

**DEPARTMENT OF PARKING AND TRANSPORTATION
SERVICES
AUDIT OF INFORMATION SYSTEMS
THE UNIVERSITY OF NEW MEXICO**

**Report 2006-18
April 6, 2006**



The University of New Mexico

Audit Committee Members

Raymond Sanchez, Chair
Don Chalmers, Vice Chair
John M. "Mel" Eaves

Audit Staff

Debra Yoshimura, Audit Director
Yvonne Cox, Internal Audit Manager
Lisa Wauneka, Information Systems Auditor

CONTENTS

EXECUTIVE SUMMARY 1

INTRODUCTION..... 3

 BACKGROUND 3

 PURPOSE..... 4

 SCOPE 4

OBSERVATIONS, RECOMMENDATIONS AND RESPONSES 5

PARKING SERVICES ISSUES 5

 Parking Services System Administration Procedures..... 5

 Parking Services Information Security Administration..... 6

 Parking Management System 8

 Parking Management System User Security Administration 10

 Parking Services Visitor Citations 11

UNIVERSITY-WIDE ISSUES 11

 Compliance with External Requirements 11

 Maintenance of Policies..... 15

 Information Security Officer..... 17

 Data Classification Policy..... 18

 Transmission of Sensitive Data over the University Network..... 19

CONCLUSION 21

APPROVALS 21

ABBREVIATIONS

CIO	Chief Information Officer
CIRT	Computer and Information Resources and Technology
CISP	Cardholder Information Security Program
COBIT	Control Objectives for Information and related Technology (published by the Information System Audit and Control Foundation, IT Governance Institute)
DBA	Database Administrator
FERPA	Federal Education Rights and Privacy Act
FTC	Federal Trade Commission
FTP	File Transfer Protocol
GLB Act	Gramm-Leach-Bliley Act
HR	Human Resources
ISO	Information Security Officer
IT	Information Technology
ODBC	Open DataBase Connectivity
Parking Services	Department of Parking and Transportation Services
PCI	Payment Card Industry
PM System	Parking Management System
PSSA	Parking Services System Administration
SSN	social security number
University	The University of New Mexico
UNM	The University of New Mexico
VPN	virtual private network

EXECUTIVE SUMMARY

The Department of Parking and Transportation Services (Parking Services) is responsible for managing approximately 10,000 parking spaces on the north, south, and main campuses. Our audit was limited to the Parking Services information systems and related University information system's policies and procedures.

Parking Services System Administration needs to be provided with the resources to administer their information systems. Parking Services needs to develop written procedures for their departmental information systems, develop security procedures and develop a migration path to a Parking Management System that will meet their future needs.

The University should ensure that it is in compliance with significant laws, regulations and contractual obligations. University documents and policies should be updated on a regular basis. University policy for University information systems should provide additional guidance for information system management University-wide.

The following summary provides management with an overview of conditions requiring attention.

PARKING SERVICES ISSUES

Parking Services System Administration Procedures

Parking Services needs to review the sufficiency of resources for Parking Services System Administration (PSSA). The Director of Parking Services responded he added staff to PSSA.

Parking Services Information Security Administration

PSSA needs to implement security administration procedures and work with other organizations [REDACTED]. The Director of Parking Services stated he will ensure procedures are implemented and [REDACTED].

Parking Management System

Parking Services should develop a migration path to a new PM System. The Director of Parking Services responded the new PM System will be implemented using system development methodology.

Parking Management System User Security Administration

PSSA should develop written user security administration procedures for the PM System. The Director of Parking Services stated the procedures will be developed and implemented.

Parking Services Visitor Citations

PSSA should alter the web site so campus visitors paying parking citations do not have to enter social security numbers. The Director of Parking Services stated the web site will be altered.

UNIVERSITY-WIDE ISSUES

Compliance with External Requirements

The University needs to develop a process to ensure the University complies with applicable laws, regulations, and contractual obligations, in a timely manner. The University should also develop a course of action to ensure the requirements of current regulations are met. The President's Office responded University Counsel will conduct a biennial review of external requirements, the Controller will develop policies to address the requirements and the Policy Office will publish them. For current regulatory issues University Counsel and the Controller will develop an action plan.

