In accordance with the Gramm-Leach-Bliley Act, West Tennessee Business College is required to take measures to safeguard personally identifiable information (PII) and to provide notice about security breaches of protected information at the college to affected individuals. West Tennessee Business College is committed to protecting the confidentiality of all sensitive data that it maintains, including the PII of faculty, staff, and students. This document exists to inform interested parties of the college's commitment to protect PII and the general nature of the policies and procedures designed to meet that commitment.

Protection of PII in printed form

Access to PII is limited to staff members with a need-to-know. Department directors are responsible for the enforcement of this policy with regard to the information within his/her office. The President of the college will resolve any disagreements and make final decisions regarding who requires access to PII. All printed documents containing PII are closely guarded when in use and stored in secure locations. Any suspected security breach of PII in printed form should be reported directly to the college registrar.

Protection of PII in electronic form

The IT Department is responsible for establishing and maintaining a set of standards that preserve the confidentiality and availability of PII in electronic form. The specifics of internal IT Department procedures are not published to protect the integrity of those procedures. However, the commitment to protect PII in electronic form will be met by:

1. Continually assessing risks and defining appropriate protection strategies
    a. The IT Dept uses a layered security approach to protect against cyber-attacks on computers containing or used to access PII
    b. Servers used to store PII are password protected and kept up to date with the latest security patches
2. Ensuring that any 3rd party provider contracted to store PII is meeting security standards equal to or greater than those of the college.
3. Ensuring that staff members with access to PII in electronic form have a need-to-know and have received proper training on the handling of PII.
4. Being vigilant in monitoring the security of data systems containing PII and responding appropriately to any suspected security breach.
    a. Any suspected security breach of PII in electronic form should be reported directly to the IT Director.

These policies have been approved by the college's senior executives and are applicable to faculty, staff, and students.