

**STATE OF FLORIDA AUDITOR GENERAL**

**Information Technology Operational Audit**

Report No. 2018-123  
March 2018

**FLORIDA GATEWAY COLLEGE**  
Ellucian Banner® Enterprise Resource  
Planning System



Sherrill F. Norman, CPA  
Auditor General

## Board of Trustees and President

During the period August 2017 through October 2017, Dr. Lawrence M. Barrett served as President of Florida Gateway College and the following individuals served as Members of the Board of Trustees:

	<u>County</u>
Suzanne M. Norris, Chair	Columbia
Lindsey Lander, Vice Chair	Gilchrist
Renae Allen	Union
Robert C. Brannan III	Baker
Kathryn L. McInnis	Dixie
Dr. Athena Randolph	Columbia
Dr. Miguel Tepedino	Columbia
Vacant <sup>a</sup>	Baker
Vacant <sup>a</sup>	Dixie

<sup>a</sup> Position vacant from August 2017 through October 2017.

The team leader was Sue Graham, CPA, CISA, and the audit was supervised by Heidi Burns, CPA, CISA.

Please address inquiries regarding this report to Heidi Burns, CPA, CISA, Audit Manager, by e-mail at [heidiburns@aud.state.fl.us](mailto:heidiburns@aud.state.fl.us) or by telephone at (850) 412-2926.

This report and other reports prepared by the Auditor General are available at:

[FLAuditor.gov](http://FLAuditor.gov)

Printed copies of our reports may be requested by contacting us at:

**State of Florida Auditor General**

**Claude Pepper Building, Suite G74 • 111 West Madison Street • Tallahassee, FL 32399-1450 • (850) 412-2722**

# FLORIDA GATEWAY COLLEGE

## Ellucian Banner® Enterprise Resource Planning System

### ***SUMMARY***

---

This operational audit of Florida Gateway College (College) focused on evaluating selected information technology (IT) controls primarily applicable to the Ellucian Banner® Enterprise Resource Planning (Banner® ERP) system for maintaining and processing student account information and on the College's compliance with the Standards for Safeguarding Customer Information<sup>1</sup> (Safeguards Rule). Our audit disclosed the following:

**Finding 1:** Some Banner® ERP access privileges to student receivables and student records were unnecessary for the users' assigned job responsibilities.

**Finding 2:** The College had not established procedures for, and did not perform, periodic reviews of Banner® ERP access privileges to student receivables and student records.

**Finding 3:** College controls over the collection of payments for services need improvement to promote an appropriate separation of duties.

**Finding 4:** The College had not developed a comprehensive information security program in compliance with the Safeguards Rule.

**Finding 5:** Certain College security controls related to the logging and monitoring of system activity need improvement.

### ***BACKGROUND***

---

Florida Gateway College (College) is under the general direction and control of the Florida Department of Education, Division of Florida Colleges, and is governed by State law and State Board of Education rules. A Board of Trustees (Board) governs and operates the College. The Board constitutes a corporation and is composed of nine members appointed by the Governor and confirmed by the Senate. The College President serves as the executive officer and the corporate secretary of the Board, and is responsible for the operation and administration of the College.

The College uses the Ellucian Banner® Enterprise Resource Planning (Banner® ERP) system for recording, processing, and reporting finance, human resources, and student-related transactions. As an institution of higher learning, the College is defined as a financial institution by the Federal Trade Commission and, therefore, is subject to the provisions of the Gramm-Leach-Bliley Act.

---

<sup>1</sup> Title 16, Section 314, Code of Federal Regulations.

## ***FINDINGS AND RECOMMENDATIONS***

---

### **Finding 1: Access Privileges**

Effective access controls include measures that restrict access privileges granted to employees to only those necessary for assigned responsibilities or functions. Appropriately restricting access privileges granted to employees helps protect the confidentiality, integrity, and availability of data and IT resources.

