County of Oconee,
State of Georgia.

COPY

RESOLUTION OF THE OCONEE COUNTY BOARD OF COMMISSIONERS TO ADOPT POLICIES IN CONNECTION WITH THE CRIMINAL HISTORY RECORD REQUIREMENTS OF THE ALCOHOL ORDINANCE LICENSE

WHEREAS, Oconee County has previously adopted an ordinance regulating the sale of alcoholic beverages in Oconee County, Georgia, known as the Alcoholic Beverages Ordinance and such Ordinance required fingerprinting and the use of the Georgia Crime Information Center (GCIC), Criminal Justice Information System (CJIS) Network/National Crime Information Center (NCIC); and

WHEREAS, model policies have been provided for such purposes; and

WHEREAS, Oconee County desires to adopt such policies for use in its administration of the Alcoholic Beverages Ordinance;

NOW THEREFORE, the Oconee County Board of Commissioners does hereby take the following actions:

1. The following policies are adopted:

A. The Criminal Justice Media Protection Policy attached hereto as Exhibit A and incorporated herein by reference;

B. The Criminal Justice Disciplinary/Personnel Sanction Policy attached hereto as Exhibit B and incorporated herein by reference; and

C. The Criminal Justice Manmade/Natural Disaster Policy attached hereto as Exhibit C and incorporated herein by reference.

Such policies shall apply to all Oconee County personnel including employees, nonpaid employees and vendors and contractors as set out in such policies

2. Each applicant who is the subject of a Georgia or Federal Bureau of Investigation national fingerprint/biometric-based criminal history record check as part of being issued a license under the Alcoholic Beverages Ordinance shall be provided a copy of the notice attached as Exhibit D and incorporated herein by reference. For the purposes set out therein, any applicant shall have a period of thirty days after written notice from Oconee County that the license under the Alcoholic Beverages Ordinance may be denied based on such criminal history record check in which to correct or complete the record, or decline to do so. Such written notice shall include a copy of such criminal history record.

So resolved this 7th day of March, 2017.

OCONEE COUNTY BOARD OF COMMISSIONERS

By: _____
John Daniell, Chairman

By: _____
Mark Thomas, Member

By: _____
Chuck Horton, Member

By: _____
W. E. Wilkes, Member

By: _____
Mark Saxon, Member

Attest: _____
Clerk, Oconee County Board of Commissioners

(County Seal)

EXHIBIT A

CRIMINAL JUSTICE
MEDIA PROTECTION POLICY

The Media Protection Policy shall be used for information derived from the Georgia Crime Information Center (GCIC) Criminal Justice Information System (CJIS) Network.

Purpose

The purpose of this policy is to ensure the protection of Criminal Justice Information (CJI)/Criminal History Record Information (CHRI). This policy applies to employees, non-paid employees, and vendors/contractors with access, to include physical and logical access, to any electronic or physical media containing CJI/CHRI while being stored, accessed or physically moved from a physically secure location. Transporting CJI outside the Agency's assigned physically secure area must be monitored and controlled.

Authorized personnel shall protect and control electronic and physical CJI/CHRI while at rest and in transit. The agency will take appropriate safeguards for protecting CJI/CHRI to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent and/or inappropriate disclosure must be reported to the Agency head and the Local Agency Security Officer (LASO). All employees, volunteers, and vendors/contractors are required to follow the policies, rules and procedures set forth by the GCIC, GCIC Council Rules, FIB CJIS Security Policy, and the laws of the State of Georgia.

Controls shall be in place to protect electronic and physical media containing CJI/CHRI while at rest, stored, or actively being accessed. "Electronic media" includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. "Physical media" includes printed documents and imagery that contain CJI/CHRI.

Media Storage and Access

To protect CJI/CHRI, personnel shall:

1. Securely store within a physically secure location or controlled area.
2. Restrict access to authorized individuals
3. Restrict the pickup, receipt, transfer and delivery to authorized individuals.
4. Ensure that only authorized users remove printed form or digital media from the CJI/CHRI.
5. Physically protect until media end of life.
6. Not use personally owned information system to access, process, store or transmit CJI/CHRI.
7. Not utilize publicly accessible computers to access, process, store or transmit CJI/CHRI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
8. Store all hard copy printouts maintained in a secure area accessible to only personnel whose job function require them to handle such documents.
9. Safeguard against possible misuse.

