A REPORT
TO THE
MONTANA
LEGISLATURE

INFORMATION SYSTEMS AUDIT

Payment Card Industry Data Security Standard and Related Controls

The University of Montana-Missoula
Montana State University-Bozeman
Montana State University-Billings
Montana Department of Transportation

JUNE 2009

LEGISLATIVE AUDIT
DIVISION

09DP-02

Information Systems Audits

Information Systems (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. We conducted this IS audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objectives.

Members of the IS audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business, accounting, education, computer science, mathematics, political science, and public administration.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

Direct comments or inquiries to:
Legislative Audit Division
Room 160, State Capitol
P.O. Box 201705
Helena, MT 59620-1705
(406) 444-3122

Reports can be found in electronic format at:
Http://leg.mt.gov/audit

LEGISLATIVE AUDIT DIVISION

Tori Hunthausen, Legislative Auditor
Monica Huyg, Legal Counsel

Deputy Legislative Auditors
James Gillett
Angie Grove

June 2009

The Legislative Audit Committee
of the Montana State Legislature:

We conducted an Information Systems audit to determine if selected entities are following specific requirements of the Payment Card Industry Data Security Standard (PCI DSS). Our audit focused on policies and processes in place at The University of Montana – Missoula, Montana State University – Bozeman, Montana State University – Billings, and the Montana Department of Transportation.

This report contains one recommendation for the development and implementation of polices to define requirements and increase awareness, and one recommendation to ensure existing devices meet requirements of the PCI DSS.

We wish to express our appreciation to personnel within each of the four entities for their cooperation and assistance.

Respectfully submitted,

/s/ Tori Hunthausen

Tori Hunthausen, CPA
Legislative Auditor

Room 160 • State Capitol Building • PO Box 201705 • Helena, MT • 59620-1705
Phone (406) 444-3122 • FAX (406) 444-9784 • E-Mail lad@mt.gov

TABLE OF CONTENTS

Appointed and Administrative Officials

The University of Montana-Missoula	George M. Dennison, President Kathy Burgmeier, Director, Internal Audit
Montana State University-Bozeman	Dr. Geoffrey Gamble, President Daniel Adams, Director, Internal Audit
Montana State University-Billings	Dr. Ronald P. Sexton, Chancellor Terrie Iverson, Administrative Vice Chancellor
Montana Department of Transportation	Jim Lynch, Director Vickie Murphy, Manager, Internal Audit Jody Brandt, Operations Manager, Accounting Controls Bureau
Montana Department of Administration	Janet R. Kelly, Director

REPORT SUMMARY

Payment Card Industry Data Security Standard and Related Controls

The State of Montana provides a diverse set of services, and citizens and businesses can pay for services using cash, check, direct billing, payment cards, etc. Payment cards include debit or credit cards which carry the major payment card brand logos such as Visa, MasterCard, or American Express. The State of Montana currently accepts payment cards for more than 400 services such as tuition, athletics tickets, and motor carrier permits. According to the most recent figures for fiscal year 2008, the State of Montana collected nearly $300 million in revenues on over four million payment card transactions.

Current information suggests the average total cost of a data breach now exceeds $7 million per organization. Cardholder data security has become a priority for the major payment card brands leading them to form their own association to establish and regulate security standards. The current version, Payment Card Industry Data Security Standard (PCI DSS) version 1.2, became effective October 1, 2008.

Our audit objective was to determine if policies and business processes at selected entities conform to specific requirements of the PCI DSS. The four entities included in the audit were selected based on revenues and transactions processed and included The University of Montana – Missoula, Montana State University – Bozeman, Montana State University – Billings, and the Montana Department of Transportation.

Payment card information is obtained by the four entities in three ways: paper-based transactions, point of sale devices, and web applications. Through the state term contract for credit card processing services, agencies are given discretion regarding which method(s) work best for their needs. We reviewed all three methods of obtaining payment card information for all four entities. We interviewed management and staff within individual departments and discussed procedures for handling payment card information. In addition to interviews, we conducted observations of business processes and the office environments where payment card transactions are conducted and cardholder data is stored.

