Black River Technical College
Gramm-Leach-Bliley Act
Information Security Program

Purpose

The Gramm-Leach-Bliley Act (15 U.S. Code § 6801 et seq., hereinafter "GLBA") requires BRTC to ensure the security, integrity, and confidentiality of covered nonpublic personal information and data, which includes student financial aid records and information.

Policy

This Information Security Program ("Program") ensures that administrative, technical and physical safeguards are implemented by BRTC to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle covered data and information in compliance with the FTC's Safeguards Rule (16 C.F.R. Part 314) promulgated under the GLBA.

These safeguards are provided to:

- Ensure the security and confidentiality of covered data and information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of covered data and information that could result in substantial harm or inconvenience to any customer.

In compliance with GLBA and FTC final Safeguards Rule, BRTC shall:

- Appoint an Information Security Program Coordinator(s).
- Conduct risk assessments of likely security and privacy risks.
- Maintain a training program for all employees who have access to covered data and information.
- Oversee service providers and contracts.

Related Policies and Activities

BRTC has established policies and implemented various activities intended to ensure the protection and confidentiality of nonpublic personal information it has been provided. Policies and procedures listed below provide more detail on steps BRTC has taken to reasonably ensure customer information is safeguarded.

- FERPA Policy
- Data Privacy Policy

Information Security Program Coordinator(s)
BRTC's designated ISP Coordinator is the Vice President for Finance and Administration. The ISP Coordinator may select others to supervise certain elements of the ISP and may designate an employee to act in the place of the ISP Coordinator for the purposes of fulfilling the responsibilities set forth in the ISP. Questions regarding the ISP should be directed to the ISP Coordinator.

Risk Assessment

Each administrative unit is tasked with the identification and assessment of reasonably predictable risks, both internal and external, to the security and confidentiality of nonpublic personal information that could result in unsanctioned disclosure, misuse, modification, or disposal of such information. Additionally, each college/administrative unit is responsible for determining safeguards in place to regulate the risks identified.

In addition BRTC will conduct a yearly risk assessment survey sent by the ISP Coordinator that will identify potential risk associated with nonpublic personal information and financial data.

Employee Training

Once per year BRTC will conduct an employee training session either in person or via digital means in order to educate employees on the rules, policies, and procedures in place to safeguard nonpublic personal information.

Oversight of Providers and Contracts

The ISP Coordinator will work with the Attorney General's Office to ensure standard data protection provisions are included in any contracts with third-party service providers.

Changes to the Program

The ISP Coordinators will evaluate and adjust the ISP as necessary based on the results of the risk identified, assessments, and testing and monitoring activities, or when modifications are required due to significant changes in the college's operations or operating environment.

Effective Date
June 30th, 2020