TENNESSEE HIGHER EDUCATION COMMISSION

**Agenda Item:** II.B.

**DATE:** January 26, 2017

**SUBJECT:** New Commission Policy- PII

**ACTION RECOMMENDED:** Approval

---

**BACKGROUND INFORMATION:** In recognition of one of THEC's primary responsibilities, the protection of student data, Mr. Krause formed a task force in the fall of 2016 to evaluate the agency's procedures related to the handling of personally identifiable information ("PII"). The task force developed recommendations for modifying some agency processes and procedures which were incorporated into an overall policy designed with three key purposes:

(1) To ensure compliance with all State and Federal laws related to PII;

(2) To ensure safe handling of PII by agency staff; and

(3) To achieve and maintain a heightened awareness among agency staff related to the handling, storage, utilization, and dissemination of PII.

The proposed policy is attached for review, discussion, and action at the January 26, 2017 meeting. Once approved, the policy will be distributed to each THEC employee. This policy clearly states the expectations of each employee as they perform their official duties on behalf of the Commission.

**Section Title:** Legal and Regulatory Policies

**Policy Title:** Protection of Personally Identifiable Information

**Policy Number:** LR7.0

7.1.10A **Purpose.** This policy has three purposes:

(1) To ensure Commission compliance with all State and Federal laws related to the protection of personally identifiable information;
(2) To ensure all agency processes related to the handling of personally identifiable information employ measures appropriate for the security of personally identifiable information; and,
(3) To achieve and maintain a heightened awareness among agency staff related to the handling, storage, utilization, and dissemination of personally identifiable information.

7.1.20A **Definitions.**

*Confidential Information*. Data or information deemed highly private or personal, the disclosure of which could potentially lead to identity theft or other malfeasance if mishandled or inadvertently distributed. This includes data or information deemed confidential by law, FERPA, regulation, or Commission policy. Confidential information includes, but is not limited to, the following:

1) Social security numbers;
2) Credit card numbers;
3) Driver's license or other government-issued identification numbers;
4) Bank account information;
5) Protected health information; and,
6) Student education records, including grades, transcripts, or financial records.

*Disclosure*. An individual discloses information when he or she permits access to or the release, transfer, or other communication of confidential, personally identifiable, or sensitive information by any means, including oral, written, or electronic, to any party, including the party who provided or created the record.

*Personally Identifiable Information*. Data is personally identifiable if it includes confidential or sensitive information and enables identification of a specific person or makes personal information about them known.

*Sensitive Information*. Some information related to the Commission's business and academic activities, although not requiring the same level of legal protection or scrutiny as confidential information, is still classified by the Commission to be "sensitive information." Examples of these types of information may include, but are not limited to:

1) Birth dates;
2) Home addresses;
3) Emergency contact information;
4) Employee/Student ID numbers;
5) Employee disciplinary records;
6) Legal documents; and,
7) Financial records.

7.1.30A **Scope.** This policy applies to all Commission members and staff. It is designed to protect confidential, personally identifiable, and sensitive information about students, teachers, Commission employees, and other individuals and entities considered stakeholders or Commission partners in higher education in the state and applies regardless of how the information is stored or transmitted (e.g., paper, electronic, other media).

7.1.40A **Procedures.** Use and release of confidential, personally identifiable, and sensitive information shall be consistent with all applicable laws and regulations, as well as Commission policy.

7.1.40B Information deemed confidential or sensitive shall be collected, stored, transmitted, and disposed of using the guidelines below. All Commission staff are responsible for ensuring that confidential and sensitive information is:

1) Collected only as necessary in conjunction with the lawful performance of Commission duties;
2) Restricted in its distribution and accessibility as is consistent with Commission policy;
3) Properly secured by the use of such safeguards as secured file storage and rooms, encryption, and other technology tools; and,
4) Disposed of through secure means such as shredding, overwriting hard drives, or other means of physical destruction as appropriate.

7.1.40C Staff shall adhere to Commission policy concerning the receipt, processing, and dissemination of personally identifiable

information. Staff shall follow the Information Security Protocol outlined by the Commission Information Systems Director and Personally Identifiable Information Coordinator ("PII Coordinator") when printing, faxing, storing, emailing, mailing, or handling any personally identifiable information.

7.1.40D Confidential and sensitive information shall be disclosed externally to individuals or entities outside of the Commission only when such disclosure is:

1) Necessary to fulfill the duties and responsibilities of the Commission;
2) Consistent with Federal, State, and local laws and regulations;
3) Compliant with this policy and the agency Information Security Protocol;
4) Provided using adequate protections, including written confidentiality and data sharing agreements, where appropriate; and,
5) When applicable, provided upon written permission or request from the affected individual, such as a student request for the release of transcripts.

