AUDITOR GENERAL

WILLIAM O. MONROE, CPA

FLORIDA INTERNATIONAL UNIVERSITY

PEOPLESOFT FINANCIALS SYSTEM

Information Technology Audit

SUMMARY

Florida International University (University) utilized the PeopleSoft financials and student administration application suites as its enterprise resource planning (ERP) solution. The applications operated within an Internet-based environment supported by the Division of Information Technology. The University Technology Services (UTS) department provided a central computer facility for the University, including support for the campuswide network backbone, computer operations, and telephone service. Although UTS provided computing services, various individual colleges and departments also maintained their own networks and computing facilities and connected to the overall FIU network through UTS-maintained routers. UTS was responsible only for the network backbone and did not assume maintenance of any equipment outside of the core network.

Our audit focused on evaluating selected information technology (IT) controls applicable to the PeopleSoft financials system, as implemented and administered by the University, and selected internal controls related to the University's overall IT environment, for the period August 2005 through January 2006, and selected actions taken through May 2006.

As described below, we noted that improvements were needed in certain controls related to the University's IT functions and practices.

Finding No. 1: There was a need for improved University-level governance of the PeopleSoft financials system and the enterprise data contained therein.

Finding No. 2: Improvements were needed in certain security controls within the overall operations of the application and the supporting network environment at the University.

Finding No. 3: Deficiencies were noted in the University's procedures for restricting access to appropriate users.

Finding No. 4: Improvements were needed in the change management process.

Finding No. 5: Deficiencies were noted in the disaster recovery plan and process.

Finding No. 6: Environmental control improvements were needed at the University's Data Center.

BACKGROUND

During the 2000-01 fiscal year, the University began a multi-year project with the goal of implementing a new Web-based ERP system to replace the State's financial accounting system, the Florida Accounting Information Resource Subsystem (FLAIR). The University purchased software applications for student administration, financials, and human resources management systems, which the University named the PantherSoft project. The student administration system is comprised of four main modules: admissions, financial aid, student financials, and student records. These modules went live during the 2003-04 and 2004-05 fiscal years. The financials system went live on July 1, 2004, and includes modules such as the general ledger, purchasing, accounts payable, asset management, and travel and expenses. The University used consulting firms for the implementation of and training for the student administration and financials systems. University personnel indicated that the University decided to outsource the payroll function to Automatic Data Processing, Inc. (ADP) and plan to transition off the State system on January 1, 2007. Additionally, software applications were acquired for the portal (Web access) and enterprise reporting.

Finding No. 1: University Governance of IT

Enterprise information resources and systems are shared resources requiring security and management strategies to be coordinated across the enterprise. Security management responsibility is optimally established at the organizationwide level to deal with overall security issues in the organization. Management's ultimate objective under an enterprise governance model is to conduct day-to-day operations of the organization and to accomplish the organization's stated missions with security commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. Management, through enterprise governance of IT, can provide increased assurance that due diligence is exercised by all individuals involved in the management, use, design, development, maintenance, or operation of information systems.

The FIU IT Security Office (ITSO) is one of five departments in the Division of Information Technology under the leadership of the University's Vice President and Chief Information Officer (CIO). Its mission is to protect FIU IT resources through awareness, policy, infrastructure, and education.

With the advent of the ERP initiative, core business processes underwent significant change affecting all aspects of the management of university resources. Accordingly, enterprise information was directly accessible on-line to increased groups of people. Consequently, the importance of enterprise level management of IT was increased. Our audit disclosed the following:

- The University did not maintain written procedures for consistent network standards to be applied across the University. Specific details of this deficiency are not disclosed in this report to avoid the possibility of compromising University information. However, appropriate University personnel have been notified of the deficiency.
- Security policies, such as the FIU General IT Security Policy and the FIUnet Acceptable Use Policy, resided on FIU's Web site. However, reading, acceptance, and agreement to adhere to these policies were not mandatory for all IT resource users and, even if users read the policies, there was not always a mechanism for the users to acknowledge in writing their understanding and acceptance of the policies. The IT Security Office did indicate that one component of its IT Security Awareness On-line Training is reading and acknowledging the General IT Security Policy. While we did note that there was an optional mechanism on the General IT Security Policy Web page, wherein users could enter and submit their Panther ID and e-mail addresses acknowledging that they had read, understood, and agreed to adhere to the security policy; there was no similar mechanism on the FIUnet Acceptable Use Policy Web page. Further, certain security policies and procedures, including the Guidelines for Data Stewardship, UTS Network Operations Center Procedures for Security Issues, and procedures governing the physical security of critical network components housed outside of the University data center, existed only in draft form.
- The FIU General IT Security Policy did not apply to United Faculty of Florida (UFF) members. As of July 1, 2005, the General IT Security Policy was adopted by the FIU Board of Trustees and applied to all non-bargaining unit faculty, Police Benevolent Association (PBA) represented employees, and non-bargaining unit employees.
- The University did not maintain logon banners for users accessing network resources. The use of banners generally complements an entity's IT security, network, and acceptable use policies. Logon banners

may include notice of authorized monitoring of users' activities while they are using the system, and warnings of legal sanctions should evidence of illegal activities or violations of IT security policies occur.

