that another agent will handle the request.

If any ODT employee becomes aware of an invalid or improper access of CPI, the employee must immediately notify his/her supervisor who will immediately notify the DPPoC as well as others in the chain of command including the Division Administrator. The DPPoC and Division Administrators shall immediately advise the Human Resources Division of the allegation. The DPPoC will notify the individual whose information was improperly accessed.³ The notification will include a description of the CPI improperly accessed and the date(s). The notification may be made in writing, by email, or by telephone.

E. Restricting Access to CPI

All ODT systems which contain CPI will be password protected, as discussed in ODT-IT-02, dated 7/15/2005, revised 2/1/2007.

F. Acquisition of New Computer Systems or Upgrades of Existing Computer Systems

When ODT acquires a new computer system that stores, manages, or contains CPI, ODT shall include a tracking mechanism which will record, for each instance of access, the date, time, and identity of the ODT employee who accessed the CPI. When ODT upgrades an existing computer system that stores, manages, or contains CPI, ODT shall include a tracking mechanism which will record, for each instance of access, the date, time, and identity of the ODT employee who accessed the CPI.

G. Manual Logging Requirements

When using existing ODT computer systems containing CPI which do not have a tracking mechanism as described in Paragraph F, ODT employees are required to make entries in a log, unless the access is subject to an exception as discussed below. The log will be in a database maintained centrally by ODT. The records in the log will be maintained for two years. Each log entry will contain the following:

- Identity of ODT employee.
- Date of access.

³ The DPPoC may delay notification of the individual for only the following reasons: If notification would impede an ongoing investigation regarding the circumstances and scope of the improper access, or jeopardize homeland or national security.

- SSN or other account number of the individual whose CPI was accessed.
- Purpose of access.

ODT employees are not required to log access to CPI when the access is made under either the following circumstances:

- The individual requests CPI about himself/herself. For example, if a taxpayer calls ODT and asks if his income tax return has been received, the ODT agent who looks up the taxpayer's filing is not required to make a log entry of that action.
- The individual requests ODT to take some action and that action requires access to CPI. For example, the individual sends a letter to ODT objecting to an income tax billing. The ODT agents who are working that correspondence are not required to log their access to the taxpayer's CPI.

ODT employees are not required to log access to CPI when the access is not directed toward a specifically named individual or a group of specifically named individuals and the access is made for any of the following purposes:

- Official ODT purposes, including research. For example, accessing CPI to determine which taxpayers should be included in an income tax delinquency program does not require logging.
- Routine office procedures. For example, searching a system with a taxpayer's name to match a payment to a taxpayer's account does not require logging.
- Incidental contact. For example, testing the search capabilities of a computer system with CPI does not require logging.

H. Data Privacy Point of Contact

ODT's Data Privacy Point of Contact (DPPoC) is the Legal Counsel for Income Tax and Compliance Divisions. ODT's DPPoC will do the following:

- Assist ODT with implementation of privacy protections for CPI which ODT maintains.
- Ensure ODT's compliance with Ohio Revised Code 1347.15 and 5703.221 and Ohio Administrative Code sections 5703-31-01 through 05.
- Complete privacy impact assessments as required by the Ohio Office of Information Technology.

3.0 APPENDIX

Ohio Administrative Code 5703-31-01 Definitions.

For the purposes of administrative rules promulgated in accordance with sections 1347.15 and 5703.211 of the Revised Code, the following definitions apply:

(A) "**Access**" as a noun means an instance of copying, viewing, or otherwise perceiving whereas "access as a verb means to copy, view, or otherwise perceive.

(B) "**Acquisition of a new computer system**" means the purchase of a "computer system," as defined in this rule, that is not a computer system currently in place nor one for which the acquisition process has been initiated as of the effective date of the agency rule addressing requirements in section 1347.15 of the Revised Code.

(C) "**Computer system**" means a "system," as defined by section 1347.01 of the Revised Code, that stores, maintains, or retrieves personal information using electronic data processing equipment.

(D) "**Confidential personal information**" (CPI) has the meaning as defined by division (A)(1) of section 1347.15 of the Revised Code and identified by rules promulgated by the agency in accordance with division (B) (3) of section 1347.15 of the Revised Code that reference the federal or state statutes or administrative rules that make personal information maintained by the agency confidential.

(E) "**Employee of the state agency**" means each employee of a state agency regardless of whether he/she holds an elected or appointed office or position within the state agency. "Employee of the state agency" is limited to the specific employing state agency.

(F) "**Incidental contact**" means contact with the information that is secondary or tangential to the primary purpose of the activity that resulted in the contact.

(G) "**Individual**" means a natural person or the natural person's authorized representative, legal counsel, legal custodian, or legal guardian.

(H) "**Information owner**" means the individual appointed in accordance with division (A) of section 1347.05 of the Revised Code to be directly responsible for a system.

(I) "**Person**" means a natural person.

(J) "**Personal information**" has the same meaning as defined in division (E) of section 1347.01 of the Revised Code.

(K) "**Personal information system**" means a "system" that "maintains" "personal information" as those terms are defined in section 1347.01 of the Revised Code.