Maintenance of Policies

The University should develop a process to ensure that University policy, and official documents and communications are reviewed and updated on a regular basis. The President's Office responded the Policy Office will ensure appropriate changes are made when policies change.

Information Security Officer

The University should hire an Information Security Officer for Information Technology (IT). The Chief Information Officer responded he requested funding for this position.

Data Classification Policy

The University should develop a data classification IT policy to determine how data should be protected. The Chief Information Officer responded he will establish a cross-campus group to develop the policy.

Transmission of Sensitive Data over the University Network

The University should develop an IT standard which states that the University will not allow [REDACTED] The standard should include acceptable options for data transmission. The Chief Information Officer responded the development of data transmission technical standards will be a top priority for the newly created cross-campus security standards groups.

INTRODUCTION

BACKGROUND

The Parking Services audit is included in the Internal Audit Department's audit plan for fiscal year 2005. The report on the business processes was finalized in January 2006. This report addresses the information systems at Parking Services.

Parking Services is a business auxiliary service of the University, responsible for managing approximately 10,000 parking spaces on the north, south, and main campuses. Parking Services System Administration (PSSA) maintains information systems hardware and software to support Parking Services business functions. The information systems include the following:

- Parking Management System (PM System),
- Parking Services web site,
- Web, mail, anti-virus, and file servers,
- Workstations,
- Applications developed in-house,
- Handheld ticket writers,
- Meter management software,
- Visitor lot software, and
- Access management software.

The PM System is Parking Services' most critical business application. It is a comprehensive parking management system designed to manage all aspects of the parking function. The PM System includes function/modules for customers, vehicle registration, citations, vehicle towing, hearings, permits, collections, wait list, event management, and permit sales and appeals over the Parking Services web site. The PM System contains data on all current and former University faculty, staff and students. The PM system receives and transmits data to multiple University systems outside of Parking Services. [REDACTED]

Gross revenue processed by the PM System for Parking Services for the fiscal year ended June 30, 2005, was \$4,579,683 consisting of: \$2,696,306 in Permit Sales, \$1,059,560 in Visitor and Event Parking Revenue, \$565,618 in Citation Fee Revenue, and \$258,199 in Metered Parking Revenue.

PURPOSE

The audit was directed toward determining whether Parking Services has developed policies and procedures to ensure an adequate and effective system of control for their information systems. These controls should ensure the following:

- effectiveness and efficiency of operations,
- reliability of information,
- compliance with laws and regulations, and
- confidentiality, integrity, and availability of Parking Services information systems and data.

SCOPE

The audit scope included the following:

- review of applicable legal, regulatory, and contractual obligations,
- review of University policy addressing applicable legal, regulatory, and contractual obligations,
- review of applicable University information system policies and procedures,
- review of Parking Services information system's policies and procedures,
- review of the administration and security of the PM System, PM System interfaces, and data.

The review of legal, regulatory, and contractual obligations was limited to those applicable to the data processed through Parking Services information systems. This data includes sensitive student, employee, and customer data such as social security and credit card numbers. University policy was reviewed to determine if policy was developed to communicate these requirements to the University community and ensure compliance with the legal, regulatory, and contractual obligations.

Due to the number of information systems maintained by Parking Services, the audit included a review of information systems policies and procedures. With the exception of the PM System, an in-depth review of all the information systems maintained by Parking Services was not performed.

Audit fieldwork was started in June of 2005 and was completed in November 2005. The audit criteria were developed using COBIT, Control Objectives for Information and related Technology (published by the Information System Audit and Control Foundation, IT Governance Institute). COBIT's purpose is to develop and publish best practices for IT Governance.

OBSERVATIONS, RECOMMENDATIONS AND RESPONSES

PARKING SERVICES ISSUES

Parking Services System Administration Procedures

PSSA has not documented the Parking Services information systems nor developed written system administration policies and procedures to manage the systems. Information systems should be developed and managed using a structured documented approach. Without documentation for all information system processes, the systems may not be configured, managed, or properly secured. COBIT AI4 best practices recommendation states: “Control over the IT process of developing and maintaining procedures that satisfies the business requirement to ensure the proper use of the applications and the technological solutions put in place is enabled by a structured approach to the development of user and operations procedures manuals...”

PSSA did not have the resources to adequately document Parking Services information systems. As of June 2005, the area was staffed with one System Administrator and one IT Support Technician in training.