- We noted a lack of formal training for Network Engineering, Telecommunications and Operations, and Enterprise Systems members of the University's Security Incident Response Team (SIRT). In addition, SIRT procedures had not been reviewed by the University to ensure that they continued to support the critical business processes and systems of the University and campus units and incorporated the requirements in Florida law[1] for notifying affected persons if their personal information is compromised.
- Improvements were needed in University policies and procedures for data backup. Specific details of this deficiency are not disclosed in this report to avoid the possibility of compromising University information. However, appropriate University personnel have been notified of the deficiency.
- The University did not have adequate written security policies and procedures in place for the periodic review of the PeopleSoft financials user access privilege lists, nor were the user lists periodically reviewed by supervisors for appropriateness. Subsequent to our audit inquiries, management indicated that it had established a review process that is handled between the PantherSoft security administrator and the user departments and that the University can create a formal procedure to document this action between the groups.
- The University's Disability Resource Center Americans with Disabilities Act (ADA) policy provides that, under the guidelines of the ADA, the University is required to make reasonable accommodations in providing services to students, staff, faculty, or visitors with disabilities. In recognition of accessibility provisions under Section 508 of the Rehabilitation Act of 1973, as amended[2] (Section 508), the University placed reliance on PeopleSoft's position of compliance with regard to its application software. However, the University's written change control procedures for the PeopleSoft applications did not include procedures to ensure that any changes or customizations to the application supported continued compliance with Section 508.

Enterprise security relegated to varying technical specialties within individual campus/departmental units may not achieve a sustainable capability for developing and implementing proactive measures to mitigate security problems or incidents. Without applying management and security procedures for enterprise IT resources and data at a University level of governance, the University may fail to identify and enact security controls necessary to adequately protect information systems that support the operations and assets of the organization and, thereby, accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, provide reliable financial reporting, and protect individuals.

Recommendation: A University-level governance model should be adopted to create a centralized authority for managing and securing enterprise data. Written procedures should be initiated to address those areas noted above with consistent enterprisewide application to support the confidentiality, availability, and integrity of information resources.

Finding No. 2:
Application Environment and Support Function

Security considerations for all components of a system environment, including application, operating system, network, and physical levels, contribute to the reliability and integrity of the applications and the data processed therein. Developing and maintaining procedures to ensure the proper use of the application, data management, and technological solutions put in place is enabled by a structured approach to the combination of general and application controls over IT operations.

We noted certain control deficiencies in the systems environment, including inadequate policies and procedures, related to system logging, wireless access, user workstation controls, user identification and

[1] Section 817.5681, Florida Statutes
[2] 29 U.S.C. Section 794d

authentication, technical management, operating system, and network controls. Specific details of these deficiencies are not disclosed in this report to avoid the possibility of compromising University information. However, appropriate University personnel have been notified of the deficiencies.

Without formal written policies and procedures outlining controls and measures necessary for the quality and consistency with which an entity's objectives are achieved, management's assurance that personnel have the appropriate guidance for performing directives in accordance with expectations or with consistent application is diminished.

Recommendation: University management should strengthen its controls surrounding its enterprise information resources and systems in the above-mentioned areas.

Finding No. 3: Access Authorization

Proper restriction of system access to authorized individuals permits user access to application software processing functions solely for purposes of performing assigned duties and precludes unauthorized persons from gaining access.

Our audit disclosed the following instances of inappropriate or unnecessary system access privileges:

- ➢ The University did not have adequate policies and procedures in place to ensure that access capabilities were timely revoked or modified, as necessary, for individuals who had terminated employment. Termination procedures are developed and responsibilities assigned to specific departments in an organization to ensure timely notification to the data security administration function of change in employee status and cancellation of access privileges to critical areas, specific data systems, and the installation as a whole. In tests of 82 employee terminations during the period of July 2004 through July 2005, and through other audit procedures, we identified 24 University employees that continued to have PantherSoft financials or network access ranging from 68 to 431 days beyond their dates of termination. In response to our audit inquiry, the University indicated that these personnel had been locked out of the system and all roles removed. Additionally, the University determined that the account of one terminated employee was used after the termination date, but was unable to determine what resources, if any, were accessed. In January 2006, subsequent to our audit inquiries, the University implemented new termination procedures for managing the account deletion process for UTS-supported systems. Further, University management indicated that UTS and Human Resources were working to develop Universitywide policies and a notification mechanism regarding termination procedures. Without adequate procedures to ensure the timely revocation of access, the risk is increased of unauthorized access to University resources.

- ➢ Our audit disclosed instances of inappropriate or unnecessary access privileges. An appropriate division of roles and responsibilities excludes the possibility of a single individual subverting a critical process. When enforced through appropriate system access privileges, such a division helps ensure that personnel are performing only those duties stipulated for their respective jobs and positions. During our testing of access privileges for an appropriate segregation of duties, we noted the following:

  - Five of 27 instances tested in which employees appeared to have inappropriate access privileges to PeopleSoft financials security roles. In response to our audit inquiry, the University indicated that the access privileges in these five instances had been removed.

  - Twenty of 27 instances tested in which employees appeared to have inappropriate access privileges to five PeopleSoft financials Superuser roles that allowed, among other things, the user to manage or update transactional data. In response to our audit inquiry, the University indicated that it had removed the access privileges in some of these instances. It further indicated that it is monitoring the use of the roles and is working closely with the Controller's Office to fully transition the access privileges away from the Administrative Software Unit (ASU) of UTS to the Controller's Office and Purchasing Department.