CRIMINAL JUSTICE
MEDIA PROTECTION POLICY

10. Take appropriate action when in possession, while not in a secure area.
    a. Must not leave the employee's immediate control. CJI printouts cannot be left unsupervised while physical controls are not in place.
    b. Precautions must be taken to obscure CJI from public view, such as by means of an opaque file folder or envelope for hard copy printouts. For electronic devices like laptops, use session lock use and/or privacy screens. CJI shall not be left in plain public view. When CJI is electronically transmitted outside the boundary of the physically secure location, the data shall be immediately protected using encryption.
        i. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected using encryption. Storage devices include external hard drives from computers, printers and copiers used with CJI. In addition, storage devices include thumb drives, backup tapes, mobile devices, laptops, etc.
        ii. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.
11. Lock or log off computer when not in immediate vicinity of work area.
12. Establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality.

Electronic Media Sanitization and Disposal

The agency shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel. Physical media shall be securely disposed of when no longer required, using formal procedures.

Incident Response

Personnel with access to CJI/CHRI are required to be familiar with their agency disciplinary policy. Agencies must report all GCIC violations in writing to the GCIC Deputy Director.

Penalties

Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, as outlined in the Disciplinary Policy.

EXHIBIT B

CRIMINAL JUSTICE
DISCIPLINARY/PERSONNEL SANCTIONS POLICY

Subject:
Georgia Crime Information Center (GCIC)/National Crime Information Center (NCIC) disciplinary/Personnel Sanctions Action for Violations.

Purpose:
The purpose of this policy is to establish guidelines for disciplinary action in regards to violations concerning the Georgia Crime Information Center (GCIC) Criminal Justice Information System (CJIS) Network/National Crime Information Center (NCIC) and information obtained thereof.

This policy applies to all agency employees, non-paid employees and vendors/contractors with access, to include physical and logical access, to GCIC/NCIC materials, records and information. This policy will establish guidelines for disciplinary action in regards to the usage of GCIC/NCIC and information obtained thereof. All personnel with access to Criminal Justice Information (CJI) or any system with stored GCIC/NCIC CJI have a duty to protect the system and related systems from physical and environmental damage and are responsible for correct use, operation, care and maintenance of the information. All technology equipment: computers, laptops, software, copiers, printers, terminals, MDTs, mobile devices, live scan devices, fingerprint scanners, software to include RMS/CAD, operating systems, etc., used to process, store, and/or transmit CJI is a privilege. To maintain the integrity and security of the systems and data, this computer use privilege requires adherence of relevant federal, state and local laws, regulations and contractual obligations. All existing laws and regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply to personal conduct.

Misuse of computing, networking or information resources may result in temporary or permanent restriction of computing privileges up to employment termination. In some misuse situations, account privileges will be suspended to prevent ongoing misuse while under investigation. Additionally, misuse can be prosecuted under applicable statutes. All files are subject for search. Where follow-up actions against a person or agency after an information security incident involves legal action (either civic or criminal), the evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s). Complaints alleging misuse computing and network resources and systems and/or data will be directed to those responsible for taking appropriate disciplinary action.

All employees are required to follow the policies, rules and procedures set forth by GCIC, NCIC, FBI CJIS Security Policy and the laws of the State of Georgia.

A. The following disciplinary action will be taken for general working errors that involve violations which are determined to be accidental errors or errors made due to the need of additional training. The severity of the error will be evaluated by the

Terminal Agency Coordinator (TAC). This is a general guideline and its use will be determined by the TAC, Administrative Head, and/or Agency Head.

1st Offense (for less severe errors): Verbal warning, additional training

1st Offense or 2nd Offense (determined by the severity of error): Written reprimand, additional training

3rd Offense: Written reprimand with possible suspension or termination, extensive additional training

4th Offense: Employment termination

B. For deliberate violations and/or misuse of GCIC/NCIC or information obtained thereof;

1st Offense: Immediate termination and possible criminal prosecution

EXHIBIT C

CRIMINAL JUSTICE
MAN-MADE/NATURAL DISASTER POLICY

Subject

Man-Made/Natural Disaster Policy for information derived from the Georgia Crime Information Center (GCIC) Criminal Justice Information System (CJIS) Network.