Recommendation 1

We recommend PSSA develop Parking Services information systems documentation. The documentation should include the following:

- Parking Services IT systems and interfaces,
- a network map,
- system development methodology,
- change control process,
- security for hardware and software,
- routine system maintenance,
- business continuity / disaster recovery,
- back-up, and
- data retention.

Response from the Director of Parking and Transportation Services

Parking and Transportation Services agrees with the recommendation and PSSA will complete documentation for the processes listed above by the end of the 2006 calendar year with the exception of processes that integrate with the legacy Parking Management System (PMS). Processes pertaining to the PMS will be developed and documented as part of the migration to the new PMS, which the department is in the process of acquiring. (Please see Recommendation Six response.) Implementation of the new PMS is contingent on the Banner implementation timeline but is tentatively scheduled for completion by September 30, 2007.

Recommendation 2

We recommend the Parking Services Director review PSSA's resources to ensure the resources are sufficient to maintain the Parking Services information systems.

Response from the Director of Parking and Transportation Services

Parking and Transportation Services agrees with the recommendation and PSSA has evaluated current staffing and estimated the needs to manage its current responsibilities as well as development requirements. PSSA is now staffed with a manager, a newly-trained full-time IT Support technician, and a new three-quarter-time User Support Analyst I. PSSA is also investigating resource sharing opportunities within Auxiliaries Enterprises. We have reviewed employee workloads and are confident that we now have sufficient resources to maintain PATS' information systems and services in a manner responsive to the recommendations of Internal Audit.

Parking Services Information Security Administration

PSSA does not have written security administration policies and procedures, a security officer, or the resources to segregate these security duties. [REDACTED]

[REDACTED] The System Administrator's job description includes all areas of system administration including security administration. The job description was not written to support segregation of duties in the functional area. [REDACTED]

[REDACTED]

Parking Services handles [REDACTED]

Parking Services information systems security should be adequate to protect the parking data in compliance with applicable laws, regulations, contractual obligations and University policies. System security is a critical component of Parking Services operations, in accordance with COBIT DS5 *Delivery and Support, Ensure Systems Security*, systems security should safeguard information against unauthorized use, disclosure or modification, damage or loss by use of logical access controls. Logical access controls will ensure access to systems, data, and programs are restricted to authorized users. Security measures should be managed by developing, implementing, and updating IT security plans.

Recommendation 3

We recommend PSSA develop and implement security administration policies and procedures. The policies and procedures should address:

- segregation of duties,
- monitoring of user system activities,
- monitoring of intrusion attempts,
- review of security activities, and
- compliance with applicable laws, regulations, contractual obligations and University policies.

Response from the Director of Parking and Transportation Services

Parking and Transportation Services agrees with the recommendation and has accelerated procedure development and/or documentation in each of these areas. We have reviewed existing procedures and are confident that we are in “compliance with applicable laws, regulations, contractual obligations and University policies” although documentation of procedure will require additional work. Procedures will be developed and/or documented in all areas not dependent on migration to the new PMS by December 31, 2006. Procedures that are PMS dependent will be documented on or before September 30, 2007, contingent on the Banner system’s readiness for PMS integration.

Recommendation 4

We recommend Parking Services work with CIRT to jointly develop an [REDACTED]

Response from the Director of Parking and Transportation Services

Parking and Transportation Services agrees with the recommendation and PSSA has initiated the process of assessing needs and capabilities with representative from CIRT [REDACTED]

[REDACTED] PSSA will have a temporary solution in place by July 1, 2006 and a permanent solution will be implemented upon migration to the new PMS tentatively scheduled for completion by September 30, 2007.

Recommendation 5

We recommend Parking Services work with Finance Systems Management Network Support [REDACTED]

Response from the Director of Parking and Transportation Services

Parking and Transportation Services agrees with the recommendation and will initiate contact with the Finance Systems Management Network team [REDACTED] and will have a temporary solution in place by July 1, 2006. PSSA has been working with the HR/Payroll Banner application development team for the purpose of integrating the new PMS with Banner. The Banner team is currently evaluating required data and processes for the project and the current plan is to have a permanent solution for full integration between Banner and the PMS tentatively scheduled for completion by September 30, 2007, contingent on Banner readiness.