Overall, we found management and staff are concerned for the security of cardholder data. However, conformity with the specific requirements of the PCI DSS can be strengthened. This report discusses our findings and includes two recommendations addressing the need to strengthen policy and cardholder data security.

Chapter I – Introduction and Background

Introduction

The State of Montana, through its agencies and universities, provides a diverse set of services. Citizens and businesses can pay for services using cash, check, direct billing, payment cards, etc. Payment cards include debit or credit cards which carry the major payment card brand logos such as Visa, MasterCard, or American Express. According to the most recent figures for fiscal year 2008, the State of Montana collected nearly $300 million in revenues on over four million payment card transactions.

According to its processing vendors (organizations which approve/deny payment card transactions), the State of Montana currently accepts payment cards for more than 400 services such as tuition, athletics tickets, and motor carrier permits. The agencies accepting payment cards for these services employ a variety of business processes for accepting, processing, and retaining cardholder data (card number, cardholder name, security code, personal identification number, etc.). Cardholder data security has become a priority for the major payment card brands leading them to form their own association to establish and regulate security standards for all merchants and service providers (users). The current version, Payment Card Industry Data Security Standard (PCI DSS) version 1.2, became effective October 1, 2008. The PCI DSS is comprised of twelve overarching standards, broken down into numerous smaller elements resulting in a very complex set of requirements.

Every method for accepting, processing, or retaining cardholder data introduces the potential for unauthorized access to cardholder data, more commonly known as a data breach. Based on our audit work, we did not identify any known data breaches with regard to cardholder data. However, lack of controls increase the potential for a data breach. Based on current information, the costs of a cardholder data breach can be high. As a result, we identified a need to review existing agency controls related to security of cardholder data.

Cost Associated With Data Breach

Current information suggests the average total cost of a data breach now exceeds $7 million per organization. The total cost to an organization is comprised of several categories including:

- detecting the data breach
- escalation (reporting the breach to the proper authorities)
- notification and response to cardholders who may have had their data stolen
- legal, investigative, and administrative expenses

- customer defection (purchasing from another merchant)
- opportunity loss (loss of revenue from potential customers)
- reputation management (public relations and damage control)
- additional expenses related to customer support such as information hotlines and credit monitoring
- expenses related to upgrading and more stringent monitoring of data security

While the average cost of a breach is significant, there are breaches that have cost organizations substantially more. In July 2005 a national retailer suffered a data breach resulting in the release of personal information on 450,000 customers. To date, the estimated total costs associated with the breach stand at nearly $1 billion including; the costs of fraudulent transactions, a class action lawsuit for gross negligence, and a $24 million settlement to one of the card brands. Governments are not immune from data breaches or their associated costs. In May 2006 a federal agency experienced a data breach as a result of a laptop stolen from a subcontracted employee's home. A settlement reached with the 26 million affected citizens will cost the Federal government $20 million. In addition to direct costs, an organization may lose its ability to accept certain card brand's payment cards.

Background

Payment card transactions are approved by processing vendors contracted by the State of Montana. The State has two contracts for processing vendors: one with Montana Interactive LLC (MI), and the other with First Data L.P. (First Data). MI is the vendor for the State of Montana web portal (mt.gov) and First Data is the primary vendor for most other forms of payment card transaction approvals.

The largest single method for accepting payment cards is through the State's MI managed web portal. The portal accounted for over $219 million in fiscal year 2008, or more than 73 percent of all revenues received through payment card transactions. Montana Interactive, as the state's web portal developer, has been certified as compliant with the PCI DSS by two independent auditing firms, including an industry recognized Cybertrust certification.

First Data is certified compliant with the PCI DSS as a processing vendor. The State of Montana, through the Department of Administration (DOA), has an exclusive term contract with First Data. The contract:

- incorporates, by reference, the Request for Proposals used to procure credit card processing services, which states "it is the individual agency's responsibility to comply with the terms of the contract"

- contains a provision which requires the State to "…comply with all security standards and guidelines that may be published from time to time by Visa, MasterCard or any other Association"

The security standard issued by the Payment Card Industry Security Council is the PCI DSS; therefore based on the above contract provisions, it is the responsibility of each agency to comply with the provisions contained within the PCI DSS.

