Incident Response for Access of Confidential or Sensitive Personally Identifiable Information for an Invalid Reason Procedure
Effective Date: January 14, 2013

Purpose: This policy includes guidance and instructions that must be followed by the employees or contractors of the Ohio Casino Control Commission ("Commission") when Confidential Personal Information (CPI) or Sensitive Personally Identifiable Information (SPII) that is contained in a Commission-managed system is accessed for an invalid reason by a Commission employee, contractor or by any other person. This document sets forth the procedures for processing illegal activity and wrongdoing, and provides for the careful, expeditious handling of all allegations and paper-based CPI and SPII. The procedure covers both electronic and paper-based CPI and SPII.

Overview: R.C. 1347.15(B)(6) requires a state agency to have a procedure to notify each person whose CPI has been accessed for an invalid reason by employees of the state agency. Depending on the circumstances, state and federal laws require notification of affected individuals when there has been a security breach or invalid access for particular types of PII. However, it is not always clear whether a given incident is in fact a breach or other notification-triggering event. This procedure requires employees and contractors to report incidents so that the agency may make a determination of the steps that need to be taken.

Definitions

Personally identifiable information is information that can be used directly or in combination with other information to identify a particular individual. It includes:

1. A name, identifying number, symbol, or other identifier assigned to a person;
2. Any information that describes anything about a person;
3. Any information that indicates actions done by or to a person; and
4. Any information that indicates that a person possesses certain personal characteristics.

It includes "personal information" as defined by R.C. 1347.01. Some examples of personally identifiable information may be:

1. Names;
2. Social Security number;
3. Resumes;
4. Contracts;
5. Correspondence;
6. Addresses;

7. Phone numbers;
8. Driver's license numbers;
9. State identification numbers;
10. Professional license numbers;
11. Financial account information;
12. Medical and health information;
13. Physical characteristics and other biometric information;
14. Education information;
15. Tax information;
16. Individuals' job classifications and salary information;
17. Performance evaluations.

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

1. Social Security numbers;
2. A person's financial account numbers and information;
3. Beneficiary information;
4. Tax information;
5. Employee voluntary withholdings;
6. Passwords;
7. Employee home addresses and phone numbers;
8. Security challenge questions and answers;
9. Employees' non-state-issued email addresses;
10. Medical and health information;
11. Fingerprints and other biometric information;
12. Driver's license numbers;
13. State ID card numbers (as issued by the Ohio Bureau of Motor Vehicles); and,
14. Confidential personal information (see below).

Confidential personal information is personal information that falls within the scope of R.C. 1347.15 and that the Commission is prohibited from releasing under Ohio's public records law. It applies to Social Security numbers, fingerprint data, and medical and health information that are maintained by the Commission.

Illegal Activity as used in this procedure includes fraud, theft, assault, and other violations of local, state or federal law, including violations of state ethics laws, committed or in the process of being committed, by a state employee on any property owned or leased by the state or during the course of executing official duties.

Incident refers to facts and circumstances that lead to a reasonable belief that there has been an access of CPI or SPII for an invalid reason that affects one or more computer systems, networks, or other components of the Commission's technology infrastructure, or to the threat of such an event.

Invalid reason means any basis for access that is not directly related to the Commission's exercise of its powers or duties as described in the agency's CPI access policies. O.A.C. 3772-2-08 through 3772-2-12 identify valid reasons for accessing CPI within the Commission.

Wrongdoing as used in this procedure includes a serious act or omission, committed by a state employee on any property owned or leased by the state or during the course of executing official duties. Wrongdoing is conduct that is not in accordance with standards of proper governmental conduct and which tends to subvert the process of government, including, but not limited to, gross violations of departmental or agency policies and procedures, executive orders, acts of mismanagement, serious abuses of time, and other serious misconduct. For purposes of this reporting procedure, wrongdoing does not include illegal or suspected illegal activity. Likewise, wrongdoing does not include activity that is most appropriately handled through the Division of Operations.

Response to access of CPI or SPII for an invalid reason:

Responsibilities: Commission employees and contractors have the following responsibilities when making a report of access of CPI or SPII for an invalid reason:

- Employees and contractors shall report incidents of suspected access of CPI or SPII for an invalid reason to a manager. If an employee or contractor is unable to report the suspected incident to a manager, the report should be made to the Data Privacy Point of Contact (DPPOC), General Counsel or the Director of the division involved.
- Managers or the party that received the initial report shall notify the agency DPPOC of the suspected incident at (614) 387-5853.
- The DPPOC shall notify the Executive Director and General Counsel that a suspected incident has occurred and will be reviewed. The DPPOC will then coordinate a review of the suspected incident to determine if:
    1. A security breach as defined by R.C. 1347.12 has occurred, where "breach" is defined as unauthorized access to computerized data that compromises the security or confidentiality of personal information owned or licensed by a state agency or an agency of a political subdivision and that causes, is reasonably believed to have caused, or is reasonably

believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state.

2. A violation of R.C. 1347.15 has occurred, where CPI has been accessed for an invalid reason by a Commission employee.
3. A violation of another regulation, such as the Health Insurance Portability and Accountability Act (HIPAA), has occurred, or that there is some other risk or threat that makes notification of affected parties appropriate.

- The DPPOC will involve the following parties in this review:
  1. Commission human resources representative;
  2. Commission Director of the area involved;
  3. Commission Executive Director;
  4. Commission General Counsel; and
  5. Other parties as deemed appropriate.

If the review of the suspected incident determines that CPI or SPII has been inappropriately accessed, the General Counsel shall report the incident in the following manner:

- Notify the Governor's Office.
- Notify the Ohio State Highway Patrol.
- If there is clear danger and the agency General Counsel is not available, the DPPOC can also contact the Ohio State Highway Patrol.

The Commission is responsible for notifying all individuals affected by CPI or SPII upon a finding that notification is required or prudent.

Although employees are reminded of their duty to comply with the whistleblower statutes R.C. 124.341 and R.C. 4113.52, employees who report an access of CPI or SPII that they believe is for an invalid reason should have a reasonable factual basis for believing that improper activities have occurred. They should provide as much specific information as possible to allow for proper assessment of the nature, extent, and urgency of the incident.

Employees and contractors should avoid reporting a suspected incident of access to CPI or SPII for an invalid reason to those parties suspected of performing or ordering such access.

Requests for Incident Information:
If a Commission employee or contractor receives a request for incident information directly from the public, or from any other individual who is not associated with the incident resolution, the Commission employee or contractor will provide no information and will forward such request to the legal Division for review.

Training:
New employees must receive training on this standard operating procedure prior to accessing any Commission system that contains CPI.

Appointing Authority Approval — Date: 1/8/13

Policy Number: CCC-IT-06