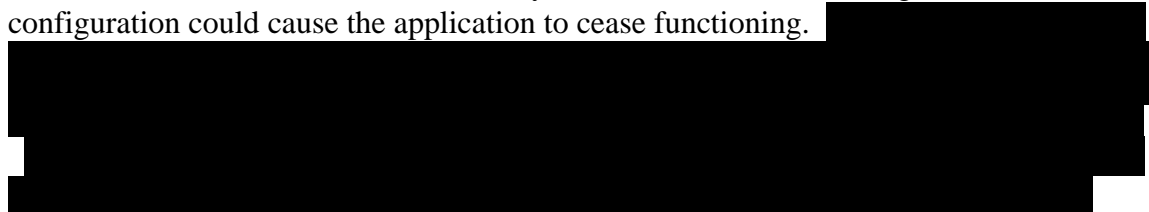
Parking Management System

Parking Services uses a commercially developed off-the-shelf PM System application to manage the parking function. Information System applications should provide the functionality to support the users business needs in a secure and efficient manner. The current PM System no longer has the ability to meet Parking Services' current and future business needs. Internal Audit noted the following issues with the PM System.

- Parking Services is not using the current version of the PM System and has not developed a migration path to the current version of the system or to a different parking management system. Parking Services has stopped paying for maintenance and support for the PM System because the vendor is no longer providing upgrades for this version of the PM System. Parking Services now pays an hourly rate for vendor support as needed. Vendors will not indefinitely support older versions of their applications.
- Parking Services has developed manual processes to supplement or replace the functionality of the PM System. Manual process were also developed out of necessity to send and received data from existing legacy mainframe systems. Manual processes are less efficient and more prone to error than automated processes. The PM System's interfaces to other University systems are currently manual processes. Automated application functions should be utilized to reduce the need for development of in-house applications and manual processes. Customization of applications and in-house

developed applications make migration to different products more difficult and expensive.

- The PM System does not have a system administrator manual. The application is difficult to administer in the absence of system documentation. Changes to the configuration could cause the application to cease functioning.



PSSA did not have the resources or the system documentation to adequately maintain the PM System. Lack of system documentation and the use of manual processes also make the application maintenance more complex and time consuming.

Recommendation 6

We recommend Parking Services develop a migration path to the new version of the PM System or to a new PM System. A formal system development methodology should be followed to effectively support the department's business needs. The methodology should address the following:

- systems software configuration,
- application controls and security requirements,
- data structures, and
- documentation requirements.

Response from the Director of Parking and Transportation Services

Parking and Transportation Services agrees with the recommendation and PSSA will develop a migration path and methodology before the implementation of the new parking management application and will have the process documented by December 31, 2006.

Response from the Chief Information Officer

The CIO also has the following comment on Parking Management System – Recommendation 6. If Parking Services plans to migrate to a new PM system, the CIO recommends that a Banner Partner product be considered and selected for a more cost-effective expenditure.

- *Integration of information*
- *Functionality*
- *Maximizing investment in IT production platforms.*

Parking Management System User Security Administration

Parking Services does not have written user security administrator procedures for the PM System. [REDACTED]

- Users should only have the access necessary to perform their job functions. Access should be changed when users' job functions change and removed when users are terminated. In the PM System:
 - 22% of active user ids have not been used in more than one year,
 - Users have been granted more access to the system than necessary to perform their job functions,
 - User History records should be created for all parking citation edits. This is not turned on for three users.
 - The PM System recommends no access to Adjust Citation Fines. This access is for emergency purposes only. This option is turned on for seven users.
 - The PM System recommends limited access to Codes menus. This access has not been reviewed or limited appropriately.
- Passwords for systems containing sensitive data should expire frequently. [REDACTED]

In accordance with COBIT DS5 *Delivery and Support, Ensure Systems Security*, systems security should safeguard information against unauthorized use, disclosure or modification, damage or loss by use of logical access controls. Logical Access controls will ensure access to systems, data, and programs is restricted to authorized users.

PSSA did not have the resources to adequately maintain the PM System.

Recommendation 7

We recommend PSSA develop written user security administration procedures for the PM System. These procedures should be in place for the current system and are also applicable to any new system Parking Services implements. The procedures should address the following.