Audit Objectives

Our audit objective was to determine if policies and business processes at selected entities conform to specific requirements of the PCI DSS.

Audit Scope and Methodology

The audit was conducted in accordance with Government Auditing Standards published by the United States Government Accountability Office. We reviewed state law, enterprise security policies', and the PCI DSS for criteria. The PCI DSS contains the only specific criteria related to the control environment.

First Data processed over $80 million in credit card transactions during fiscal year 2008. We identified four agencies or universities which accounted for nearly 92 percent of all revenues and 88 percent of all transactions processed under the First Data contract: The University of Montana-Missoula (UM), Montana State University-Bozeman (MSU), Montana State University-Billings (MSUB) and the Montana Department of Transportation (MDT), hereinafter referred to as "agencies". While our work focused on these four agencies, any state agency using DOA's term contract for payment card services can benefit from this work. We did not perform any additional audit work with regard to the state web portal or MI.

Payment card information is obtained by the four agencies in three ways: paper-based transactions (hand-written forms), point of sale (POS) devices (payment card information transmitted electronically), and web applications (card information entered through an internet web page). Through the contract with First Data, agencies are given discretion regarding which method(s) work best for their needs. We reviewed all three methods of obtaining payment card information for all four agencies.

Per the PCI DSS, once payment card information is received by an agency it must be processed, then destroyed or stored appropriately. Each stage of a payment card transaction is governed by standards contained within the PCI DSS. The specific PCI DSS elements used for this audit were selected based on payment card business processes in place at the agencies we audited.

We interviewed management and staff within individual departments at UM, MSU, MSUB, and MDT. Interviews discussed departmental or unit procedures for handling payment card information. In addition to interviews, we conducted observations of business processes and the office environments where payment card transactions are conducted and cardholder data is stored.

CONCLUSION

Due to the sensitive nature of cardholder data, specific details of our findings were shared with the agencies directly. The findings in this report have been generalized to protect cardholder data. However, based on our audit work, we conclude policies and business processes at the four agencies provide limited controls, and can be strengthened to meet specific elements of the Payment Card Industry Data Security Standard.

Potential Issue for Future Audit Work—Contract Management

During the course of this audit, we identified an issue related to contract management with potential for future audit work. DOA is statutorily responsible for governing the procurement of supplies and services obtained by the state. As mentioned previously, DOA has an exclusive term contract for procurement of credit card processing services. This exclusive term contract was negotiated and signed by DOA, but any state government entity may procure credit card processing services under the contract. While we determined ultimate responsibility for compliance rests with the entities utilizing the contract, DOA shares some responsibility for adherence to contract terms, including communication of contract provisions. As noted later in the report (page 9) there was a lack of awareness of the specific requirements of the PCI DSS; however, this audit did not address contract management or distribution of responsibility with regard to contract terms. Future audit work could include a review of the Montana Procurement Act (Title 18, Chapter 4) and DOA responsibilities for communicating contract expectations and monitoring contract compliance.

Chapter II – PCI DSS Requirements and Issues

Introduction

The Payment Card Industry Data Security Standard (PCI DSS) addresses security concerns by requiring merchants (agencies) to develop policies and implement business processes to handle payment cardholder data in a secure manner. Any agency using the state contract for credit card processing services, is required by the contract to follow the provisions contained within the PCI DSS.

Based upon the business processes in place at The University of Montana-Missoula, Montana State University-Bozeman, Montana State University-Billings, and the Montana Department of Transportation, we selected specific PCI DSS elements for this audit. Our audit examined payment card applications and associated cardholder data in three general areas: processing and storage of cardholder data, point of sale (POS) security, and web-based applications. The specific requirements we reviewed are detailed in the following sections.