Each division shall maintain a log or database of any external discolsure of PII. Staff shall confer with the Office of General Counsel for guidance as to whether an external disclosure of confidential, personally identifiable, or sensitive information complies with these requirements.

7.1.40E Confidential, personally identifiable, and sensitive information shall be disseminated internally between divisions and staff only when necessary to fulfill the duties and responsibilities of the Commission. If shared internally, staff shall be informed of the confidential or sensitive nature of the information and the need to safeguard it. Staff shall confer with the Office of General Counsel when a question arises as to whether the internal disclosure of confidential, personally identifiable, or sensitive information complies with this policy.

7.1.40F When directed by statute or required to fulfill the duties of the Commission, staff may be required to report data that was once personally identifiable to the general population through research briefs and reports. Staff should adhere to national data reporting standards and ensure that no data presented in aggregate may be systematically reduced to personally identifiable form. Staff shall adhere to the appropriate procedures for de-identification and reporting outlined in the agency Information Security Protocol.

Questions regarding the protection of data should be referred to the appropriate Commission division head and to the Office of General Counsel.

7.1.40G Commission staff shall not save confidential, personally identifiable, or sensitive information to their local desktop or laptop hard drive, except when necessary for temporary data processing or analysis and only after consultation with the PII Coordinator. If confidential, personally identifiable, or sensitive information must be saved to a user's desktop or laptop, the information should remain saved only for the period of time absolutely necessary for completion of processing and analyses and shall be immediately and permanently deleted thereafter.

7.1.40H Commission staff shall ensure that laptops, desktops, mobile devices or other machines provided by the State are password-locked and fully secured when not in use or under the immediate possession or control by the responsible individual. Staff shall not leave machines with access to personally identifiable information unattended. If a breach is suspected or a machine reported as missing or stolen, staff shall immediately inform the Executive Director, Information Systems Director, General Counsel, and the PII Coordinator, as well as their immediate supervisor.

7.1.40I The Commission shall establish and annually update a Data Breach Countermeasure Protocol and Crisis Plan to outline responsible parties, actions, and notification procedures in the event that personally identifiable, confidential, or sensitive information is disseminated or inadvertently distributed in an inappropriate or unintended manner. This protocol shall be reviewed annually by the PII Coordinator, in conjunction with the Executive Director, Office of General Counsel, Information Systems Director, and division leadership.

7.1.50A **Responsible Offices.** Commission leadership shall designate a Commission Information Systems Director to monitor handling of sensitive and confidential information, as well as develop tools, services, and guidance related to the security of the Commission's information technology assets. Questions related to these services, as well as questions related to the theft or potential theft of confidential, personally identifiable, or sensitive information, should be directed to this individual. The Information Systems Director shall ensure that all employees remain compliant with State and Commission procedures regarding information security, including the maintenance of employee acceptable use policies, information systems onboarding procedures, employee account

termination, and yearly user access audits. The Information Systems Director is responsible for developing and maintaining the Information Security Protocol for the Commission and initiating an annual review of the data breach countermeasure protocol and crisis plan.

7.1.50B The Executive Director shall designate a PII Coordinator who shall work with the Information Systems Director, the General Counsel, and each division head to maintain the Information Security Protocol for the Commission and conduct the following procedures annually:

1) Audit Commission staff rights and access privileges;
2) Update the Personal/Confidential Data Questionnaire;
3) Maintain on- and off-boarding procedures for employees regarding the protection of personally identifiable information; and,
4) Develop and implement ongoing employee trainings on the protection of personally identifiable information and acceptable handling of personally identifiable information.

7.1.50C The Office of General Counsel shall provide legal guidance for all questions related to the treatment of confidential, personally identifiable, or sensitive information and shall be consulted as needed for direction and advice.

**References:**

Tenn. Code Ann. § 10-7-504(a)(4)(A) – confidentiality of student records
Tenn. Code Ann. § 10-7-504(a)(29)(A) – disclosure of personally identifying information
Tenn. Code Ann. § 10-7-504(b) – destruction of records containing confidential information
Tenn. Code Ann. § 10-7-504(f) – confidentiality of certain state employee information
Tenn. Code Ann. § 10-7-504(m) – records related to the security of any government building
20 USCA § 1232g – Family Educational Rights and Privacy Act

Approved: January 26, 2017