- Four of 14 instances tested where user access privileges to certain panels within the PeopleSoft financials was inappropriate. In response to our audit inquiry, the University indicated that it will remove the access privileges in these instances.
- Twenty-three of 279 instances tested in which employees appeared to have inappropriate PeopleSoft financials financial-related roles. In response to our audit inquiry, the University indicated that the access privileges had been removed for three of the instances and adjusted accordingly for the remaining instances.

Absent appropriate segregation of duties, the risk is increased that erroneous or fraudulent transactions could be processed.

- Good controls over security administration include specific policies and procedures on the use and assignment of the correct history action type. In the PeopleSoft application, correction mode access allows the alteration, insertion, or deletion of data regardless of the data's effective date and without logging the action. Consequently, as data integrity and management reporting from the system may be adversely affected, correction mode access is best granted under limited and monitored circumstances. The University had not formally defined circumstances or designated personnel appropriate for correction mode usage. The extension of correction mode access to multiple users without clearly defined circumstances and responsibility severely diminishes the University's ability to detect, identify, and subsequently investigate inappropriate changes.

Subsequent to our field work, management indicated that it consulted with PeopleSoft support and had limited its use of the correction mode to those users that specifically needed it to perform their job functions. It further indicated that detailed procedures had been developed and communicated to the users.

Recommendation: In order to preserve the integrity, confidentiality, and availability of its information resources, the University should strengthen access authorization controls in the above-cited areas. Specifically, users' roles should be reviewed to ensure that they are reflective of the job duties of the individual to whom they are assigned and correction mode access should be granted on a limited basis according to defined circumstances and responsibilities. Further, the University should develop detailed procedures necessary to ensure that all terminated or transferred employees' access rights are timely revoked.

Finding No. 4:
Change Management Process

Establishing controls over the modification of application software helps to ensure that only authorized programs and authorized modifications are implemented. This is accomplished by instituting policies, procedures, and techniques that help ensure that all programs and program modifications are properly authorized, tested, and approved and that access to and distribution of programs is carefully controlled. Additionally, a proper segregation of duties regarding software change management includes a separation between who performs program changes, user acceptance testing, and the movement of programs into the production environment.

During our audit we noted the following deficiencies:

- Although the University had a written Technical Standards and Procedures manual that included procedures for the modification/change management process, staff did not always follow the procedures. Although procedures stated that the starting point for any application changes made to the PeopleSoft system required the use of a Business Process Reengineering Session Form, requests were communicated and authorized through informal verbal discussions or via e-mail with ASU staff.
- The Technical Standards and Procedures manual further stated that a Manual Data Change (MDC) request form should be used to document the request and approval of manual data changes. According to the

Financials Application Manager, requests for manual data changes were made via e-mail because the MDC request form was inefficient.

- The Technical Standards and Procedures manual did not address procedures regarding independent testing of application program changes or written user approval before the changes are moved into production.
- The PeopleSoft Financials Application Manager had the access capability to create and approve changes through the entire system development life cycle, including approval to Production. In response to our audit inquiry, the University indicated that development access for the Financials Application Manager had been deleted and was being granted in emergency situations only.

The aforementioned deficiencies in the change management process increased the risk that unauthorized or erroneous programs could be moved into the production environment without timely detection, which could jeopardize the ability of the University to meet its objectives.

Subsequent to our audit inquiries regarding the change management process, the University indicated that ASU had developed a new database, PantherTracks, to log and track issues and changes. According to the Financials Application Manager, the University began using the PantherTracks system on February 6, 2006. PantherTracks allows the University to track and manage the change management process from the users' input of issues into the system through the Application Manager being automatically e-mailed that the change is ready for production. It includes the assignment of developers, automatic e-mails for testing, user sign-offs, and ultimately an e-mail to the database administrator to move the item into production.

Recommendation: The University should take the necessary steps to update its policies and procedures to incorporate the PantherTracks process and ensure that the policies are being followed.

Finding No. 5: Disaster Recovery Planning

Disaster recovery planning is an element of IT controls established to manage the availability of valuable data and computer resources in the event of a processing disruption. Its main objective is to provide the organization with a plan for continuing critical operations, and, in an IT environment such as the University's, should take into consideration the significant dependence of its business processes on the ERP system. The success and effectiveness of a disaster recovery plan requires detailed development of back-up and recovery procedures, including identification of facilities, personnel, hardware, software, communications, and support services, as well as a commitment from management.

Although the University maintained a written disaster recovery plan, it was in draft form and was not current. Also, each department had its own emergency response plan, but this information was not included in or referenced from the disaster recovery plan. The lack of an approved and detailed disaster recovery plan may jeopardize the University's efforts to efficiently and effectively continue operations with minimal loss and processing disruption, should an event occur that interrupts IT services.

Recommendation: The University should continue with its efforts to complete the disaster recovery plan, along with incorporating the detailed departmental emergency response plans, to ensure a minimum business impact in the event of a major disruption.

Finding No. 6: Environmental Controls

Environmental controls can diminish interruption in service or data losses by allowing operation through short-term power outages or provide time to backup data and perform an orderly shutdown during extended power outages. The University did not have in place adequate environmental safeguards for its Data Center. Specifically, the University indicated that the power generator that provides emergency backup power to its Data Center does not have enough capacity to meet the needs of all hardware within the facility. Since the generator was donated by Monroe County for the primary purpose of supplying essential power to the building while it is being occupied by evacuees from Monroe County during disasters, the needs of the University were secondary. The University indicated that due to the critical nature of this issue becoming clear during Hurricane Wilma, funding has been allocated for a new generator or possible outsourcing of critical systems to an off-campus data center.