Processing and Storage of Cardholder Data

Many of the requirements of the PCI DSS address processing and storage of cardholder data. Merchants must process payment card transactions in a secure manner. If a merchant requires any cardholder data be retained, it must be stored in a manner that allows access by authorized personnel only. The PCI DSS elements discussed in this section address these requirements.

Data Retention Policy

Requirement 3.1 of the PCI DSS states:

> *"Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy."*

As stated in Chapter I, the PCI DSS was developed to protect agencies from a cardholder data breach. Policy provides the foundation for data security. We asked agency management to provide policy specifically related to the handling of payment cards or cardholder data. Based on suggested testing procedures in the PCI DSS, we reviewed the information provided by the agencies to determine policy provisions for:

- retention of cardholder data
- disposal of cardholder data when no longer needed
- storage of cardholder data
- programmatic (automatic) removal of stored cardholder data

Two agencies stated no payment card policy existed. Policy at one of the other agencies specifically addressed payment card handling; however, it did not address specific details required by the PCI DSS. In particular this policy:

- contained some requirements for retention of cardholder data; however, these neither addressed payment card forms, nor defined a "secure location".
- contained provisions for storage of cardholder data; however, it did not define specific circumstances requiring storage of cardholder data nor specify what kind of cardholder data can be stored.
- did not include specific requirements for the programmatic removal of stored cardholder data.

The fourth agency had related policy which provided guidance for handling sensitive information and the retention of documents containing confidential information. Although this policy included some provisions regarding payment cards, it did not address important aspects for handling cardholder data. Specifically this policy:

- did not contain specific provisions for the retention of cardholder data.
- did not define "confidential information" nor state when, or under what circumstances, this information should be destroyed.
- did not define under what circumstances restricted cardholder data should or could be stored or accessed, nor provide guidance with regard to the secure storage of cardholder data.
- did not provide for the programmatic removal of stored cardholder data.

Storage of Sensitive Authentication Data

Requirement 3.2 of the PCI DSS states:

> *"Do not store sensitive authentication data after authorization (even if encrypted)." The PCI DSS defines sensitive authentication data as "Security-related information (card validation codes/values, full magnetic-stripe data, PINs (personal identification numbers), and PIN blocks) used to authenticate cardholders, appearing in plain-text or otherwise unprotected form".*

Sensitive authentication data verifies the identity of the cardholder and the validity of the card number. Having this information could allow unauthorized individuals to conduct fraudulent transactions. We reviewed the four agencies for storage of sensitive authentication data. Of the four, we identified concerns at two. Each of the two agencies has two departments storing sensitive authentication data, specifically the card validation code or value along with other cardholder data, one on handwritten forms or notes, such as yellow sticky notes, the other on system generated forms. These agencies' policies and procedures did not conform to the PCI DSS which specifically prohibits the storage of sensitive authentication data.

Securing Primary Account Numbers

Requirement 3.3 of the PCI DSS states:

"Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed)."

According to the standard, the primary account number (PAN) must be masked (hidden) on computer screens, paper receipts and other media except to those with a legitimate business need to see the full PAN. Should unauthorized individuals obtain the PAN, they could have the ability to conduct fraudulent transactions.

We reviewed the four agencies to determine if they were properly masking the PAN from those without a legitimate business need to see it. We identified concerns at each of the four agencies. Twelve individual departments of the agencies we reviewed did not mask the PAN as required. Specifically:

- nine departments had the PAN on forms used to process payment card transactions. These forms either did not have the PAN masked as required or the masking was not sufficient. The procedures in place in the departments left the forms visible to those without at business need to see the PAN, including other customers.
- three departments were printing detail reports from point of sale devices. These reports contain the full, unmasked PAN. Detail reports were then forwarded to other departments through interoffice mail for additional processing and storage. Prior to storage the PAN was not masked and the reports were stored with other documents unrelated to payment cards. Staff searching through the stored documents often did not have a business need to see the full PAN.

