MIDDLE TENNESSEE STATE UNIVERSITY
Office of Compliance and Enterprise Risk Management

Compliance Tip for the Month – December 2020

Data Access and Security

As we approach the remainder of the year, please continue to assist the University's efforts to maintain the security of PII data and student educational records by:

1. Reviewing your employee's access to institutional platforms if they have changed job titles, departments, or divisions, and/or have left the University.
2. Determining which University platforms your employees need access to related to their job functions.
3. Ensuring your staff utilize the required multi-factor authentication to access University accounts and platforms.
4. Ensuring staff have completed the annual, video FERPA training related to access to student educational records and reviewed Policy 500, Access to Educational Records.
5. Utilizing the University's Secure Send/Accellion software to send confidential information and/or PII.
6. Contacting abuse@mtsu.edu if you receive a suspicious email.
7. Locking office cabinets/drawers containing student educational information or other confidential University information including, but not limited to: financial records, confidential Board documents, investigation reports, and account information.

Additionally, please remember that student educational records should only be accessed if the employee has a need to know the information as part of their University job.

For additional information on data access and data security tips, please contact ITD.

For additional information on FERPA compliance, please contact the following offices:

- Office of University Counsel
- Office of Compliance and Enterprise Risk Management
- ITD Security

I AM trueBLUE
MIDDLE TENNESSEE STATE UNIVERSITY

CAERM
OFFICE OF COMPLIANCE & ERM