"System" includes manual and computer systems.

(L) "**Research**" means a methodical investigation into a subject.

(M) "**Routine**" means commonplace, regular, habitual, or ordinary.

(N) "**Routine information that is maintained for the purpose of internal office administration, the use of which would not adversely affect a person**" as that phrase is used in division (F) of section 1347.01 of the Revised Code means personal information relating to employees and maintained by the agency for internal administrative and human resource purposes.

(O) "**System**" has the same meaning as defined by division (F) of section 1347.01 of the Revised Code.

(P) "**Upgrade**" means a substantial redesign of an existing computer system for the purpose of providing a substantial amount of new application functionality, or

application modifications that would involve substantial administrative or fiscal resources to implement, but would not include maintenance, minor updates and patches, or modifications that entail a limited addition of functionality due to changes in business or legal requirements.

(Q) "**Database**," as used in section 5703.211 of the Revised Code, means a "system" that contains "personal information" as those terms are defined in section 1347.01 of the Revised Code.

5703-31-02 Procedures for accessing confidential personal information.

For personal information systems, whether manual or computer systems, that contain confidential personal information, the agency shall do the following:

(A) Criteria for accessing confidential personal information. Personal information systems of the agency are managed on a "need-to-know" basis whereby the information owner determines the level of access required for an employee of the agency to fulfill his/her job duties. The determination of access to confidential personal information shall be approved by the employee's supervisor and the information owner prior to providing the employee with access to confidential personal information within a personal information system. The agency shall establish procedures for determining a revision to an employee's access to confidential personal information upon a change to that employee's job duties including, but not limited to, transfer or termination. Whenever an employee's job duties no longer require access to confidential personal information in a personal information system, the employee's access to confidential personal information shall be removed.

(B) Individual's request for a list of confidential personal information. Upon the signed written request of any individual for a list of confidential personal information about the individual maintained by the agency, the agency shall do all of the following:

- (1) Verify the identity of the individual by a method that provides safeguards commensurate with the risk associated with the confidential personal information;
- (2) Provide to the individual the list of confidential personal information that does not relate to an investigation about the individual or is otherwise not excluded from the scope of Chapter 1347. of the Revised Code; and
- (3) If all information relates to an investigation about that individual, inform the individual that the agency has no confidential personal information about the individual that is responsive to the individual's request.

(C) Notice of invalid access.

- (1) Upon discovery or notification that confidential personal information of a person has been accessed by an employee for an invalid reason, the agency shall notify the person whose information was invalidly accessed as soon as practical and to the extent known at the time. However, the agency shall delay notification for a period of time necessary to ensure that the notification would not delay or impede an investigation or jeopardize homeland or national security. Additionally, the agency may delay the notification consistent with any measures necessary to determine the scope of the invalid

access, including which individuals" confidential personal information invalidly was accessed, and to restore the reasonable integrity of the system. "Investigation" as used in this paragraph means the investigation of the circumstances and involvement of an employee surrounding the invalid access of the confidential personal information. Once the agency determines that notification would not delay or impede an investigation, the agency shall disclose the access to confidential personal information made for an invalid reason to the person.

(2) Notification provided by the agency shall inform the person of the type of confidential personal information accessed and the date(s) of the invalid access.

(3) Notification may be made by any method reasonably designed to accurately inform the person of the invalid access, including written, electronic, or telephone notice.

(D) Appointment of a data privacy point of contact. The agency director shall designate an employee of the agency to serve as the data privacy point of contact. The data privacy point of contact shall work with the chief privacy officer within the office of information technology to assist the agency with both the implementation of privacy protections for the confidential personal information that the agency maintains and compliance with section 1347.15 of the Revised Code and the rules adopted pursuant to the authority provided by that chapter.

(E) Completion of a privacy impact assessment. The agency director shall designate an employee of the agency to serve as the data privacy point of contact who shall timely complete the privacy impact assessment form developed by the office of information technology.

5703-31-03 Restricting and logging access to confidential personal information in computerized personal information systems.

For personal information systems that are computer systems and contain confidential personal information, the agency shall do the following:

(A) Access restrictions. Access to confidential personal information that is kept electronically shall require a password or other authentication measure.

(B) Acquisition of a new computer system. When the agency acquires a new computer system that stores, manages or contains confidential personal information, the agency shall include a mechanism for recording specific access by employees of the agency to confidential personal information in the system.

(C) Upgrading existing computer systems. When the agency modifies an existing computer system that stores, manages or contains confidential personal information, the agency shall make a determination whether the modification constitutes an upgrade. Any upgrades to a computer system shall include a mechanism for recording specific access by employees of the agency to confidential personal information in the system.

(D) Logging requirements regarding confidential personal information in existing computer systems.

(1) The agency shall require employees of the agency who access confidential personal information within computer systems to maintain a log that records

that access.

(2) Access to confidential information is not required to be entered into the log under the following circumstances:

(a) The employee of the agency is accessing confidential personal information for official agency purposes, including research, and the access is not specifically directed toward a specifically named individual or a group of specifically named individuals.