Restricting Access to Cardholder Data

Requirements 7 and 9 of the PCI DSS are similar in nature and are combined for the purposes of this report and state respectively:

"Restrict access to cardholder data by business need to know."
"Restrict physical access to cardholder data."

Restricting access to cardholder data reduces the risk of a cardholder data breach. We reviewed the four agencies to determine if they were limiting access to cardholder data in accordance with these two requirements. We identified concerns at all four agencies.

Our concerns fit into two categories: those associated with the payment card transactions, and those associated with the storage of cardholder data. Four individual departments processed payment card transactions in an open office environment.

Individuals, such as customers or staff from other departments not authorized to view or have access to cardholder data, are allowed access to the offices and can move about freely. Documents containing cardholder data were in locations visible to any individual in the office. Access controls such as locks on doors or visitor and staff identification are either not present or insufficient.

Five individual departments stored cardholder data in an unsecure manner. Documents were kept on desktops or countertops, or in unlocked file cabinets. The offices where these documents were kept were usually locked. However, in each instance, janitorial or maintenance staff had unmonitored access to the offices after regular business hours. Other documents were placed in long term storage facilities where individuals from other departments or functions had unmonitored access.

None of the agencies had procedures in place to monitor or record access to stored cardholder data.

Point of Sale Inventory

Requirement 12.3 of the PCI DSS mandates the development of:

"usage policies for critical employee facing technologies…"
and the usage policy should include *"a list of all such devices…"*

Critical employee-facing technologies are those technologies, such as POS devices, used directly by agency staff for the processing of cardholder data. We reviewed agency use of POS devices against requirement 12.3. POS devices allow a payment card to be swiped through a magnetic stripe reader and transmit cardholder and transaction information to the acquiring bank. We only reviewed POS devices that are also pin entry devices (PED). These devices allow the cardholder to enter a personal identification number (PIN) to authenticate the payment card. Because some of these devices retain cardholder data and can be reportedly compromised, agencies should maintain an accurate accounting of these devices.

Of the four agencies we reviewed, two had lists of the departments using POS devices and the number of devices at each department. The lists provided by the two agencies were neither complete nor accurate; therefore, they did not list "all such devices". They did not contain details specifically identifying each device at each location. Based on our observations, these two agencies had POS devices in use in departments that were not listed, and devices with incorrect model numbers on the list. The other two agencies did not have POS lists.

None of the four agencies had any usage policies in place which address critical employee-facing technologies.

Summary

Based on our audit work, we conclude agency policy and business processes do not conform to specific elements of the PCI DSS related to processing and storage of cardholder data for the following reasons:

- Policy regarding the handling of payment cardholder information either does not exist or does not completely address requirements.
- Sensitive authentication data is being stored after authorization.
- The primary account number (PAN) is not always being properly masked from those without a business need to view it.
- Access to cardholder data is not being limited effectively to those with a business need to know, and overall physical access to stored cardholder data is not properly restricted.
- Lists of all POS devices in use are either not kept or are incomplete.

Lack of controls in these areas could lead to unauthorized access to cardholder data. Any unauthorized individual obtaining cardholder information contained on payment forms or other documents would have some or all of the necessary elements to fraudulently conduct payment card transactions. This could result in losses to cardholders that vary in scope based on factors such as the number of cards stolen, dollar limit on the cards, etc. These costs may become the responsibility of the state due to legal action. According to current information direct costs associated with a data breach in the United States averaged more than $7 million in 2008. However, costs for some of these breaches are nearing $1 billion. Ultimately, continued failure to comply with the PCI DSS could result in the loss of the privilege to accept payment cards.

Agency management is responsible for ensuring agency compliance with any state term contract they are a party to. This responsibility includes obtaining all related contract documents and noting and following any specific requirements. In this case, the contract requires agencies to conform to the standards issued by the payment card industry which is the PCI DSS. Because agency management was not fully informed of the specifics of the PCI DSS, they were unable to provide specific guidance to agency personnel, either written or verbal, for properly handling cardholder data. Additionally, given the decentralized nature of payment card processing at the four agencies, monitoring the procedures being used by individual departments was limited.

