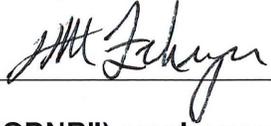


<p style="text-align: center;">STATE OF OHIO</p>  <p style="text-align: center;">DEPARTMENT OF NATURAL RESOURCES</p>	<p>SUBJECT: Confidential Personal Information Security</p>	<p>PAGE <u>1</u> of <u>7</u> PAGES</p>
		<p>POLICY #DNR-OIT-0006</p>
	<p>RULE/CODE REFERENCE: ORC §1347.15 ORC §5703.211 OAC §1501 et seq.</p>	<p>SUPERSEDES: Logging of Confidential Personal Information – 4/1/2010</p>
	<p>PURPOSE: The purpose of this policy is to provide guidance on handling Confidential Personal Information (CPI).</p>	<p>EFFECTIVE DATE: 12/01/2014</p>
	<p>APPOINTING AUTHORITY: ORC §1501.01 ODNR Director</p>	<p>REVISION DATE: 10/21/2014</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
Access	Access, for the purposes of this policy, means the retrieval of confidential personal information (CPI) from a personal information system by name or personal identifier so that CPI is viewed, or so that CPI is copied or retained outside of the personal information system.
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 “CPI” in ORC §1347.15(A)(1) and “public records” in ORC §149.43)
Information Owner	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.
Investigation	Investigation means the investigation of the circumstances and involvement of an Employee surrounding the invalid access of the CPI. Once the Department determines that notification would not delay or impede an investigation, the Department shall disclose the access to CPI made for an invalid reason to the person.

Personal Information System	<p>A personal information system is a system of record that contains <u>all</u> of the following attributes:</p> <ol style="list-style-type: none"> 1) It is a group or collection of records that are kept in an organized manner in either electronic or paper formats. (See the definition of “system” in ORC §1347.01(F)) 2) It contains “personal information” which is a person’s name or other identifier (such as SSN or driver’s license number) associated with any information that describes anything about a person or indicates that a person possesses certain personal characteristics. (See the definition of “personal information” in ORC §1347.01(E)) 3) Personal information is retrieved from the system by name or other identifier. (See the definition of “system” in ORC §1347.01(F)) 4) The Department has ownership of, control over, responsibility for, or accountability for that system of record. (See the definition of “maintains” in ORC §1347.01(D))
-----------------------------	---

II. POLICY:

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

1. Criteria for accessing CPI
 - 1.1. Personal information systems of the Department are managed on a “need-to-know” basis where by the information owner determines the level of access required for an Employee of the Agency to fulfill the Employee’s job duties.
 - 1.2. The determination of access to CPI shall be approved by the Employee’s supervisor and the information owner prior to providing the Employee with access to CPI within a personal information system.
2. Individual’s request for a list of CPI

Upon the signed written request of any individual for a list of CPI about the individual maintained by the Department, the Department shall do the following:

 - 2.1. Verify the identity of the individual by a method that provides safeguards commensurate with the risk associated with the CPI.
 - 2.2. Provide to the individual the list of CPI 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.
 - 2.3. If all information relates to an investigation about that individual, inform the individual that the Department has no CPI about the individual that is responsive to the individual’s request.
3. Notice of invalid access
 - 3.1. Upon discovery or notification that CPI 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. Notification may be delayed for the following reasons:

- 3.1.1. For a period of time necessary to ensure that the notification would not delay or impede an investigation or jeopardize homeland or national security.
 - 3.1.2. The Department may delay the notification consistent with any measures necessary to determine the scope of the invalid access, including which individuals' CPI invalidly was accessed, and to restore the reasonable integrity of the system.
 - 3.2. Notification provided by the Department shall inform the person of the type of CPI accessed and the date of the invalid access.
 - 3.3. Notification may be made by any method reasonably designed to accurately inform the person of the invalid access, including written, electronic, or telephone notice.
4. What is Not Covered
 - 4.1. In limited circumstances, routine information that is maintained for the purpose of internal office administration, the use of which would not adversely affect a person.
 - 4.1.1. This applies primarily to internal Human Resource records on employees as long as the information would not "adversely affect a person." This type of information is not considered part of a personal information "system" pursuant to ORC §1347.01(F).
 5. Content of Logs
 - 5.1. The record of access shall be maintained in a log. Each log shall contain the following information:

Information Recorded in Logs	Description
Name of the Personal Information System	Name of the personal information system from which a person's confidential personal information (CPI) is being viewed or otherwise retrieved by name or personal identifier.
Date	The date of the access. Note: The format should be standardized, such as DD-MM-YYYY or MM-DD-YYYY. "DD" means date; "MM" means month; and "YYYY" means year.
Time	The time of the access occurred (HH:MM for manual logs; HH:MM:SS for automated logs). Note: If the log is automated, it should capture U.S. Eastern Time as the default or Greenwich Mean Time with the offset. "HH" means hour; "MM" means minute; and "SS" means second.
Name of the State Official Accessing CPI	The name of the senior official accessing or attempting to access CPI in the personal information system. Note: A system username is sufficient as long as the username is associated only with a single user who is the director, assistant director or deputy director accessing CPI directly or indirectly.
Identification of the Person Whose CPI Was Accessed	The name or identifier of the person whose CPI was accessed. Note: When possible, do not record identifiers that are considered confidential such as Social Security Number, but record an identifier that is not confidential.

6. Managing the Logs

The ODNR Office of Information Technology (OIT) shall deploy technical or procedural security controls to support the enforcement of this policy. As a minimum, the Agency shall:

- 6.1. Provide employees covered by this policy with an electronic mechanism or paper form (see form attached) as the log for recording access
- 6.2. Establish a retention schedule for the logs created as a result of this policy
- 6.3. Establish a written procedure for storing and securing the logs

7. Awareness and Training

The Information Owner of systems identified with CPI shall be trained by the Data Privacy Point of Contact on the implementation of the logging policy and procedure.

8. Procedure

Granting Access to CPI		
	Task	Task Owner
1	Before granting access to CPI, determine the valid reason. Is there a valid reason for granting access? <ul style="list-style-type: none"> • No > Stop do not grant access • Yes > Proceed to next step 	Information Owner
2	Complete form: <ul style="list-style-type: none"> • Name of personal Information System • Data Access (MMDDYYYY) • Time Accessed (HH:MM) • Name of Person Accessing • Identification of the person whose CPI was accessed • Reason for accessing the information from the list of valid reasons 	Information Owner
Providing a list of CPI to individuals		
	Task	Task Owner
1	Do you have a signed written request from the requester? <ul style="list-style-type: none"> • No > Stop. Get a signed written request from the requester. • Yes > Proceed to next step 	Information Owner
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 sensitive or confidential personal information.	Information Owner, Deputy Director

3	<p>Provide the requester a list of the actual CPI maintained by the Department that:</p> <ul style="list-style-type: none"> • Does not relate to an investigation** about the individual • Is otherwise not excluded from the scope of Chapter 1347 of the Revised Code <p>Example: If the Agency maintains the requesters social security number (SSN) then provide the number.</p> <p>** If all information relates to an investigation about that individual, inform the individual that the Agency has no CPI about the individual that is responsive to the individual's request. Check with the Office of Human Resources (HR) Chief and Chief Legal Counsel to determine if the individual is under investigation.</p>	Information Owner, HR Chief, Chief Legal Counsel
Notice of Invalid Access		
	Task	Task Owner
1	<p>Upon discovery or notification that CPI of an individual was accessed by an Employee 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:</p> <ul style="list-style-type: none"> • You are reporting a CPI invalid access issue • Your contact information 	Information Owner, Information Owner Supervisor, Data Owner, OIT Helpdesk
2	The OIT Helpdesk shall notify the Chief Information Security Officer (CISO)	OIT Helpdesk, CISO
3	The CISO shall fill out a security incident report working with the person who reported the incident.	CISO and others
4	<p>The Department shall notify the person as soon as practical and to the extent known at the time. Notification may be delayed for the following reasons:</p> <ul style="list-style-type: none"> • For a period of time necessary to ensure that the notification would not delay or impede an investigation or jeopardize homeland or national security. • The Department may delay the notification consistent with any measures necessary to determine the scope of the invalid access, including which individuals' CPI that was breached, and to restore the reasonable integrity of the system. 	Information Owner, Information Owner's Supervisor, CISO
5	Notification provided by the Department shall inform the person of the type of CPI accessed and the date of the invalid access. Example: If the Agency maintains medical information and it was accessed for an invalid reason the Department would inform the individual their medical information was breached, but not the actual information.	Information Owner, Information Owner's Supervisor, Agency Contact

