OHIO CASINO CONTROL COMMISSION

Accessing Confidential Personal Information
CCC-IT-05
Effective Date: January 14, 2013
Amended Date: October 27, 2016

1.0 Purpose

The Ohio Casino Control Commission ("Commission") takes seriously the protection of personally identifiable information. This policy provides the requirements for protecting the privacy of people who have personally identifiable information in our databases, electronic and paper files and other records. This policy lays out basic handling expectations for all types of personally identifiable information and it provides important additional handling requirements for sensitive personally identifiable information.

2.0 Scope

This policy applies to all records kept by the Commission, whether in electronic or paper form or any other medium. This policy covers all Commission employees. It also covers contractors and agents of the Commission who gain access to the Commission's physical facilities, data, or computer systems. This policy lays out basic handling expectations for all types of personally identifiable information and it provides important additional handling requirements for sensitive personally identifiable information.

3.0 Authority

A. O.R.C. 3772.05

4.0 Definitions

As used in R.C. 1347.15 and in this policy, the following definitions apply:

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.

Additionally, R.C. 3772.16 defines confidential information as follows:

(A) Any information concerning the following submitted, collected, or gathered as part of an application to the commission for a license under this chapter is confidential and not subject to disclosure by any state agency or political subdivision as a record under section 149.43 of

the Revised Code:

(1) A minor child of an applicant;

(2) The social security number, passport number, or federal tax identification number of an applicant or the spouse of an applicant;

(3) The home address and telephone number of an applicant or the spouse or dependent of an applicant;

(4) An applicant's birth certificate;

(5) The driver's license number of an applicant or the applicant's spouse;

(6) The name or address of a previous spouse of the applicant;

(7) The date of birth of the applicant and the spouse of an applicant;

(8) The place of birth of the applicant and the spouse of an applicant;

(9) The personal financial information and records of an applicant or of an employee or the spouse or dependent of an applicant, including tax returns and information, and records of criminal proceedings;

10) Any information concerning a victim of domestic violence, sexual assault, or stalking;

(11) The electronic mail address of the spouse or family member of the applicant;

(12) Any trade secret, medical records, and patents or exclusive licenses;

(13) Security information, including risk prevention plans, detection and countermeasures, location of count rooms or other money storage areas,

emergency management plans, security and surveillance plans, equipment and usage protocols, and theft and fraud prevention plans and countermeasures;

(14) Information provided in a multijurisdictional personal history disclosure form, including the Ohio supplement, exhibits, attachments, and updates.

(B) Notwithstanding any other law, upon written request from a person, the commission shall provide the following information to the person except as provided in this chapter:

(1) The information provided under this chapter concerning a licensee or an applicant;

(2) The amount of the wagering tax and admission tax paid daily to the state by a licensed applicant or an operating agent; and

(3) A copy of a letter providing the reasons for the denial of an applicant's license or an operating agent's contract and a copy of a letter providing the reasons for the commission's refusal to allow an applicant to withdraw the applicant's application, but with confidential information redacted if that information is the reason for the denial or refusal to withdraw.

(C) The individual's name, the individual's place of employment, the individual's job title, and the individual's gaming experience that is provided for an individual who holds, held, or has applied for a license under this chapter is not confidential. The reason for denial or revocation of a license or for disciplinary action against the individual and information submitted by the individual for a felony waiver request is not confidential. The cover sheet completed by an applicant for a key employee license under section 3772.13 of the Revised Code is not confidential.

(D) An individual who holds, held, or has applied for a license under this chapter may waive the confidentiality requirements of division (A) of this section.

(E) Confidential information received by the commission from another jurisdiction relating to a person who holds, held, or has applied for a license under this chapter is confidential and not subject to disclosure as a public record under section 149.43 of the Revised Code. The commission may share the information referenced in this division with, or

disclose the information to, the inspector general, any appropriate prosecuting authority, any law enforcement agency, or any other appropriate governmental or licensing agency, if the agency that receives the information complies with the same requirements regarding confidentiality as those with which the commission must comply.

Personal refers to information about a natural person or individual as used in R.C 1347.12 (A)(2)(b)(5).

Records have the same meaning as set forth in R.C. 149.011.

System means any collection or group of related records that are kept in an organized manner and that are maintained by a state or local agency, and from which personal information is retrieved by the name of the person or by some identifying number, symbol, or other identifier assigned to the person. This includes both records that are manually stored (e.g., paper files) and records that are stored using electronic data processing equipment.

5.0 Policy

A. Rationale for Access to Confidential Personal Information

Commission employees are only permitted to access confidential personal information that is acquired by or in the possession of the Commission for valid business reasons. "Valid business reasons" are those reasons that reflect the employee's execution of the duties of the Commission as set forth in R.C. Chapter 3772 and in rules promulgated thereunder. Employees are also permitted to access their individual employment records, which contain confidential personal information, for time, hour and other payroll reasons.