RECOMMENDATION #1

We recommend the four agencies comply with the contract by:

A. *Developing and implementing specific payment card data security policies which include:*
   - *Cardholder data retention*
   - *Storage of sensitive authentication data*
   - *Securing (masking) primary account numbers*
   - *Restricting access to cardholder data*
   - *Completing and tracking an inventory of all point of sale devices*

B. *Formally communicating specific payment card data security policies to staff to increase awareness at the departmental level.*

C. *Formally monitoring the implementation of payment card data security policies.*

Point of Sale (POS) Security

The majority of non web based payment card transactions are processed through a POS device. Transactions where the payment card is present are conducted by swiping the card through the POS device. The cardholder information is read by the device, the transaction information is hand keyed, and the data is transmitted to the processing vendor for authorization. Agencies can also accept payment card transactions where the card is not physically present. In these instances the card information is hand keyed into the device for transmission.

POS Encryption

Requirement 4.1 of the PCI DSS states:

> *"Use strong cryptography and security protocols... to safeguard sensitive cardholder data during transmission over open, public networks".*

Encryption is the scrambling of data rendering it unreadable to unauthorized parties. During our audit we reviewed POS devices in use by the four agencies. At each of the agencies, we identified POS devices that may not be encrypting data as required by the PCI DSS. We spoke with agency management, the processing vendor (First Data), and with the manufacturers of the POS devices in question. We confirmed at least two models of POS devices currently in use by three of the agencies are unable to encrypt cardholder data.

Our audit work also identified one model of POS device that can reportedly be compromised. The device stores cardholder data for a period of time and the data is not encrypted. It allows any individual with knowledge of the device's master password codes to obtain saved payment card data from the memory of the device. The instructions to obtain the master passwords are readily available to the public.

Summary

Based on our audit work, we conclude the four agencies are using POS devices which do not conform to the PCI DSS requirement related to safeguarding cardholder data during transmission.

Unencrypted cardholder data can be obtained by unauthorized individuals when transmitted over an open, public network or through a physically compromised device. The definition of an "open, public network" and whether it applies to a transmission over a public telephone network is unclear. We inquired as to the specific inclusion of telephone networks and received no clarification. In the interest of cardholder data security, we have taken a conservative approach that data should be encrypted, no matter how it is transmitted. Without encryption, cardholder data could then be used to conduct fraudulent transactions. The reportedly compromised models could be removed from the agency or tampered with if not monitored. Individuals who could remove the device or gain unmonitored access would be able to obtain the master password. Individuals with enough knowledge would then be able to obtain all the cardholder data stored in the device memory. Once traced back to the agency responsible for the data, the agency is faced with the costs associated with a data breach as described in the previous section.

Agency management were unaware the POS devices in use were not encrypting cardholder data, nor were they aware of PCI DSS requirement 4.1. Also, management relies on the difficulty of obtaining payment card data from one agency phone connection among many other phone calls. This does not comply with the PCI DSS as the data would still be compromised in a data breach involving cardholder data transmitted via phone lines. Management was also unaware of the weaknesses of the model that could be compromised.

According to an estimate provided by management at one of the four agencies, it will cost approximately $25,000 to replace all POS devices which do not encrypt data. Although the costs associated with replacing POS devices may be significant, the cost of a data breach could far exceed the cost of replacement and, the contract requires agencies to conform to the PCI DSS.

RECOMMENDATION #2

We recommend the four agencies ensure all point of sale devices encrypt cardholder data as required by the Payment Card Industry Data Security Standard.

Web Based Applications

Web based applications provide agency customers with the ability to purchase services or pay bills using the Internet. Such applications provide customers with the convenience of making their purchase anywhere they can access the Internet. These applications also allow agency staff to perform their duties from remote locations throughout the state. While convenient and efficient, these applications are targeted for obtaining cardholder information. The PCI DSS requires merchants to ensure any web based applications they use were developed in accordance with the PCI DSS.