6	Notification may be made by any method reasonably designed to accurately inform the person of the invalid access, including written, electronic, or telephone notice.	Information Owner, Information Owner's Supervisor, Agency Contact
7	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.	Agency Contact
Access Log Security		
	Task	Task Owner
1	When you start logging access to CPI enter the date (MMDDYYYY) in the Log Beginning space.	Information Owner
2	If the log becomes full <ul style="list-style-type: none"> • enter the date (MMDDYYYY) in the Log Ending space when the log becomes full • secure the form in a locked cabinet until the retention date is reached 	Information Owner
3	When the retention date is reached, shred the document.	Information Owner
Access To CPI Systems Annual Verification		
	Task	Task Owner
1	Ask the Information Owner of each CPI system every January via email the following questions: <ul style="list-style-type: none"> • How are the files secured? • Who has access to the files? • Are the persons with access still approved by management to have that role? 	CISO
2	Maintain an electronic copy in text format of the email response.	CISO

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 OIT	(614) 265-6854	ODNR OIT

Related Department Forms:

- Incident Response Form
- Reasons for Granting Access
- Access Log

Initial Security Incident Report

1. NAME OF PERSON REPORTING INCIDENT (<i>Print First, Middle Initial, Last</i>)		2. DATE (MMDDYYYY)	
3. TYPE OF INCIDENT		4. WAS CONFIDENTIAL INFORMATION BREACHED? Yes ___ No ___	
5. WHO WAS INVOLVED IN THIS INCIDENT? Name (<i>Print First, Middle Initial, Last</i>) Work Phone Work Email Address			
6. WHEN DID THE INCIDENT OCCUR?			
Date (MMDDYYYY)			
Time (HH:MM)			
7. WHERE DID THE INCIDENT OCCUR? (Be specific: home, parking garage, etc)			
8. HOW DID THE INCIDENT OCCUR? (Be specific: lost, stolen, virus, social engineering, etc.)			
9. IF THIS INCIDENT INVOLVES STOLEN or LOST STATE OWNED EQUIPMENT OR PERSONALLY OWNED EQUIPMENT WITH STATE DATA ON IT THEN NOTIFY THE CHIEF OF OES (614-644-2100) AND CHIEF LEGAL COUNSEL (614-644-2782) AND PROVIDE THE FOLLOWING INFORMATION:			
State Inventory Tag Number			
Serial / PIN / Phone Number			
Model			
Cost			
10. WAS THE UNIT PASSWORD PROTECTED? Yes ___ No ___		11. WAS THE USER LOGIN OR PASSWORD INFORMATION VISIBLE WITH THE UNIT? Yes ___ No ___	
12. DATA OWNERS NAME (<i>Print First, Middle Initial, Last</i>)		13. DATA OWNER'S PHONE NUMBER	
14. IS THE INCIDENT ONGOING? Yes ___ No ___		15. WHAT IS THE RISK TO THE AGENCY? (<i>High, Moderate, Low</i>)	
16. INDICATE WHICH OF THE FOLLOWING OFFICES WERE NOTIFED OF THIS INCIDENT:			
Law enforcement (State Patrol – 614-752-0234, after hours – 877-772-8765, local police department)		ODNR Chief Legal Counsel – 614-	
OIT Help Desk – 614-265-7082		ODNR Law Enforcement	
ODNR EOC – 614-799-9572		ODNR HR Director	
Chief Information Officer – 614-265-6844		ODNR Deputy Director	
Chief Information Security Officer – 614-265-6854			
State of Ohio Office of Information Technology (CSC)– 614-644-6860 (csc@ohio.gov)			
Ohio Chief Information Security Officer – 614-728-2037			
Ohio Chief Privacy Officer – 614-752-7204			
17. DESCRIBE WHAT HAS HAPPENED AND NEXT STEPS			

LIST of Valid Reasons for Accessing CPI

- (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 or payment of claims or otherwise administering a program with individual participants or beneficiaries;
- (8) For auditing purposes;
- (9) Licensure [or permit, eligibility, filing, etc.] processes;
- (10) Investigations or law enforcement purposes;
- (11) Administrative hearings;
- (12) Litigation, complying with an order of the court, or subpoena;
- (13) Human resource matters (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 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
- (16) Complying with a collective bargaining agreement provision.