Without sound environmental safeguards, data center resources, equipment, and data may not be sufficiently protected from service disruption.

Recommendation: The University should implement and maintain environmental controls as noted above to ensure the safety of data center resources from environmental hazards.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this IT audit were to determine the effectiveness of selected University IT controls, including management's control framework for securing the application and the surrounding technology infrastructure. Our scope focused on evaluating selected internal controls and IT functions applicable to PeopleSoft financials during the period August 2005 through January 2006, and selected actions taken through May 2006. In conducting our audit, we interviewed appropriate personnel, observed University processes and procedures, and performed various other audit procedures to test selected IT controls.

AUTHORITY

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our information technology audit.

William O. Monroe

William O. Monroe, CPA
Auditor General

MANAGEMENT RESPONSE

In a letter dated July 17, 2006, the President provided responses to our preliminary and tentative findings. This letter is included at the end of this report as Appendix A.

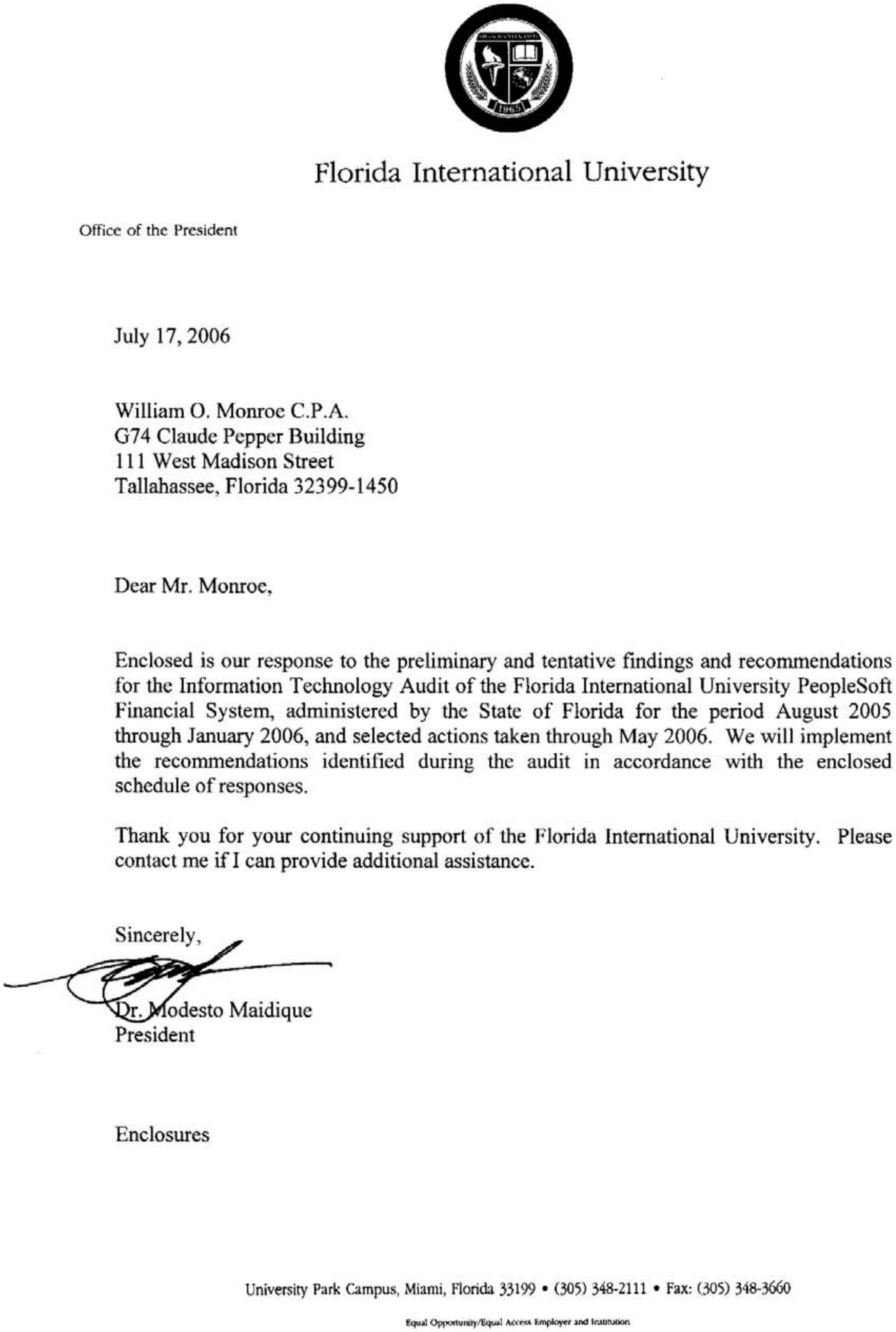
To promote accountability and improvement in government operations, the Auditor General makes audits of the information technology programs, activities, and functions of governmental entities. This information technology audit was made in accordance with applicable standards contained in ***Government Auditing Standards*** issued by the Comptroller General of the United States. This audit was conducted by Kathy Sellers, CISA, and supervised by Nancy Reeder, CPA*, CISA. Please address inquiries regarding this report to Jon Ingram, CPA*, CISA, Audit Manager, via e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other audit reports prepared by the Auditor General can be obtained on our Web site (http://www.state.fl.us/audgen); by telephone (850 487-9024); or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).