Purpose

The purpose of this policy is to establish guidelines in the event of a man-made or natural disaster to ensure that GCIC CJIS Network material, records and information obtained thereof are secure.

This policy applies to all agency employees, non-paid employees, and vendors/contractors with access, to include physical and logical access, to GCIC materials, records and information. This policy will establish guidelines for securing GCIC materials, records and information obtained thereof in the event of a man-made or natural disaster.

All employees, non-paid employees, and vendors/contractors are required to follow the policies, rules and procedures set forth by GCIC, GCIC Council Rules, CJIS Security Policy, and the laws of the State of Georgia.

In the event of a man-made or natural disaster, the agency head or designee and/or the local Agency Security Officer (LASO) shall have the responsibility of ensuring that GCIC materials and records maintained by the agency are not in danger of being damaged or destroyed. In the event that the materials or records are not secure, or have been damaged or destroyed, the affected agency personnel shall make immediate notification to the agency head or designee and/or LASO to inform of the situation. If necessary, personnel shall be stationed in the area to secure GCIC materials and records. Affected areas include: Records and administrative offices. The agency head, designee and/or LASO shall be responsible for taking necessary steps to ensure that all materials and records are secure on-site or that the materials and records are moved to another secure location.

EXHIBIT D

NON-CRIMINAL JUSTICE APPLICANT'S PRIVACY RIGHTS

As an applicant that is the subject of a Georgia only or a Georgia and Federal Bureau of Investigation (FBI) national fingerprint/biometric-based criminal history record check for a non-criminal justice purpose (such as an application for a job or license, immigration or naturalization, security clearance, or adoption), you have certain rights which are discussed below.

- You must be provided written notification that your fingerprints/biometrics will be used to check the criminal history records maintained by the Georgia Crime Information Center (GCIC) and the FBI, when a federal record check is so authorized.
- If your fingerprints/biometrics are used to conduct a FBI national criminal history check, you are provided a copy of the Privacy Act Statement that would normally appear on the FBI fingerprint card.
- If you have a criminal history record, the agency making a determination of your suitability for the job, license, or other benefit must provide you the opportunity to complete or challenge the accuracy of the information in the record.
- The agency must advise you of the procedures for changing, correcting, or updating your criminal history record as set forth in Title 28, Code of Federal Regulations (CFR), Section 16.34.
- If you have a Georgia or FBI criminal history record, you should be afforded a reasonable amount of time to correct or complete the record (or decline to do so) before the agency denies you the job, license or other benefit based on information in the criminal history record.
- In the event an adverse employment or licensing decision is made, you must be informed of all information pertinent to that decision to include the contents of the record and the effect the record had upon the decision. Failure to provide all such information to the person subject to the adverse decision shall be a misdemeanor [O.C.G.A. § 35-3-34(b) and §35-3-35(b)].

You have the right to expect the agency receiving the results of the criminal history record check will use it only for authorized purposes and will not retain or disseminate it in violation of state and/or federal statute, regulation or executive order, or rule, procedure or standard established by the National Crime Prevention and Privacy Compact Council.

If the employment/licensing agency policy permits, the agency may provide you with a copy of your Georgia or FBI criminal history record for review and possible challenge. If agency policy does not permit it to provide you a copy of the record, information regarding how to obtain a copy of your Georgia, FBI or other state criminal history may be obtained at the GBI website (http://gbi.georgia.gov/obtaining-criminal-history-record-information).

If you decide to challenge the accuracy or completeness of your Georgia or FBI criminal history record, you should send your challenge to the agency that contributed the questioned information. Alternatively, you may send your challenge directly to GCIC provided the disputed arrest occurred in Georgia. Instructions to dispute the accuracy of your criminal history can be obtained at the GBI website (http://gbi.georgia.gov/obtaining-criminal-history-record-information).

EXHIBIT D

PRIVACY ACT STATEMENT

Authority: The FBI's acquisition, preservation, and exchange of fingerprints and associated information is generally authorized under 28 U.S.C. 534. Depending on the nature of your application, supplemental authorities include Federal statutes, State statutes pursuant to Pub. L. 92-544, Presidential Executive Orders, and federal regulations. Providing your fingerprints and associated information is voluntary; however, failure to do so may affect completion or approval of your application.