- issuing, approving, and monitoring user access.
- granting users the minimum access needed to perform their job functions.
- timely deletion/disabling of user ids when users are terminated or job responsibilities are changed.
- process for user supervisors to review user access reports to ensure user access is still appropriate for the users' job functions.
- [REDACTED]
- procedures for issuing, approving, monitoring and deleting [REDACTED]

- passwords standards requiring changing of passwords every 30 days due to the sensitive student and employee data in the PM System.
- reviewing the PM System's User Access recommendations to ensure users are given access to only recommended system functions.

Response from the Director of Parking and Transportation Services

Parking and Transportation Services agrees with the recommendation and PSSA has corrected all of the concerns noted in the recommendation within the limits of the current PMS. Written documentation of these processes will be completed by the December 31, 2006. Full implementation of the recommendation will be following migration to the new PMS, tentatively scheduled for September 30, 2007, contingent on Banner readiness.

Parking Services Visitor Citations

Campus visitors attempting to pay a parking citation on the Parking Services web site must enter a [REDACTED]. Parking Services used the same format for a visitor paying a citation as for University students and employees whose [REDACTED]. This should not be required for these citations. Parking Services should make the process of paying a citation as user friendly as possible in order to collect the citation fees. Citations may remain unpaid if the process to pay online is difficult and requires unnecessary information.

Recommendation 8

We recommend PSSA alter the web site so campus visitors attempting to pay or appeal a parking citation on the Parking Services web site do not have to enter a [REDACTED].

Response from the Director of Parking and Transportation Services

Parking and Transportation Services agrees with the recommendation and PSSA will modify the website or create a new module where visitors can pay for citations without using their [REDACTED]. The expected launch date for this application is on or before July 1, 2006.

UNIVERSITY-WIDE ISSUES

Compliance with External Requirements

Internal Audit reviewed the laws, regulations, University policies, standards, and guidelines applicable to Parking Services' information systems and data. During this review, Audit noted the University has not developed policies to address compliance with the following:

- the Gramm-Leach-Bliley Act (GLB Act), with a compliance deadline of May 2003; and

- the Cardholder Information Security Program (CISP), which requires an Information Security Policy to address the Payment Card Industry (PCI) Data Security Standard.

Best practices recommend that management ensure compliance with external requirements to meet legal, regulatory, and contractual obligations, per COBIT PO8 *Planning & Organisation, Ensure Compliance with External Requirements*.

Gramm-Leach-Bliley Act

The deadline for compliance with the GLB Act for colleges and universities was May 2003. Colleges and universities are subject to the Standards for Safeguarding Customer Information Safeguards Rule. The Safeguards Rule requires financial institutions to secure customer records and information. Colleges and universities are considered financial institutions because they perform financial activities, such as making Federal Perkins loans.

16 CFR Part 314, published in May 2002 (May 23 Federal Register, p. 346484) states: "...the standards are intended to: Ensure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer."

FTC (Federal Trade Commission) Facts for Business: *Financial Institutions and Customer Data: Complying with the Safeguards Rule*, published September 2002 states.

The Safeguards Rule requires financial institutions to develop a written information security plan that describes their program to protect customer information. The plan must be appropriate to the financial institution's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each financial institution must:

1. designate one or more employees to coordinate the safeguards;
2. identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
3. design and implement a safeguards program, and regularly monitor and test it;
4. select appropriate service providers and contract with them to implement safeguards; and
5. evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business arrangements or operations, or the results of testing and monitoring of safeguards.

To retain appropriate flexibility, the FTC will rely on its discretion in enforcing the Safeguards Rule, and not describe any particular schedule or methods for enforcement. The FTC is bringing administrative actions against businesses that violate the GLB Act's Safeguards Rule.

Cardholder Information Security Program

The CISP was mandated in June 2001 to protect cardholder data. CISP compliance is required of all merchants and service providers that store, process, or transmit cardholder data. To achieve compliance with CISP, merchants and service providers must adhere to the PCI Data Security Standard.

The PCI Data Security Standard was designed to safeguard sensitive customer data for all card brands. There are six main topics in the Standard:

- Build and Maintain a Secure Network;
- Protect Cardholder Data;
- Maintain a Vulnerability Management Program;
- Implement Strong Access Control Measures;
- Regularly Monitor and Test Networks; and
- Maintain an Information Security Policy.

The Information Security Policy is a critical piece of the PCI Data Security Standard. In brief, it requires the following.