*Regulated by State of Florida.

APPENDIX A

MANAGEMENT RESPONSE



Florida International University

Office of the President

July 17, 2006

William O. Monroe C.P.A.
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Monroe,

Enclosed is our response to the preliminary and tentative findings and recommendations for the Information Technology Audit of the Florida International University PeopleSoft Financial System, administered by the State of Florida for the period August 2005 through January 2006, and selected actions taken through May 2006. We will implement the recommendations identified during the audit in accordance with the enclosed schedule of responses.

Thank you for your continuing support of the Florida International University. Please contact me if I can provide additional assistance.

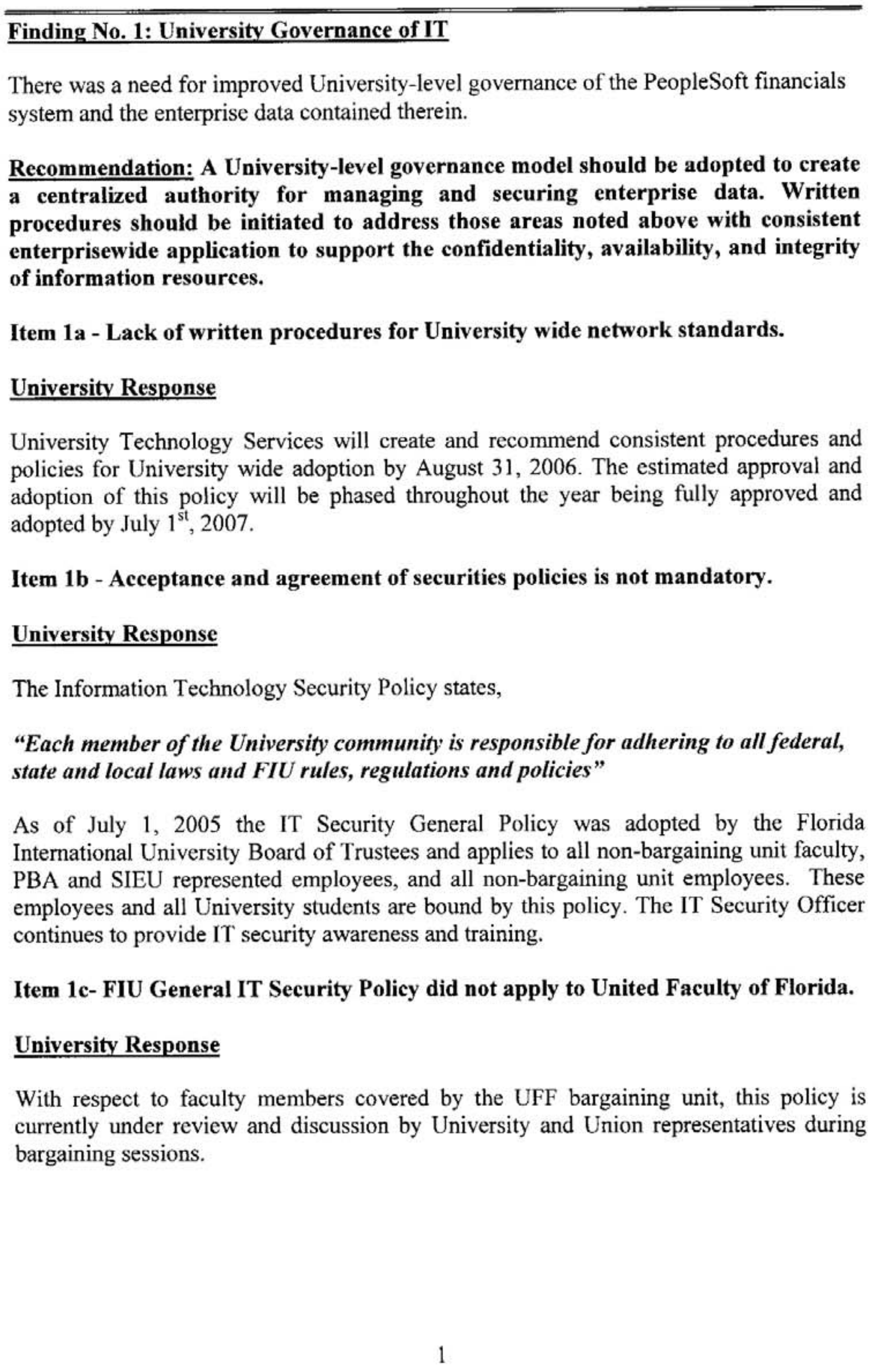
Sincerely,

Dr. Modesto Maidique
President

Enclosures

University Park Campus, Miami, Florida 33199 • (305) 348-2111 • Fax: (305) 348-3660

Equal Opportunity/Equal Access Employer and Institution



Finding No. 1: University Governance of IT

There was a need for improved University-level governance of the PeopleSoft financials system and the enterprise data contained therein.

