Florida Gulf Coast University Board of Trustees
September 17, 2013

SUBJECT: Banner Student Database Access Audit

PROPOSED BOARD ACTION

Accept the Banner Student Database Access Audit Report provided on August 16, 2013 to President Wilson Bradshaw, Vice President for Administrative Services and Finance Steve Magiera, and Assistant Vice President of Business Technology Services Mary Banks.

BACKGROUND INFORMATION

This report presents the results of a limited scope audit of the Banner student database access. Banner is the Enterprise Resource Package (ERP) used by University personnel to gather and process data for students, faculty, and staff. The audit objectives were to determine whether the individuals with access to the Banner Student Database are currently employed by the University, and whether the type of access in the Banner Student Database is appropriate based on the employee’s position description. The third objective was to determine the adequacy of the process to ensure that roles and responsibilities in the Banner Student Database are current and appropriate.

The audit was part of the 2012 - 2013 internal audit work plan approved by the FGCU Board of Trustees at its September 18, 2012 meeting.

Upon acceptance of the report by the FGCU Board of Trustees, a copy of the report will be sent to the Board of Governors as required.

Supporting Documentation Included: Banner Student Database Access Audit Report issued August 16, 2013

Prepared by: Director of Internal Audit Carol Slade

Legal Review by: Vice President and General Counsel Vee Leonard (August 9, 2013)

Submitted by: President Wilson Bradshaw
INTEROFFICE MEMORANDUM

To:      Steve Magiera, Vice President for Administrative Services and Finance
         Mary Banks, Assistant Vice President, Business Technology Services

Cc:      Dr. Wilson Bradshaw, President
         Susan Evans, Vice President & Chief of Staff

From:    Deborah McEwan, CIA, Senior Auditor
         Carol Slade, CPA, CIA, Director, Internal Audit

Date:    August 16, 2013

Re:       Banner Student Database Access Audit (FINAL REPORT)

Please see the attached final report of the Banner Student Database Access Audit, which includes the management response. The report is dated July 31, 2013, which is the date Internal Audit received the management response from the Assistant Vice President, Business Technology Services.

On August 9, 2013, Vee Leonard, Vice President and General Counsel, completed a legal review of the audit report.

The audit was performed by Deborah McEwan, Senior Auditor and reviewed by Carol Slade, Director, Internal Audit.
Florida Gulf Coast University

Banner Student Database Access Audit

Internal Audit

Report Date: July 31, 2013
BANNER STUDENT DATABASE ACCESS AUDIT

EXECUTIVE SUMMARY

This Report represents a limited-scope audit of logical access to the Banner Student Database. Banner is the Enterprise Resource Package (ERP) used by University personnel to gather and process data for students, faculty, and staff. The Banner ERP is divided into several modules, i.e. Student, Finance, Human Resources, and others. Additional University software applications also interface with the Banner Database to provide consistent information for University operations. The Banner Student Database was the primary focus of this audit. Audits of the other modules may be conducted in subsequent years.

In our opinion, Management processes and controls related to the access of University employees to the Banner Student Database are adequate. Notwithstanding, as of the date of this Report, Management will continue to implement additional procedures pertaining to employee separations and transfers within the University as noted in the Observations and Recommendations beginning on Page 4 of this Report. An additional recommendation pertaining to network access terminations is also provided for Management consideration.

OBJECTIVES

A. Determine whether the individuals with access to the Banner Student Database are currently employed by the University.
B. Determine whether the type of access in the Banner Student Database is appropriate based on the employee’s position description.
C. Determine the adequacy of the process to ensure that roles and responsibilities in the Banner Student Database are current and appropriate.

This audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing, issued by the Institute of Internal Auditors. The audit procedures provided a reasonable basis for our opinion and the following reportable observations and recommendations.