- Establish, publish, maintain, and disseminate a security policy that addresses information security for employees and contractors.
- Develop daily operational security procedures.
- Develop usage policies for critical employee-facing technologies, such as modems and wireless.
- Ensure the security policy and procedures clearly define information security responsibilities for all employees and contractors.
- Assign to an individual or team information security management responsibilities.
- Make all employees aware of the importance of cardholder information security.
- Screen potential employees to minimize the risk of attacks from internal sources.
- Contractually require all third parties with access to cardholder data to adhere to payment card industry security requirements.
- Implement an incident response plan. Be prepared to respond immediately to a system breach.

There are fines for non-compliance with the PCI Data Security Standards. Visa and MasterCard may impose fines on their member banking institutions, in this case Wells Fargo, our merchant bank, for non-compliance. The University is contractually obligated to indemnify and reimburse Wells Fargo for such fines. If cardholder data the University is responsible for is compromised,

the University may be subject to the following liabilities and fines associated with non-compliance.

- potential fines of up to \$500,000 (at the discretion of Visa, MasterCard or other card companies);
- all fraud losses incurred from the use of the compromised account numbers from the date of compromise forward;
- cost of re-issuing cards associated with the compromise;
- cost of any additional fraud prevention/detection activities required by the card associations (i.e. a forensic audit) or costs incurred by credit card issuers associated with the compromise (i.e. additional monitoring of system for fraudulent activity).

Recommendation 9

We recommend the President's Office ensure a process is developed for external requirements review. This process should include procedures for continuous research for requirements applicable to the University, development of policies to address the requirements, and for the timely implementation of the requirements.

Response from the Acting President

The Office of the President agrees with the recommendation and has charged University Counsel with conducting a biennial review of external requirements, the Controller/Associate Vice President Financial Services, Main Campus, with development of policies to address the requirements, and the Policy Office with publication of the requirements. Initial review and preparation of a draft policy will be completed by June 30, 2007.

Recommendation 10

We recommend the President's Office ensure that policies and procedures detailing the action to be taken to ensure the University is compliant with the GLB Act and the CISP are developed.

Response from the Acting President

The Office of the President agrees with the recommendation and has charged University Counsel and the Controller/Associate Vice President Financial Services, Main Campus, with developing an action plan for implementing and confirming compliance with the policies developed in response to Recommendation Nine and in compliance with FTC guidelines. The action plan will be completed no later than December 31, 2006.

Maintenance of Policies

The University has not developed a process to ensure official University policies, documents, and communications are in compliance with applicable laws and regulations. University organizations responsible for this official University documentation are not reviewing and updating their documentation to maintain compliance with the Privacy Act of 1974. This may result in the University being in noncompliance with the Privacy Act of 1974 or other significant laws and regulations. The University should ensure official University documentation is reviewed and updated on a regular basis. The following policy issues illustrate this point.

A. Board of Regents Policy Manual Privacy Act of 1974 Policy Removed

The University uses an exception to the Privacy Act of 1974 to require student to disclose their social security numbers (SSN) to the University for use as their student identification number. The University referred to the exception in the Board of Regents Policy Manual in past editions of the manual but the policy was removed from the current manual. The policy is referred to in the student handbook and on official documents throughout the University.

Overview of the Privacy Act of 1974, U.S. Department of Justice (May, 2004) Social Security Number Usage states: "It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number."

According to Overview of the Privacy Act of 1974, U.S. Department of Justice (May, 2004) Social Security Number Usage, the provision does not apply to "...any disclosure of a social security number to any federal, state or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual."

B. Inconsistent, Incorrect, Non-existent Social Security Number Disclosure Statements in Accordance with the Privacy Act of 1974

The language on the University's documents requiring students to disclose their SSNs is inconsistent, incorrect, or non-existent.

Overview of the Privacy Act of 1974, U.S. Department of Justice (May, 2004) Social Security Number Usage states: "Any Federal, State or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it."

The following official University documentation contain incorrect or conflicting statements on this requirement:

- the student handbook, Student I.D. Number;
- the UNM Catalog 2003-2005, Undergraduate Admissions, Use of Social Security Number; and
- Prospective Students Undergraduate Online Applications web page.

The required reference is not included on the Robert O. Anderson School of Management BBA Admission packet “Application on Pre-Admission Worksheet.”