Our test of selected access privileges granted within Banner® ERP for student receivables and student records disclosed that some access privileges assigned to certain employees were unnecessary for the employees' assigned job duties. Specifically, we found that:

- One of the 5 College employees granted access privileges to update selected student receivable transactions, including student account balances, (e.g., tuition and fees charged), payments received on student accounts, and exemptions authorized for student accounts, did not need the ability to update student account balances and payments received to perform her assigned responsibilities. Subsequent to our audit inquiry, College management changed the employee's access privileges to inquiry only.
- The access privileges for 7 of the 105 employees granted access privileges to selected student record information, including demographics, admissions, and registration, were unnecessary for the employees' assigned responsibilities. Specifically, although not required to perform their assigned job duties, 3 employees had the ability to update student demographic information; 2 employees had the ability to update student course registration; 1 employee had the ability to create and update admissions applications; and 1 employee had the ability to update demographics, student course registration, and create and update admissions applications. Subsequent to our audit inquiry, College management removed the access or changed the access privileges granted to inquiry only, as appropriate.

Appropriately restricted access privileges help protect data and IT resources from unauthorized modification, loss, or destruction.

**Recommendation: We recommend that College management ensure that employee access privileges granted within Banner® ERP for student receivables and student records are necessary for the employees' assigned responsibilities.**

### **Finding 2: Periodic Review of Access Privileges**

Effective access controls include periodic reviews of employee access privileges granted to business data to help ensure that only authorized employees have access and that the access provided to each employee remains appropriate and necessary for the employee's assigned job duties.

Our audit procedures disclosed that as of October 2017, College management had not established procedures for, and had not performed since August 2015, periodic reviews of access privileges granted within Banner® ERP for student receivables. Although College management performed in January 2017 a review of access privileges granted within Banner® ERP related to student records, the review did not include employees outside the Registrar's Office. In response to our audit inquiry, College management indicated that a comprehensive review of all users' access privileges, including access to student receivables and student records, was initiated in December 2017 and will continue through the beginning of 2018.

Periodic reviews of user access privileges increase management's assurance that user access privileges continue to be authorized and appropriate and reduces the risk that unauthorized disclosure, modification, or destruction of College-maintained data may occur.

**Recommendation:** We recommend that College management establish procedures requiring periodic review of the access privileges granted within Banner® ERP for student receivables and student records to verify that the access privileges are appropriate.

### **Finding 3: Separation of Duties**

Effective separation of duties prevents an employee from controlling all critical steps of a process. Our audit disclosed that certain separation of duties controls related to collections of payments for services need improvement. We are not disclosing specific details of the issues to avoid the possibility of compromising the integrity of data and related IT resources. However, we have notified appropriate College management of the specific issues.

Without adequate separation of duties related to collections of payments for services, the risk is increased for erroneous or fraudulent transactions to occur.

**Recommendation:** We recommend that College management improve separation of duties controls over collections of payments for services to promote the safeguarding and proper reporting of College revenue.

### **Finding 4: Information Security Program**

Standards for Safeguarding Customer Information<sup>2</sup> (Safeguards Rule), issued by the Federal Trade Commission as required by the Gramm-Leach-Bliley Act, requires the development, implementation, and maintenance of a comprehensive information security program that includes reasonable measures to secure customer information (i.e., nonpublic personal information) and to regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

The College designated an Information Security Program Coordinator as required by the Safeguards Rule and informally identified risks and the control measures in place. However, College management had not developed a comprehensive information security program, including a risk assessment which documents assessed risks and needed mitigating controls, giving consideration to the classification of, storage for, and monitoring and handling of confidential and sensitive customer information.

A comprehensive information security program demonstrates College management's compliance with the Safeguards Rule and supports the College's obligation to protect the security, confidentiality, and integrity of customer information.

**Recommendation:** We recommend that College management develop a comprehensive information security program in compliance with the Safeguards Rule.

---

<sup>2</sup> Title 16, Section 314, Code of Federal Regulations.

## **Finding 5: Security Controls – Logging and Monitoring**

Security controls are intended to protect the confidentiality, integrity, and availability of College data and IT resources. Our audit disclosed that certain College security controls related to logging and monitoring need improvement. We are not disclosing the specific details of the issues in this report to avoid the possibility of compromising College data and IT resources. However, we have notified appropriate College management of the specific issues.

Without adequate security controls related to logging and monitoring, the confidentiality, integrity, and availability of College data and IT resources may be compromised, increasing the risk that College data and IT resources may be subject to improper disclosure, modification, and destruction.