SCOPE – End of field work was June 28, 2013

- Reviewed policies, procedures, guidance, and regulations related to access of Banner Student Database.
- Reviewed Banner Student Database access list as of April 8, 2013 and June 5, 2013.
- Reviewed a sample of job descriptions, roles, and responsibilities.
- Reviewed individuals with “general class,” access as of June 10, 2013. These individuals also had access to student data.
GENERAL INFORMATION

Student Banner Database

The Banner Student Database contains various elements of student data. Access is granted based on a “class” designation. A class designation is customized for the specified users within the class. Each class is comprised of various forms and queries that are unique to a particular job function and are accessible only to its assigned users. Some employees are assigned to multiple classes based on the needs of their positions.

Access Request

Access to the Banner Student Database must be approved by a Banner Data Custodian (Data Custodian). In general, Data Custodians are high–level employees (i.e. directors) who have significant responsibilities and authority for the data under their purview.

Currently, the Banner Student Database is managed by two Data Custodians who are located in the Registrar’s Office, and they process requests for access to the student data. Only specified individuals across the University are authorized to submit requests to the Data Custodians. These Authorized Account Requestors are typically directors, deans, and/or supervisors who have received delegated authority to request access for subordinate employees.

When a Data Custodian receives a written request for access to the student database, he or she reviews the request and if considered acceptable, an electronic work order is submitted to Business Technology Services (BTS), the department which ultimately provides the technical access to the database.

Banner Quarterly Maintenance (On Going Access Monitoring)

Quarterly, BTS sends an email to all Data Custodians with a listing of employees with database access and their respective class assignments. Database Custodians are asked to review the report and submit a work order if any changes to employee access are needed. Also, Database Custodians are required to respond if no changes are needed based on the most current quarterly report.

The Banner Quarterly Maintenance Report is a comprehensive list of all individuals with access to the Banner database. This report is lengthy and consists of approximately 180 pages in the most recent years. As the University continues to grow the number of employees along with their assigned Banner classes will result in the extension of this report.
OBSERVATIONS AND RECOMMENDATIONS

I. Terminated Employees With Banner Student Database Access

**Criteria:** All employees who separate from the University should have all systems access, including access to the Banner database terminated before departing the University.

**Condition:** An audit test was performed to determine if any employees who had previously separated from University employment still had access to the Banner Student Database. Based on a list of 366 individuals, 11 individuals as of June 5th, 2013 were still included as Banner Student Database users although they were no longer employed by the University. The individual with the longest separation was from December 3, 2011 and the most recent separation was from November 10, 2012. Ten of the 11 individuals were Other Personal Service (OPS) employees and the remaining individual was a former Support Personnel.

**Cause:** The Student Database Custodians do not always receive information pertaining to the departure of an employee or there may be a delay in receiving the information.

**Effect:** Former employees may still have potential access to the database after separating from the University. In the test sample, the actual risk was limited because these 11 former employees did not have current access to the University’s network. In order to gain access to the Banner Student Database these employees would need access to the network. Verification of network access for these 11 individuals revealed that their network accesses were already terminated.

**Recommendation**

Business Technology Services should ensure that any instance of network termination, including expired accounts that may be automatically terminated should generate a subsequent process that verifies that any corresponding accesses to the Banner database are also removed.

**Management Response**

*Provided by:* Charles Weaver, Director Helpdesk & Network Services

I agree with the finding and subsequent recommendation on removing Banner Access at the same time or shortly after Network Access has been removed.

We have modified our process for closing network accounts to include the steps to close Banner accounts.

Effective 7/29/13; the new process is in place.
II. Employee Transfers or New Positions

**Criteria:** Any employee who transfers positions within the University should only have access to any University system or database class that is aligned with the roles and responsibilities of the most current position.

**Condition:** Based on a population list of 357 individuals with access to the Banner Student Database as of April 8, 2013, a sample of 60 individuals or 17% of the population was tested. The purpose of the audit test was to determine if the employees’ accesses to the Banner Student Database were aligned with their current job descriptions. Based on the test results, 2 individuals had access to Banner classes that were not consistent with the nature of their current positions. Subsequently, these individuals had their unnecessary accesses removed.