Principal Purpose: Certain determinations, such as employment, licensing, and security clearances, may be predicated on fingerprint-based background checks. Your fingerprints and associated information/biometrics may be provided to the employing, investigating, or otherwise responsible agency, and/or the FBI for the purpose of comparing your fingerprints to other fingerprints in the FBI's Next Generation Identification (NGI) system or its successor systems (including civil, criminal, and latent fingerprint repositories) or other available records of the employing, investigating, or otherwise responsible agency. The FBI may retain your fingerprints and associated information/biometrics in NGI after the completion of this application and, while retained, your fingerprints may continue to be compared against other fingerprints submitted to or retained by NGI.

Routine Uses: During the processing of this application and for as long thereafter as your fingerprints and associated information/biometrics are retained in NGI, your information may be disclosed pursuant to your consent, and may be disclosed without your consent as permitted by the Privacy Act of 1974 and all applicable Routine Uses as may be published at any time in the Federal Register, including the Routine Uses for the NGI system and the FBI's Blanket Routine Uses. Routine uses include, but are not limited to, disclosures to: employing, governmental or authorized non-governmental agencies responsible for employment, contracting, licensing, security clearances, and other suitability determinations; local, state, tribal, or federal law enforcement agencies; criminal justice agencies; and agencies responsible for national security or public safety.

EXHIBIT D

28 CFR 16.30 through 16.34

§ 16.30 Purpose and Scope
This subpart contains the regulations of the Federal Bureau of Investigation (FBI) concerning procedures to be followed when the subject of an identification record requests production of that record to review it or to obtain a change, correction, or updating of that record.

§ 16.31 — Definition of identification record

An FBI identification record, often referred to as a "rap sheet," is a listing of certain information taken from fingerprint submissions retained by the FBI in connection with arrests and, in some instances, includes information taken from fingerprints submitted in connection with federal employment, naturalization, or military service. The identification record includes the name of the agency or institution that submitted the fingerprints to the FBI. If the fingerprints concern a criminal offense, the identification record includes the date of arrest or the date the individual was received by the agency submitting the fingerprints, the arrest charge, and the disposition of the arrest if known to the FBI. All arrest data included in an identification record are obtained from fingerprint submissions, disposition reports, and other reports submitted by agencies having criminal justice responsibilities. Therefore, the FBI Criminal Justice Information Services Division is not the source of the arrest data reflected on an identification record.

§ 16.32 — Procedure to obtain an identification record

The subject of an identification record may obtain a copy thereof by submitting a written request via the U.S. mails directly to the FBI, Criminal Justice Information Services (CJIS) Division, ATTN: SCU, Mod. D-2, 1000 Custer Hollow Road, Clarksburg, WV 26306. Such request must be accompanied by satisfactory proof of identity, which shall consist of name, date and place of birth and a set of rolled-inked fingerprint impressions placed upon fingerprint cards or forms commonly utilized for applicant or law enforcement purposes by law enforcement agencies.

§ 16.33 — Fee for production of identification record

Each written request for production of an identification record must be accompanied by a fee of $18 in the form of a certified check or money order, payable to the Treasury of the United States. This fee is established pursuant to the provisions of 31 U.S.C. 9701 and is based upon the clerical time beyond the first quarter hour to be spent in searching for, identifying, and reproducing each identification record requested as specified in § 16.10. Any request for waiver of the fee shall accompany the original request for the identification record and shall include a claim and proof of indigency. Subject to applicable laws, regulations, and directions of the Attorney General of the United States, the Director of the FBI may from time to time determine and establish a revised fee amount to be assessed under this authority. Notice relating to revised fee amounts shall be published in the *Federal Register*.

§ 16.34 — Procedure to obtain change, correction or updating of identification records

If, after reviewing his/her identification record, the subject thereof believes that it is incorrect or incomplete in any respect and wishes changes, corrections or updating of the alleged deficiency, he/she should make application directly to the agency which contributed the questioned information. The subject of a record may also direct his/her challenge as to the accuracy or completeness of any entry on his/her record to the FBI, Criminal Justice Information Services (CJIS) Division, ATTN: SCU, Mod. D-2, 1000 Custer Hollow Road, Clarksburg, WV 26306. The FBI will then forward the challenge to the agency which submitted the data requesting that agency to verify or correct the challenged entry. Upon the receipt of an official communication directly from the agency which contributed the original information, the FBI CJIS Division will make any changes necessary in accordance with the information supplied by that agency.