C. Policies do not Address Privacy Act of 1974

The Banner project is resulting in changes to University policies and procedures. Two changes dealing with student social security numbers, “Management and Security of SSN” and “Consistent University Application for Admissions” have been approved but not yet implemented. These change requests do not address the Privacy Act of 1974. The Privacy Act of 1974 needs to be incorporated in the new policies before the policies are issued.

Recommendation 11

We recommend the President’s Office ensure a process is developed to review and update official policy, documents, and communications on a regular basis.

Response from the Acting President

The Office of the President agrees with the recommendation and has charged the University Policy Office with, each time a change is approved to the University Business Policy or the Regents’ Policy Manual, seeking other documents or processes dependent on the existing policy and confirming that appropriate changes are made to those dependent documents. The review process will be in place no later than June 30, 2006.

Recommendation 12

We recommend the President’s Office ensure official University policy, documents, and communications are reviewed and revised to make certain the documentation is compliant with the Privacy Act of 1974.

Response from the Acting President

The Office of the President agrees with the recommendation and has charged University Counsel with comprehensive review of University Business Policy and the Regents' Policy Manual to ensure compliance with the Privacy Act of 1974 and presentation of required changes to the University Policy Office for their action. The three areas addressed in the audit will be addressed no later than June 30, 2006. A comprehensive review will be completed no later than December 31, 2006.

Information Security Officer

The University does not have an Information Security Officer (ISO) to handle University-wide information security issues. The ISO position was to be funded by the Banner budget but the funding was cut and the position was not filled. The recommended practices per COBIT P04.6 state: "Management should formally assign the responsibility for assuring both the logical and physical security of the organisation's information assets to an information security manager, reporting to the organisation's senior management. At a minimum, security management responsibility should be established at the organisation-wide level to deal with overall security issues in an organisation. If needed, additional security management responsibilities should be assigned at a system-specific level to cope with the related security issues."

Without a central point of information security administration to develop security policies, procedures and standards, information security may not be adequate or effective. Information systems staff University-wide may be able to develop and maintain information security in a more efficient manner by following standards. Standards may also give management assurance that the University systems are functioning in a secure and efficient manner.

Recommendation 13

We recommend the Chief Information Officer (CIO) request the funding for and fill the ISO position. The position should report to the CIO and have University-wide authority to develop, implement and enforce IT security policies. These policies should include data security and privacy policies. The position should also assist the University in its compliance with relevant laws, regulations, and contractual agreements with IT-related provisions.

Response from the Chief Information Officer

- **Agreement:** *The CIO is in agreement with this audit finding.*
- **Corrective Action:** *Funding to establish an Information Security Compliance office was requested in at the February 2006 Budget Hearing and has been identified in a Strategy of the 2006 IT Strategic Plan. Efforts are being made to establish UNM-wide groups to develop IT security and privacy policies, and a Security Day takes place every semester now. In the absence of an employee with expertise and time available to do this, training and increasing general awareness is not effectively coordinated, nor does security awareness impact the whole University.*
- **Dates for Implementation:** *There is currently one person within the CIO organization with technical qualifications for security work, and his time is spent responding to incidents at an operational level. Therefore, advancing security work would entail a new hire. When funding is available, this function can be staffed.*

Data Classification Policy

The PM System contains [REDACTED] but the level of security protection required to adequately protect this data has not been defined because the University has not developed a data classification policy. University data may not be uniformly protected without clearly defined University-wide data classification policy. A data classification policy should define security levels for data based on the sensitivity, value, and criticality of the data as follows:

- COBIT P02.3 states: “A general classification framework should be established with regard to placement of data in information classes (i.e., security categories) as well as allocation of ownership. The access rules for the classes should be appropriately defined.”
- COBIT P02.4 states: “Management should define, implement and maintain security levels for each of the data classifications identified above the level of ‘no protection required.’ These security levels should represent the appropriate (minimum) set of security and control measures for each of the classifications and should be re-evaluated periodically and modified accordingly. Criteria for supporting different levels of security in the extended enterprise should be established to address the needs of evolving e-commerce, mobile computing and telecommuting environments.”

These policies have not been developed because before the CIO was hired in December 2004, the University did not have a position with University-wide authority to develop, implement, and enforce high-level IT policies.