Recommendation: A University-level governance model should be adopted to create a centralized authority for managing and securing enterprise data. Written procedures should be initiated to address those areas noted above with consistent enterprisewide application to support the confidentiality, availability, and integrity of information resources.

Item 1a - Lack of written procedures for University wide network standards.

University Response

University Technology Services will create and recommend consistent procedures and policies for University wide adoption by August 31, 2006. The estimated approval and adoption of this policy will be phased throughout the year being fully approved and adopted by July 1st, 2007.

Item 1b - Acceptance and agreement of securities policies is not mandatory.

University Response

The Information Technology Security Policy states,

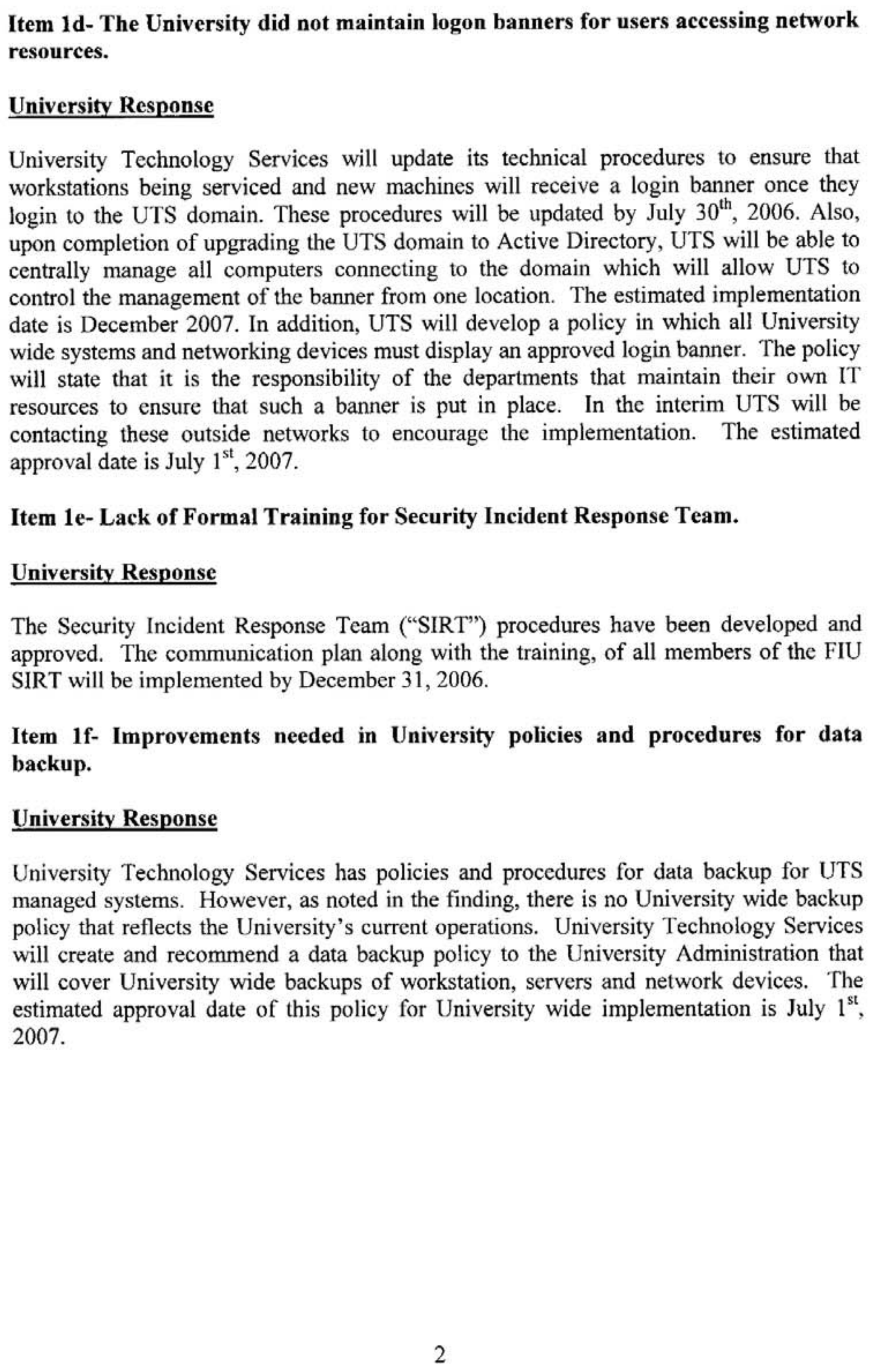
"Each member of the University community is responsible for adhering to all federal, state and local laws and FIU rules, regulations and policies"

As of July 1, 2005 the IT Security General Policy was adopted by the Florida International University Board of Trustees and applies to all non-bargaining unit faculty, PBA and SIEU represented employees, and all non-bargaining unit employees. These employees and all University students are bound by this policy. The IT Security Officer continues to provide IT security awareness and training.

Item 1c- FIU General IT Security Policy did not apply to United Faculty of Florida.

University Response

With respect to faculty members covered by the UFF bargaining unit, this policy is currently under review and discussion by University and Union representatives during bargaining sessions.



Item 1d- The University did not maintain logon banners for users accessing network resources.