(b) The employee of the agency is accessing confidential personal information for routine office procedures and the access is not specifically directed toward a specifically named individual or a group of specifically named individuals.

(c) The employee of the agency comes into incidental contact with confidential personal information and the access of the information is not specifically directed toward a specifically named individual or a group of specifically named individuals.

(d) The employee of the agency accesses confidential personal information about an individual based upon a request made under either of the following circumstances:

(i) The individual requests confidential personal information about himself/herself.

(ii) The individual makes a request that the agency takes some action on that individual's behalf and accessing the confidential personal information is required in order to consider or process that request.

(3) For purposes of this paragraph, the agency may choose the form or forms of logging, whether in electronic or paper formats.

(E) Log management. The agency shall issue a policy that specifies the following:

(1) Who shall maintain the log;

(2) What information shall be captured in the log;

(3) How the log is to be stored; and

(4) How long information kept in the log is to be retained.

Nothing in this rule limits the agency from requiring logging in any circumstance that it deems necessary.

(F) Compliance with the logging requirements set forth in this rule shall constitute compliance with the provisions for tracking searches of databases set forth in R.C. 5703.211.

5703-31-04 Confidentiality statutes.

The following federal statutes or state statutes make personal information maintained by the agency confidential and identify the confidential personal information within the scope of rules promulgated by this agency in accordance with section 1347.15 of the Revised Code:

(A) Social security numbers: 5 U.S.C. 552a., unless the individual was told that the number would be disclosed;

- (B) "Bureau of Criminal Investigation and Information" criminal records check results: section 4776.04 of the Revised Code;
- (C) Confidentiality and disclosure of returns and return information: Internal Revenue Code 6103;
- (D) Unauthorized disclosure of information: Internal Revenue Code 7213;
- (E) Unauthorized inspection of returns or return information: Internal Revenue Code 7213A;
- (F) Civil damages for unauthorized inspection or disclosure of returns and return information: Internal Revenue Code 7431
- (G) Prohibition against divulging information: Ohio Revised Code 5703.21;
- (H) Confidentiality of financial information regarding personal property taxation: Ohio Revised Code 5711.101;
- (I) Confidentiality of certain estate tax information: Ohio Revised Code 5731.90;
- (J) Confidentiality of annual franchise tax report: Ohio Revised Code 5733.03(G);
- (K) Confidentiality of information resulting from investigations: Ohio Revised Code 5739.35;
- (L) Confidentiality of income tax information: Ohio Revised Code 5747.18(C);
- (M) Confidentiality of commercial activity tax information: Ohio Revised Code 5751.12;
- (N) Confidentiality of information relating to opinions of the tax commissioner: Ohio Revised Code 5703.53;
- (O) Confidentiality of motor fuel tax information: Ohio Revised Code 5735.33;
- (P) Confidentiality of use tax investigation information: Ohio Revised Code 5741.24; and
- (Q) Confidentiality of cigarette tax information: Ohio Revised Code 5743.45.

5703-31-05 Valid reasons for accessing confidential personal information.

Pursuant to the requirements of division (B)(2) of section 1347.15 of the Revised Code, this rule contains a list of valid reasons, directly related to the department of taxation's exercise of its powers or duties, for which only employees of the agency may access confidential personal information (CPI) regardless of whether the personal information system is a manual system or computer system:

(A) Performing the following functions constitute valid reasons for authorized employees of the agency to access confidential personal information:

- (1) Responding to a public records request;
- (2) Responding to a request from an individual for the list of CPI the agency maintains on that individual;
- (3) Administering a constitutional provision or duty;
- (4) Administering a statutory provision or duty;
- (5) Administering an administrative rule provision or duty;
- (6) Complying with any state or federal program requirements;
- (7) Processing of tax returns, including all submitted tax payments, and processing of refunds due to taxpayers;
- (8) Auditing purposes;
- (9) Licensure or permit processes;
- (10) Investigation or law enforcement purposes;
- (11) Administrative hearings;

- (12) Litigation, complying with an order of the court, or subpoena;
- (13) Human resource matters (e.g., hiring, promotion, demotion, discharge, salary/compensation issues, leave requests/issues, time card approvals/issues);
- (14) Complying with an executive order or policy;
- (15) Complying with an agency policy or a state administrative policy issued by the department of administrative services, the office of budget and management or other similar state agency; or
- (16) Complying with a collective bargaining agreement provision.

(B) To the extent that the general processes described in paragraph (A) of this rule do not cover the following circumstances, for the purpose of carrying out specific duties of the Ohio department of taxation, authorized employees would also have valid reasons for accessing CPI in these following circumstances:

- (1) Working with the attorney general's office regarding collection and compromise matters;
- (2) Developing, implementing, or supporting agency computer systems;
- (3) Administering programs to discover delinquent or noncompliant taxpayers;
- (4) Internal audit functions and investigations;
- (5) Considering taxpayer appeals of assessments and other findings of the tax commissioner and drafting of final determinations from such appeals; and
- (6) Assisting other agencies in their tax administration and compliance efforts as allowed under Ohio law.