February 2018, Spring Semester
Issue 2, Vol. 1

COMPLIANCE IN BLUE

The Institutional Compliance and Risk Management Newsletter of Middle Tennessee State University

Inside this Issue:

New Compliance Calendar Database

A new compliance calendar database ("CCD") has been developed that lists the annual, monthly, and quarterly regulatory compliance reports for MTSU Divisions. The CCD provides a one-stop location to view the dates of upcoming reports to local, state, and federal agencies, as well as other financial and academic program reports that are sent to MTSU's accrediting agencies.

The CCD will be distributed twice per year to the Division Vice Presidents (during the Spring and Fall semesters) to review the list of reporting dates and...

continued on page 2

Compliance Quote of the Day:

"Doing the right thing doesn't automatically bring success, but compromising ethics almost always leads to failure."

General Data Protection Regulation (GDPR): MTSU's Compliance Preparations

On May 25, 2018, the European Union General Data Protection Regulation, also commonly known as 'GDPR,' becomes effective for organizations that collect, maintain, transfer, or sell personal identifiable information to EU citizens. GDPR is designed to protect the data privacy of EU citizens. The regulation applies to organizations with a physical presence or location within the EU, as well as organizations located outside of the EU (such as in the United States) who offer goods or services to EU citizens (such as academic or athletics programs), or who collect and monitor data from EU citizens.

How is the GDPR applicable to MTSU?

While the University does not have a physical campus location in any of the EU countries, MTSU provides academic, study-abroad, online, and athletics programs to its students and graduate...

continued on page 2

Policy Updates: Conflict of Interest (COI) and Free Speech on Campus

The following is a summary of the updates to Policy 12—Conflict of Interest, and information regarding Policy 102—Free Speech on Campus.

continued on page 4

I AM trueBLUE
Find out what it means: www.mtsu.edu/trueblue
MIDDLE TENNESSEE STATE UNIVERSITY

COMPLIANCE IN BLUE

New Compliance Calendar Database *continued from page 1*

regulatory agencies for accuracy. The CCD also provides a brief description of the report type and the reporting agency.

For additional information on the CCD or its content, contact the Office of Compliance and Enterprise Risk Management at carem@mtsu.edu. The CCD also can be viewed on the **CAREM website**.

GDPR: MTSU's Compliance Preparation *continued from page 1*

researchers. European Union citizens also may apply to jobs at MTSU, and the University currently employs some EU citizens.

What constitutes personal data under the GDPR?

Under the GDPR, personal data is ***any information*** that can be used to identify a natural person. This includes email addresses, biometric information (used Rec Center), genetic information, photos, computer IP addresses, and social media posts, to name a few. The personal data covered under GDPR also includes "sensitive personal data," which consists of data on an individual's race, ethnicity, religion, political views, and/or sexual orientation.

How is the personal data regulated under the GDPR different from the data protections under FERPA?

FERPA focuses on post-collected data at the time an application for admission is submitted. GDPR, however, covers the entire life-cycle of information that could be used to identity a person.

What does GDPR require for compliance purposes?

GDPR requires the following:

1. **Consent and Notice provisions**. Organizations must develop provisions to allow students, job applicants, researchers, and visitors to consent to the use of their data.
2. **Data Collection Information.** Organizations must provide information on how we use data; the retention period for the data; and where the data will be maintained.
3. **Breach Notification.** Notifications of a data breach under GDPR require a response and remediation plan within 72 hours of breach discovery.
4. **Right to Information.** Individuals have the right to request a copy of the data collected by an organization.
5. **Opt-Out/Right of Withdrawal.** GDPR requires individuals to have the "right to be forgotten," which allows the individual's data to be erased or withdrawn upon their request. The request to be forgotten can be denied, however, if it conflicts with: (a) laws and regulations of the United States, (b) a request by a government agency to maintain a legal hold on the records; and/or (c) the needs of a government investigatory agency, such as homeland security, or other similar agencies.

continued on page 4

I AM trueBLUE
Find out what it means: www.mtsu.edu/trueblue
MIDDLE TENNESSEE STATE UNIVERSITY

COMPLIANCE IN BLUE

It's That Time Again! Annual Risk Assessments

Risk assessments in 2018 will focus on the Divisions of Business and Finance, and Academic Affairs. The University also will prepare an institution-wide risk assessment report utilizing the State of Tennessee's risk assessment forms that aligns with the Government Accountability Office's "Green Book" on creating, maintaining, and assessing financial and operational internal controls.