B. Criteria for Access to Confidential Personal Information

R.C. 1347.15(B)(1) requires every state agency, including the Commission, to develop criteria for determining which of its employees may have access to confidential personal information, and which supervisors may authorize those employees to have such access. The Executive Director shall give final approval of all employees that have access to confidential personal information in the possession of the Commission. Employees of the Commission, including Commission members, shall maintain confidentiality regarding confidential personal information acquired while employed by the Commission, including, but not limited to, social security numbers of applicants/licensees, and information obtained in the course of an investigation.

i. For the Commission, the following criteria apply:

1. The Executive Director, Deputy Executive Director, all Division Directors, Commission members, and all employees of the Legal and Enforcement Divisions may have access to any and all confidential personal information in the possession of the Commission;
2. Employees of the Licensing & Investigation, Regulatory Compliance & Skilled Games Divisions and the office manager at each casino may have access to any and all confidential personal information contained in the e-License System, all paper files and any other system used that relates to persons applying for licensure or are licensed by the Commission;
3. Employees assisting with Problem Gambling issues may have access to confidential personal information regarding individuals registered for the Commission's Voluntary Exclusion Program;
4. Employees of the Operations Division may have access to all personnel records of the Commission and all financial records contained on paper or in OAKS.
5. The Commission's Assistant Attorney General or other staff assigned by the Attorney General may have access to any files

necessary to prepare for a hearing or provide the Commission with requested legal information and/or opinions.

6. Any hearing officer employed by the Commission may have access to any files necessary to prepare for a hearing or provide the Commission with requested reports and recommendations.
7. Any employee of the Commission or of DAS/OIT who maintains the responsibility of the Commission's computer systems and any electronic storage mediums may have access to any and all confidential personal information in the possession of the Commission.
8. The Executive Director may authorize others to have access to any files in order to fulfill the mission of the Commission.

C. Existing Computer Systems and Computer Upgrades

In the event that the Commission intends to upgrade its existing computer systems or purchase any new computer system that stores, manages, or contains confidential personal information, the new system and/or upgrades shall contain a mechanism for recording specific access by employees of the Commission to the confidential personal information.

Until an upgrade or new acquisition of such a computer system is made, employees accessing confidential personal information should keep a log that records access of the confidential personal information accessed in the computer system.

D. Requests for information from Individuals

The Commission may receive requests from individuals who want to know what confidential personal information is kept by this agency. However, Commission employees that receive such a request should consult with the Executive Director and General Counsel before any response is provided. Pursuant to R.C. 1347.08(E)(2), the Commission is not required to provide a person who is the subject of personal information in a personal information system, the person's legal guardian, or an attorney authorized by the person, with a right to inspect or have copied or to maintain a personal information system to permit the inspection of or to copy, a confidential law enforcement investigatory record or trial preparation record, as defined in divisions (A)(2) and (4) of section 149.43 of the Revised Code.

E. Notification of Access for Invalid Reasons

Even though appropriate safeguards are in place for protecting the confidentiality of personal information, it is possible that an employee of the Commission might gain access to such information for invalid reasons. Should an incident of invalid access occur, the Commission will advise the individual whose information was invalidly

accessed as soon as possible. However, if such notice would compromise the outcome of an investigation, notice may be provided upon completion of the investigation.

F. Data Privacy Point of Contact (DPPOC)

By law, the Commission must appoint a Data Privacy Point of Contact (DPPOC). That individual will work with the State's Chief Privacy Office to ensure that confidential personal information is properly protected and that the requirements of R.C. 1347.15 are satisfied. The DPPOC will be responsible for completing the privacy impact assessment form(s) for the Commission. The Director of Operations shall serve as the Commission's DPPOC.

G. Use of Authentication Measures

Every Commission employee is required to have a personal and secure password for their computer access. Commission employees are to keep passwords confidential and are prohibited from using their own passwords to log onto systems for non-employees or other persons.

H. Training and Publication of Policy

The Commission will develop a training program for all of its employees so that they are made aware of all the rules, laws and policies governing their access to confidential personal information. In addition, this policy will be distributed to each Commission employee. Employees will acknowledge receipt of the policy in writing. Amendments to this policy will be distributed and acknowledged in the same way.

I. Disciplinary Measures for Violations

No employee of the Commission shall knowingly access, use, or disclose confidential personal information for reasons that would violate this policy. Knowingly accessing, using, or disclosing confidential personal information in violation of this policy is a first degree misdemeanor, is cause for discipline, including immediate termination from employment.

J. Access to Confidential Personal Information Logs

For purposes of R.C. 1347.15(A), the logging requirements relating to computer system "specific access by employees" do not apply when non-public information is accessed as a result of a request by an individual about that individual; or access occurs as a result of research performed for official agency purposes, routine office procedures, or incidental contact with the information, unless the conduct resulting in the access is specifically directed toward a specifically named individual or a group of specifically named individuals. Any employee that accesses non-public information for a reason other than those explained herein shall sign a log to document the employee's access. (See attached logging form). Log forms will be reviewed quarterly by the

Commission's Executive Director and the DPPOC. Log forms will be maintained by the DPPOC in accordance with the Commission's records retention schedule.

K. Logging requirements

If manual logging is required, use the attached form to log the following: 1) name (or identifier) of the person whose CPI was accessed and 2) the date. This logging requirement applies whenever access is targeted to a specifically named individual or group of specifically named individuals and does not otherwise come within an exception.

Appointing Authority Approval:	Date:
Policy Number: CCC-IT-05	