University Response

University Technology Services will update its technical procedures to ensure that workstations being serviced and new machines will receive a login banner once they login to the UTS domain. These procedures will be updated by July 30th, 2006. Also, upon completion of upgrading the UTS domain to Active Directory, UTS will be able to centrally manage all computers connecting to the domain which will allow UTS to control the management of the banner from one location. The estimated implementation date is December 2007. In addition, UTS will develop a policy in which all University wide systems and networking devices must display an approved login banner. The policy will state that it is the responsibility of the departments that maintain their own IT resources to ensure that such a banner is put in place. In the interim UTS will be contacting these outside networks to encourage the implementation. The estimated approval date is July 1st, 2007.

Item 1e- Lack of Formal Training for Security Incident Response Team.

University Response

The Security Incident Response Team ("SIRT") procedures have been developed and approved. The communication plan along with the training, of all members of the FIU SIRT will be implemented by December 31, 2006.

Item 1f- Improvements needed in University policies and procedures for data backup.

University Response

University Technology Services has policies and procedures for data backup for UTS managed systems. However, as noted in the finding, there is no University wide backup policy that reflects the University's current operations. University Technology Services will create and recommend a data backup policy to the University Administration that will cover University wide backups of workstation, servers and network devices. The estimated approval date of this policy for University wide implementation is July 1st, 2007.

Item 1g- Lack of written security policies and procedures for the periodic review of the PeopleSoft financials user access privileges lists.

University Response

The Controllers Office has begun the process of reviewing all user access outside of the standard University access request form, and will complete this process on August 31, 2006. The different security roles have been reviewed and are in the process of being clearly defined and consolidated. Once the review and adjustments are completed, subsequent review will be performed on a quarterly basis. Expected completion date for review is October 31, 2006.

Item 1h- PeopleSoft did not include procedures to ensure that changes or customizations to the application supported compliance with Section 508, of the Americans with Disabilities Act ("ADA").

University Response

University Technology Services will create a procedure to ensure that all PantherSoft custom software development is compliant with ADA standards. This procedure will require that all custom software development be performed by developers trained on the ADA standards. Software code review will be performed by the lead software developer to the extent that is necessary and appropriate in order to ensure that custom software is ADA compliant. Additionally, UTS issues and software changes tracking solution (PantherTracks) will be updated to include signoff for ADA compliance for all software customizations going into the PantherSoft systems.

The estimated implementation date is February 1, 2007.

Finding No. 2: Application Environment and Support Function

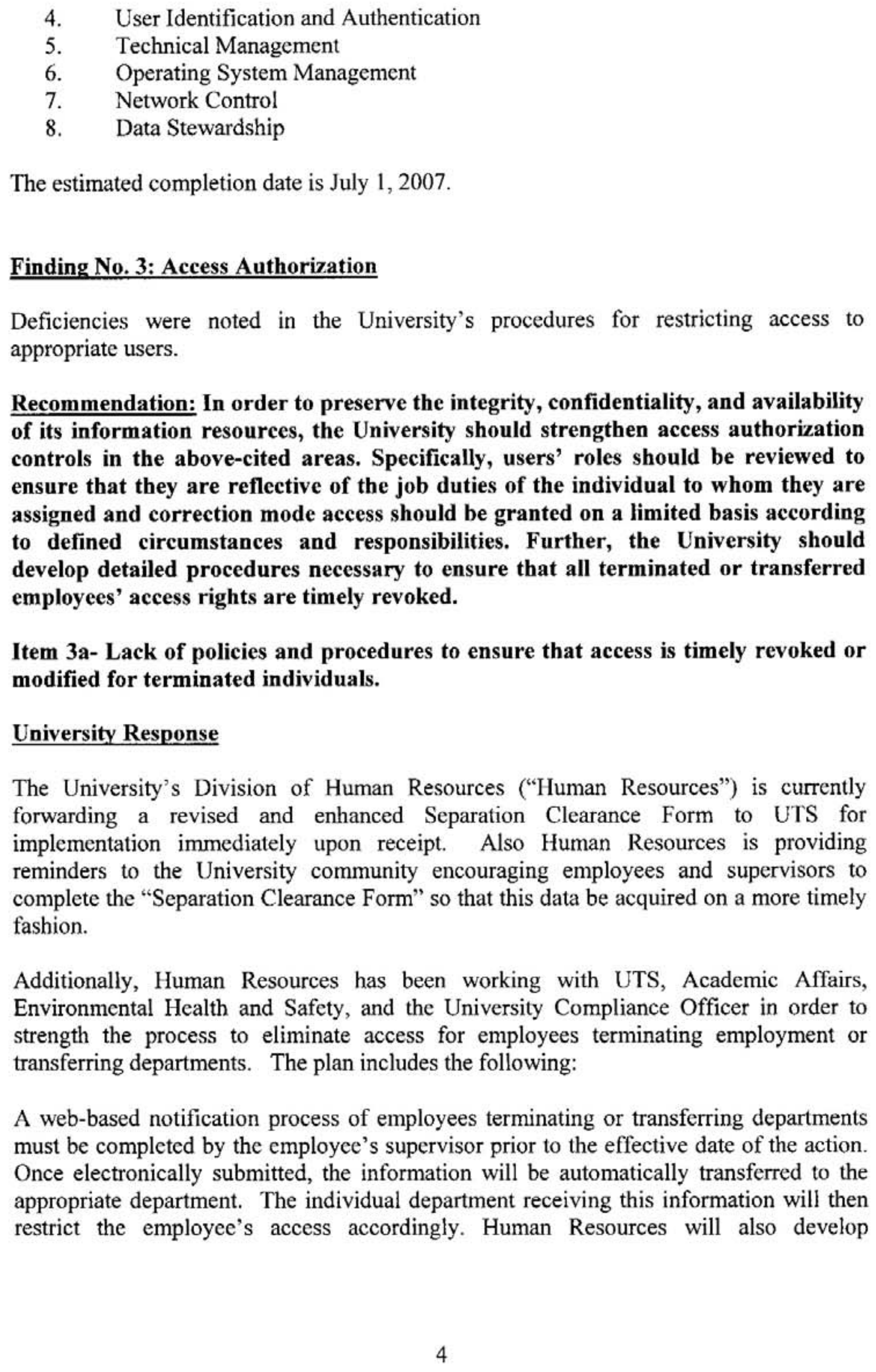
Improvements were needed in certain security controls within the overall operations of the application and the supporting network environment at the University.