Recommendation 14

We recommend the CIO develop a data classification IT policy to address the classification of data. The policy should include security levels for each of the data classifications identified from the level of no protection required to high protection required. These security levels should contain the minimum set of security and controls necessary to ensure data is protected in a manner commensurate with its sensitivity, value, and criticality. The data classification and security levels should be reviewed and updated on a regular basis.

Response from the Chief Information Officer

- **Agreement:** *The CIO is in agreement with this audit finding.*
- **Corrective Action:**
 - Policy: *Gather 'data stewards' responsible for management of the data from Finance, HR, Student Services, etc, to develop a UNM policy governing this data, regardless of the form it takes.*
 - Data Classification: *As more of Project LINK is implemented, technical applications and security staff are anticipated to become available to work with the data stewards to address the classification of data stored electronically.*
- **Dates for Implementation:**
 - Policy: *Draft by December, 2006*
 - Classification:
 - *Plan draft by Summer 2006.*
 - *Classification by July 2008*

Transmission of Sensitive Data over the University Network

The University has not developed security standards for data transmitted across the University network. [REDACTED]

Without adequate systems security sensitive data may not be protected against unauthorized use, disclosure or modification, damage or loss. COBIT DS5.16 best practices recommendation states: "Organisational policy should ensure that sensitive transaction data is only exchanged over a trusted path. Sensitive information includes security management information, sensitive transaction data, passwords, and cryptographic keys. To achieve this, trusted channels may need to be established using encryption between users, between users and systems, and between systems."

[REDACTED]

Before the CIO was hired in December 2004, the University did not have a position with University-wide authority to develop, implement, and enforce high-level IT policies. In May

2005, the CIO created the IT Cabinet, which is charged with and is working toward developing and advocating policies, procedures, and standards, but standards for sensitive data crossing the network lines have not yet been developed.

Recommendation 15

We recommend the CIO ensure the development of standards for IT. [REDACTED]

Response from the Chief Information Officer

- **Agreement:** *The CIO is in agreement with this audit finding.*
- **Corrective Action:**
 - *Immediate Action – [REDACTED]*
 - *Technical Standards - Developing detailed technical standards for data transmission can become a top priority for cross-campus security standards groups coming together now. These standards will address policy, process, adoption and compliance. This work is tied to Recommendation 13.*
- **Dates for Implementation:**
 - *Immediate Action – Parking Services could technically implement encryption by July 2006 – but they need to commit to this date.*
 - *Standards can be developed by June 2007.*

CONCLUSION

Parking Services System Administration needs to be provided the resources to effectively administer their information systems. This may be accomplished by providing more resources to Parking Services System Administration or by combining some of these functions with other University departments. Parking Services needs to develop written policies and procedures for their departmental information systems, develop security procedures and develop a migration path to a Parking Management System that will meet their future business requirements.

The University does not have a process to ensure compliance with external requirements in a timely manner. University policy needs to be written to communicate these external requirements to the University community. University policy should also be periodically reviewed to ensure it is up to date and consistent across all official University documents.

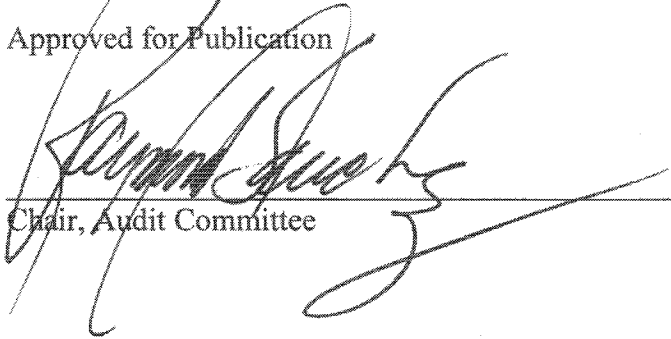
University policy communicates requirements for University information systems. University policy should be further developed to provide guidance for CIRT and University departmental information systems. An Information Security Officer should be hired to develop and enforce University-wide information systems security policies and standards. Providing guidance from the University level would be a more effective use of University resources than requiring the departments to develop their own standards on a case-by-case basis.

APPROVALS



Debra Yoshimura CPA, CIA, CGAP
Director, Internal Audit Department

Approved for Publication



Chair, Audit Committee