Procedure: 3.5.1p3.
FTC Safeguards Rule Compliance

Revised:

Last Reviewed:

Adopted: July 16, 2024

I. PURPOSE:
The purpose of this procedure is to outline the requirements for compliance with section 314 of the Federal Trade Commission Safeguards rule as it applies to the college student information systems.

II. RELATED AUTHORITY:
15 U.S.C. § 6801 - Title 15 of the Gramm-Leach-Bliley Act
16 CFR 314 - Section 314 of the FTC Safeguards Rule

III. APPLICABILITY:
All work units and Technical Colleges associated with the Technical College System of Georgia.

IV. DEFINITIONS:
Banner: The student information system used by all TCSG colleges.

Admin Pages: The administrative user interface for Banner.

Data Owner(s): The college employee or employees responsible for approving access to Banner Admin Pages for individual college employees according to their job duties.

Banner Project Leader: The college employee who serves as the primary point of contact for student information systems operations at each college.

Security Class: A logical grouping of Banner Admin Pages user interface elements organized by job responsibilities used to enforce access control.

HECVAT: Higher Education Cloud Vendor Assessment Tool

SOC1: System & Organization Controls 1 security assessment

SOC2: System & Organization Controls 2 security assessment

V. ATTACHMENTS: N/A

VI. PROCEDURE:

1. Each college will review security access information for all employees with Banner Admin Pages user accounts bi-annually. This review will be led by the college Banner Project Leader and Banner Data Owners. The review will verify the following for each active Banner Admin Pages user account:
    - That the account owner is still employed by the college.
    - That the account owner is assigned to the correct Banner Security Classes matching their current job description.

2. For any service provider with access to personally identifiable information (PII) that is transmitted to or stored by the service provider, each college will:
    - Require that service provider contracts include a commitment to implement and maintain data safeguards for college data.
    - Annually assess the service provider contract and verify that the service provider has maintained and independent security assessment of their data security policies, procedures and infrastructure
    - Maintain a copy of the latest service provider contract along with the most recent independent security assessment (HECVAT, SOC1 or SOC2)

VII. RECORD RETENTION:

Evidence of Banner Admin Pages user account verification should be maintained for 18 months.

Service provider contracts and security assessments should be maintained for 12 months.