Information regarding the risk assessment process for 2018, as well as instructions on the use of the new forms will be distributed to the two, aforementioned Divisions by MTSU's Records' Officer, Mrs. Carroll Lewis in early February.

For additional information regarding the risk assessment process, or the State of Tennessee's risk assessment forms, please contact **carem@mtsu.edu** or **gene.stephens@mtsu.edu**.

Compliance Information and ERM Trivia

Did you know?

1. The Albert Gore Research Center on campus can be utilized to store, original permanent records for historical purposes for your department or division. Contact the **University Archivist** for more information.
2. You can document electronic records and electronic files in the MTSU Records Retention Database by listing them under the State's corresponding RDA or SW number for the record type.
3. **Trivia Question:**

MTSU's internal controls and risk management activities are reviewed by which standing Committee of the Board of Trustees?

a. Finance & Personnel

b. Executive and Governance

c. Audit and Compliance

the correct answer to #3 above is "c" - Audit and Compliance.

I AM trueBLUE
Find out what it means: www.mtsu.edu/trueblue
MIDDLE TENNESSEE STATE UNIVERSITY

COMPLIANCE IN BLUE

COI and Free Speech *continued from page 1*

The **Conflict of Interest Policy** has an updated **Checklist** that can be found under the "Forms" section of the Policy, as well as on Office of Compliance and Risk Management **webpage.** The updated Checklist is designed for faculty who wish to utilize textbooks in their classes for which they have authored and for which they receive royalties. The revised Checklist requires the signature of the Department Chair and Dean, as well as additional documentation.

Policy 103—**Free Speech on Campus**, is a new policy that became effective January 1, 2018. The policy affirms the University's principles on freedom of speech and expression on campus in alignment with the First Amendment to the U.S. Constitution. The Policy also provides information regarding the exceptions to protected speech. Additional information can be found at the **Freedom of Speech** section of the CAREM webpage, along with a list of MTSU resources, which includes the University's **First Amendment Encyclopedia**.

GDPR *continued from page 2*

6. **Protection of Data related to Children.** GDPR requires parental consent for the use or collection of data concerning children under the age of 16 who are EU citizens.

What are the penalties, if any, for noncompliance?

Organizations can be fined two (2) percent of their global revenue for failure to maintain records or to conduct data impact assessments. For more serious infractions of non-compliance (such as not having a sufficient consent process or violating data privacy design concepts), organizations can be fined up to four (4) percent of their global revenue.

For additional information or questions regarding MTSU's GDPR compliance preparedness, please email the Data Protection Officer at **dpo@mtsu.edu**, or email **carem@mtsu.edu.**

Regulatory Minute: What's Going On?

- **The Tennessee Student Assistance Corporation** ("TSAC") will be on campus to conduct a review of MTSU's compliance with State financial aid program requirements. TSAC representatives will conduct the review from February 20 - 23, 2018. Director of Financial Aid, Stephen White, is coordinating MTSU's efforts and preparation for the TSAC visit.

- MTSU is compiling and documenting its original records (both paper and electronic) in the Records Retention Database by March 31, 2018 (the Database will be locked after March 31 and will reopen on July 1) in preparation for the submission of a Records Holding Report due by June 30, 2018 to the State's Records Management Division. For additional information, or for questions regarding the use of MTSU's Records Retention Database, contact the University Records Officer, Mrs. Carroll Lewis, at **recordsretention@mtsu.edu**.

Special thanks to Vice President for Business and Finance, Alan Thomas, and Division Administrative Assistant, Beth Todd, for their assistance and support.

Gené Stephens, JD, LLM — Assistant Vice President
Office of Compliance and Enterprise Risk Management
Cope Administration Building, Suite 119
Office: (615) 494-8812
Email: carem@mtsu.edu or gene.stephens@mtsu.edu
Department Webpage: CAREM

I AM trueBLUE
Find out what it means: www.mtsu.edu/trueblue
MIDDLE TENNESSEE STATE UNIVERSITY