Also, there were employees who had access to student data which was embedded in other “general class” designations. A list of 96 individuals with access to general classes as of June 10, 2013 was tested. Three of the 96 individuals had access to student data that might not have been necessary based on their current positions. The auditor consulted with the 3 individuals and their respective supervisors, and the access was revised based on their current positions.

**Cause:** University employees transfer from one position to another and their access to the Banner Student Database is not being reassessed and revised based on their new positions.

**Effect:** An employee retains access to student data that may be unnecessary for his or her current roles and responsibilities.

**Recommendation**

Best practices require an account user to possess only privileges which are essential to that person’s position. Also, removing access to student data which is no longer necessary limits the number of employees who can view student data.

a. When BTS initiates the Banner Quarterly Maintenance review process, BTS can remind Data Custodians that any known employees who have obtained new positions within the University may potentially need revisions to their access.

b. BTS could also request a customized report from Human Resources (HR) listing all employees who may have transferred or assumed new positions during the last three months. This report could be used to supplement the Quarterly Maintenance Report which BTS routinely disseminates to all Banner Data Custodians.

The HR report of transferred employees will allow the Data Custodians to initially focus on any appropriate revisions to the access for these employees who have recently changed positions.
Management Response

Provided by: Mary Banks, Assistant Vice President, Business Technology Services

I agree with the finding. Currently, the employee separation process is used to notify departments that an employee is leaving the university. The current process includes notification to Business Technology Services (BTS) who is responsible for removing network and Banner access. Currently, this is not used for employees who change positions. Human Resources will expand the notification process to BTS for separating employees to also address all employees transferring positions. Business Technology Services will then remove access for the employee changing positions. If network and/or Banner access is required for the employee’s new position the new department will need to follow current process to give employee access.

This new process will be in place by 9/30/2013.

III. Additional Matter for Management Consideration

Condition

During the test of employees separated from the University who retained student database access (Observation I), it was discovered that, in all 11 test exceptions, network access was already removed based on network termination procedures previously instituted by BTS. A review of network terminations was not within the scope of this audit. As noted above, the network access terminations limited the risk of former employees using their existing Banner access to the student database. However, in 4 of the 11 instances, network access termination was not completed until almost 60 days to 1 year + after an effective date of separation as listed by the Human Resources Department. All 4 individuals were former OPS employees.

Discussions with BTS and Human Resource employees and Data Custodians revealed the challenges related to timely cross-dissemination of information pertaining to employee separations, especially for OPS employees. Human Resource’s current Departmental Separation Clearance Form (Clearance Form) is required for all Faculty, Administrative & Professional, and Support Personnel, but OPS employees are not addressed. This Clearance Form is routinely used to ensure that separating employees are appropriately processed prior to leaving the University. The Clearance Form includes, but is not limited to, returning any University assets, satisfying outstanding liabilities, and terminating access to the network and any related University systems.
Recommendation

Best practices require an employee’s access to any University systems be terminated as soon as possible based on the employee’s date of separation. Current BTS procedures effectively provided a default method to ensure that access to the network for OPS employees is terminated based on inactivity or end of semester appointment dates. However, Management should consider implementing additional procedures for separating OPS employees to ensure a more timely termination from network access and University systems, such as the Banner ERP.

Management Response

Provided by: Mary Banks, Assistant Vice President, Business Technology Services

I agree with the recommendation. As reported, the main area of concern centers on our OPS employees. The University has in place an effective procedure for regular fulltime employees who terminate from the University. The Departmental Separation Clearance Form is routed to the Business Technology Services Department to notify them that separating employees need to have their access terminated. However, no such form currently exists for the OPS employees. Business Technology Services Department together with the Human Resources Department will create a Departmental Separation Clearance Form for OPS, thus eliminating the problem.

This new process will be in place by 9/30/2013.

Performed by: Deborah McEwan, Senior Auditor

Reviewed by: Carol Slade, Director of Internal Audit