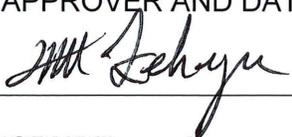


<p style="text-align: center;">STATE OF OHIO</p>  <p style="text-align: center;">DEPARTMENT OF NATURAL RESOURCES</p>	<p>SUBJECT: Information Owner Policy</p>	<p>PAGE <u>1</u> of <u>5</u> PAGES</p>
		<p>POLICY #DNR-OIT-0003</p>
	<p>RULE/CODE REFERENCE: ORC §1347.05 OAC §1501 et seq.</p>	<p>SUPERSEDES: N/A</p>
	<p>PURPOSE: The purpose of this policy is to guide Information Owners and ensure information is treated as an asset and protected in accordance to State of Ohio rules, federal requirements, and Department policies.</p>	<p>EFFECTIVE DATE: 12/01/2014</p> <p>REVISION DATE: N/A</p>
	<p>APPOINTING AUTHORITY: ORC §1501.01 ODNR Director</p>	<p>APPROVER AND DATE: </p>

This policy applies to all Ohio Department of Natural Resources (“ODNR”) employees, and in no way supersedes the negotiated language in the applicable collective bargaining agreements.

I. DEFINITIONS:

TERM	DEFINITION
Confidential Personal Information	Confidential Personal Information (CPI) for the purposes of this policy is personal information that the law prohibits the Department from releasing. Examples of personal information that may fall within the scope of CPI – depending on department-specific legal requirements – include Social Security Numbers, medical diagnoses, benefit-related information, certain information relating to children and income tax information in certain circumstances. (See also the definition of “confidential personal information” in ORC 1347.15(A)(1) and “public records” in ORC 149.43)
Information Owner	The Information Owner is the individual or group responsible for a personal information system.
Personally Identifiable Information	Personally Identifiable Information (PII) is information that can be used to directly or indirectly identify a particular individual.

II. POLICY:

An Information Owner is an individual who is directly responsible, as part of their job duties, for a personal information system containing CPI and shall be accountable for complying with the Department CPI policy and procedure.

1. Ensure CPI is accessed only for the following valid reasons:
 - 1.1. Responding to a public records request;
 - 1.1.1. Redaction may be necessary
 - 1.2. Responding to a request from an individual for the list of CPI the Department maintains on that individual;
 - 1.3. Administering a constitutional provision or duty;

- 1.4. Administering a statutory provision or duty;
 - 1.5. Administering an administrative rule provision or duty;
 - 1.6. Complying with any state or federal program requirements;
 - 1.7. Processing or payment of claims or otherwise administering a program with individual participants or beneficiaries;
 - 1.8. For auditing purposes;
 - 1.9. Licensure [or permit, eligibility, filing, etc.] processes;
 - 1.10. Investigations or law enforcement purposes;
 - 1.11. Administrative hearings;
 - 1.12. Litigation, complying with an order of the court, or subpoena;
 - 1.13. Human resource matters (hiring, promotion, demotion, discharge, salary/compensation issues, leave requests/issues, time card approvals/issues);
 - 1.14. Complying with an Executive Order or policy;
 - 1.15. Complying with a department 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
 - 1.16. Complying with a collective bargaining agreement provision.
2. Complete the CPI access log each time an access occurs
 - 2.1. Name of personal Information System
 - 2.2. Data Access (MMDDYYYY)
 - 2.3. Time Accessed (HH:MM)
 - 2.4. Name of Person Accessing
 - 2.5. Identification of the person whose CPI was accessed
 - 2.6. Reason for accessing the information from the list of valid reasons
3. Provide a list of CPI to individuals upon a written request
 - 3.1. Verify the individual has a signed written request
 - 3.2. Verify the identity by having the requester appear in person and present a valid driver's license, official state identification card or passport. In the event the requester cannot present one of those three photo IDs, the business unit may accept a similarly trustworthy form of verification. Use of an alternative form of verification shall be approved by a deputy director prior to releasing the confidential personal information.
 - 3.3. Provide the requester a list of the actual CPI maintained by the Department that:
 - 3.3.1. Does not relate to an investigation about the individual
 - 3.3.2. Is otherwise not excluded from the scope of Chapter 1347 of the Revised Code
 - 3.4. If all information relates to an investigation about that individual, the Department shall respond as follows: The Department has no CPI about the individual that is responsive to this request.
 - 3.5. Check with the Office of Human Services (HR) Chief and Chief Legal Counsel to determine if the individual is under investigation.
4. Notify individuals of a breach of their CPI
 - 4.1. Upon discovery or notification that confidential personal information has been accessed for an invalid reason, the Information Owner or Information Owner's

Supervisor shall open a ticket with the OIT Helpdesk and provide the following information:

- 4.1.1. You are reporting a CPI invalid access issue
 - 4.1.2. Your contact information
 - 4.2. The OIT Helpdesk shall notify the Chief Information Security Officer (CISO) who will fill out an incident report
 - 4.3. The Department shall notify the person whose information was breached as soon as practical and to the extent known at the time. Notification may be delayed for the following reasons:
 - 4.3.1. For a period of time necessary to ensure that the notification would not delay or impede an investigation or jeopardize homeland or national security.
 - 4.3.2. The Department may delay the notification consistent with any measures necessary to determine the scope of the invalid access, including which individuals' confidential personal information was breached, and to restore the reasonable integrity of the system.
 - 4.4. Notification provided by the Department shall inform the person of the type of confidential personal information accessed and the date of the invalid access.
 - 4.5. Notification may be made by any method reasonably designed to accurately inform the person of the invalid access, including written, electronic, or telephone notice.
 - 4.6. The Department Contact who notified the individual of the breach will update the OIT helpdesk ticket and inform the CISO of the method of communication, date and time notified.
5. Keep the CPI logs secure
 - 5.1. When you start logging access to CPI enter the date (MMDDYYYY) in the Log Beginning space.
 - 5.2. If the log becomes full
 - 5.2.1. enter the date (MMDDYYYY) in the Log Ending space when the log becomes full
 - 5.2.2. secure the form in a locked cabinet until the retention date is reached
 - 5.3. When the retention date is reached shred the log
 - 5.3.1. CPI logs are retained for 1 year

III. RESPONSIBILITIES:

POSITION OR OFFICE	RESPONSIBILITIES
Office of Human Resources	A. To process violations of the policy according to the disciplinary process and grid.
ODNR Data Privacy Point of Contact	A. Maintains Division specific policies, procedures, directives and Executive Orders, and ensures their periodic review and update, as necessary. B. Monitor workforce, ensure compliance, and report violations to Human Resources. C. Proactively communicate questions, concerns and issues to the appropriate contact listed below. D. Ensure employees have access to and successfully complete any necessary ELM training in a timely fashion.

Information Owner	A. Read and comply with policy. B. Proactively communicate questions, concerns and issues to the appropriate contact listed below. C. Complete all associated policy training in a timely fashion.
-------------------	--

IV. CONTACTS:

SUBJECT	OFFICE	TELEPHONE	EMAIL/URL
Policy Issues	Office of Human Resources/Labor Relations	(614) 265-6981	Policy.Coordinator@dnr.state.oh.us
Policy Compliance	ODNR Office of Information Technology	(614) 265-6854	ODNR Office of IT Technology

Related Department Forms:

- Access Log