**Recommendation:** We recommend that the College improve IT security controls related to logging and monitoring.

## **OBJECTIVES, SCOPE, AND METHODOLOGY**

The Auditor General conducts operational audits of educational entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit from August 2017 through October 2017 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This operational audit focused on evaluating selected IT controls primarily applicable to Banner® ERP for maintaining and processing student account information and on the College's compliance with the Safeguards Rule during the period August 2017 through October 2017. The overall objectives of the audit were:

- To evaluate the effectiveness of selected IT controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for the IT records systems and controls included within the scope of the audit, deficiencies in management's internal controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT systems and controls included within the scope of this audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an understanding of the IT systems and controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of College management and staff and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting this audit, we:

- Interviewed College staff and reviewed operational documentation to obtain an understanding of and evaluate:
  - The College's information security program addressing student records and information and designating a coordinator for the program.
  - The College's critical revenue transaction components (e.g., tuition, fees, meal plans, and cosmetology services) and the generating, processing, and posting of revenue in Banner® ERP.
- Examined and evaluated the appropriateness of user access privileges, as of August 9, 2017, granted within Banner® ERP for four selected receivable transactions.
- Examined and evaluated the appropriateness of user access privileges, as of August 9, 2017, granted within Banner® ERP for eight selected student records transactions.
- Evaluated user authentication controls related to accessing Banner® ERP student receivables and student records.
- Evaluated the effectiveness of logical access controls, including periodic reviews of access privileges assigned within Banner® ERP related to student receivables and student records.
- Evaluated the controls over collections of payments for cosmetology services.
- Evaluated the information security program over student records.
- Evaluated the controls for logging and monitoring student receivable and student record transactions in Banner® ERP.
- Evaluated the controls for logging and monitoring the actions of privileged database users in Banner® ERP.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.

- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading **MANAGEMENT'S RESPONSE**.

## ***AUTHORITY***

---

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.



Sherrill F. Norman, CPA

Auditor General

# MANAGEMENT'S RESPONSE

---



*From the Office of the President*

---

March 2, 2018

Ms. Sherrill F. Norman, CPA  
Auditor General of the State of Florida  
Claude Denson Pepper Building, Suite G74  
111 West Madison Street  
Tallahassee, FL 32399-1450

Dear Ms. Norman:

The following is the response to the preliminary and tentative findings of your IT audit of Florida Gateway College.

**Finding No. 1 Access Privileges**

**Recommendation:** College management should ensure that employee access privileges granted within Banner ERP for student receivables and student records are necessary for the employees' assigned responsibilities.

**Response:** The College agrees with the recommendation. The Executive Director of Technology has implemented a procedure for periodic review of user access to determine if the access is necessary for the employees' assigned responsibilities and will update access privileges as needed.

**Finding No. 2 Periodic Review of Access Privileges**

**Recommendation:** College management should establish procedures requiring periodic review of the access privileges granted within Banner ERP for student receivables and student records to verify that the access privileges are appropriate.

**Response:** The College agrees with the recommendation. The Executive Director of Technology has implemented a procedure for periodic review of user access to determine if the access is necessary for the employees' assigned responsibilities and will update access privileges as needed.

**Finding No. 3 Separation of Duties**

149 SE College Place  
Lake City, FL 32025-2007

www.fgc.edu  
(386) 752-1822

Ms. Sherrill F. Norman, CPA  
March 2, 2018  
Page 2

**Recommendation:** College management should improve separation of duties controls over collections of payments for services to promote the safeguarding and proper reporting of College revenue.

**Response:** The College agrees with the recommendation. The College is in the process of preparing a procedure that will detail separation of duties in the area noted.

**Finding No. 4 Information Security Program**

**Recommendation:** College management should develop a comprehensive information security program in compliance with the Safeguards Rule.

**Response:** The College agrees with the recommendation. The College is in the process of preparing a comprehensive information security program in compliance with the Safeguards Rule.


**Finding No. 5 Security Controls – Logging and Monitoring**

**Recommendation:** The College should improve IT security controls related to logging and monitoring.

**Response:** The College agrees with the recommendation and is developing procedures to improve IT security controls related to logging and monitoring.

Sincerely,

  
Lawrence Barrett, President

  
Michelle Holloway, Chief Financial Officer