Recommendation: University management should strengthen its control surrounding its enterprise information resources and systems in the mentioned areas.

University Response

The FIU IT Security Council is developing written policies and procedures for the following areas:

1. System Logging
2. Wireless Access
3. Work Station Control and Security



4. User Identification and Authentication
5. Technical Management
6. Operating System Management
7. Network Control
8. Data Stewardship

The estimated completion date is July 1, 2007.

Finding No. 3: Access Authorization

Deficiencies were noted in the University's procedures for restricting access to appropriate users.

Recommendation: In order to preserve the integrity, confidentiality, and availability of its information resources, the University should strengthen access authorization controls in the above-cited areas. Specifically, users' roles should be reviewed to ensure that they are reflective of the job duties of the individual to whom they are assigned and correction mode access should be granted on a limited basis according to defined circumstances and responsibilities. Further, the University should develop detailed procedures necessary to ensure that all terminated or transferred employees' access rights are timely revoked.

Item 3a- Lack of policies and procedures to ensure that access is timely revoked or modified for terminated individuals.

University Response

The University's Division of Human Resources ("Human Resources") is currently forwarding a revised and enhanced Separation Clearance Form to UTS for implementation immediately upon receipt. Also Human Resources is providing reminders to the University community encouraging employees and supervisors to complete the "Separation Clearance Form" so that this data be acquired on a more timely fashion.

Additionally, Human Resources has been working with UTS, Academic Affairs, Environmental Health and Safety, and the University Compliance Officer in order to strength the process to eliminate access for employees terminating employment or transferring departments. The plan includes the following:

A web-based notification process of employees terminating or transferring departments must be completed by the employee's supervisor prior to the effective date of the action. Once electronically submitted, the information will be automatically transferred to the appropriate department. The individual department receiving this information will then restrict the employee's access accordingly. Human Resources will also develop guidelines to the University supervisors' and explain the critical need to successfully implement this initiative.

The estimated implementation date is no later than December 31, 2006.

Item 3b- Inappropriate or unnecessary access privileges.

University Response

As noted in the finding, the university removed or adjusted accordingly the access privileges to the instances whereby the employees appeared to have inappropriate roles with the exception of certain technical support which is critical to operations. This functionality is being transitioned to the appropriate functional user and will be completed by August 31, 2006. In the instances where the user access privileges to certain panels (pages) within the financials system was inappropriate the access was removed. Further review of all financial users is being undertaken, please refer to response 1g above for the noted review process.

Item 3c- No defined circumstances or designated personnel appropriate for correction mode usage.

University Response

As noted in the finding, during February 2006 procedures have already been implemented to address the correction mode access. Furthermore, correction mode was restricted to a selection of users to specific functionality and justification for this access.

Finding No. 4: Change Management Process

Improvements were needed in the change management process.

Recommendation: The University should take the necessary steps to update its policies and procedures to incorporate the PantherTracks process and ensure that the policies are being followed.

University Response

University Technology Services developed an in-house software tool, named PantherTracks, to control the Change Management process for all software changes in PantherSoft. This tool tracks adjustments from the initial change request made by personnel in the functional areas through final deployment into the production environment. It also includes an entire approval process for Unit Testing and User Acceptance Testing, with notification to the proper functional and technical personnel, as well as the application managers. University Technology Services will update its technical procedures to incorporate the new Change Management tool.

The estimated date the procedure will be updated is November 30, 2006.

Finding 5: Disaster Recovery Planning

Deficiencies were noted in the disaster recovery management process.

Recommendation: The University should continue with its efforts to complete the disaster recovery plan, along with incorporating the detailed departmental emergency response plans, to ensure a minimum business impact in the event of a major disruption.

University Response

The Division of Information Technology is in the process of completing and approving the current Disaster Recovery Plan, including incorporation of the emergency plans. The estimated completion date is April 30, 2007.

Finding 6: Environmental Controls

Environmental control improvements were needed at the University's Data Center.

Recommendation: The University should implement and maintain environmental controls as noted above to ensure the safety of data center resources from environmental hazards.

University Response

University Technology Services has identified three options to maintain environmental controls and ensuring safety of the data center resources from environmental hazards. Once a selection is made the plan will include the resolution of the generator power issue in the Data Center.

Due to potential construction needed and/or physical transfer of infrastructure, the completion date is estimated to be no later than June 1st, 2007.

THIS PAGE INTENTIONALLY LEFT BLANK