Web Application Compliance

Requirement 6.3 of the PCI DSS states:

> *"Develop software applications in accordance with PCI DSS… and based on industry best practices…"*

All of the web based applications we reviewed for this audit were developed by third party contracted vendors. We understand this requirement to mean state agencies must ensure that application developers meet the requirements of the PCI DSS.

The PCI Security Council has two lists showing either vendors (developers) or applications that are PCI DSS compliant. We reviewed 10 separate web based applications in use by the four audited agencies. Each of these applications was developed and is maintained by vendors who are PCI DSS certified compliant.

CONCLUSION

Based on our audit work, we conclude these four agencies are using web application developers who are compliant with the PCI DSS.

Department and University Responses

The University of Montana-Missoula

Montana State University-Bozeman

Montana State University-Billings

Department of Transportation

The University of Montana

Office of the President
The University of Montana
Missoula, MT 59812-3324
Office: (406) 243-2311
FAX: (406) 243-2797

9 June 2009

Ms. Tori Hunthausen
Legislative Auditor
Legislative Audit Division
Room 135 State Capitol
P. O. Box 201705
Helena, MT 59620-1705

Dear Ms. Hunthausen:

We thank the Legislative Audit staff for the professional work on the Payment Card Industry Security Standard and Related Controls Information System Audit. The Audit staff brought important security and control issues to our attention. Please know that we of The University of Montana will address those issues as indicated in the attached response to the audit report. We appreciate the cooperative efforts made by the audit team and thank those involved for their assistance.

Sincerely,

George M. Dennison

George M. Dennison,
President

GMD/kc
Denlet3953

c: S. Stearns, Commissioner of Higher Education

The University of Montana - Missoula

Response to Legislative Audit Division –Payment Card Industry Data Security Standards and Related Controls

Information Security Audit

May 2009

RECOMMENDATION #1

WE RECOMMEND THE FOUR AGENCIES COMPLY WITH THE CONTRACT BY:

A. DEVELOPING AND IMPLEMENTING SPECIFIC PAYMENT CARD DATA SECURITY POLICIES WHICH INCLUDE:

- Cardholder data retention
- Storage of sensitive authentication data
- Securing (masking) primary account numbers
- Restricting access to cardholder data
- Completing and tracking an inventory of all point of sale devices

B. FORMALLY COMMUNICATING SPECIFIC PAYMENT CARD DATA SECURITY POLICIES TO STAFF TO INCREASE AWARENESS AT THE DEPARTMENTAL LEVEL.

C. FORMALLY MONITORING THE IMPLEMENTATION OF PAYMENT CARD DATA SECURITY POLICIES.

The University of Montana concurs with the recommendations. University personnel will revise current credit card policies and procedures to insure that we include all relevant PCIDSS elements. Staff will distribute the revised policies to applicable departments across campus by 30 September 2009. University personnel will implement a formal monitoring program in conjunction with the new policies and procedures.

RECOMMENDATION #2

WE RECOMMEND THE FOUR AGENCIES ENSURE ALL POINT OF SALE DEVICES ENCRYPT CARDHOLDER DATA AS REQUIRED BY THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD.

The University of Montana concurs with the recommendation. The University will replace the POS devices by 30 September 2009. In addition, the University will establish compensating controls to mitigate the risk prior to replacing the machines.

MONTANA
STATE UNIVERSITY
BILLINGS

Access & Excellence

Office of the Chancellor

June 8, 2009

Kent Rice
IS Audit Manager
Legislative Audit Division
State Capitol Building
Helena, MT 59620-1705

Dear Mr. Rice:

Montana State University Billings has reviewed and discussed the findings in your audit report on the Payment Card Industry Data Security Standards (PCI DSS) and related controls. MSU Billings does understand the importance of PCI DSS and we emphatically are committed to ensuring the security of our customer information.

Recommendation #1 – Concur

A. – MSU Billings will develop and implement a policy that covers all points addressed by the end of the calendar year.

B. – MSU Billings will train departmental personnel on the provisions of the policy in the same timeline.

C. – MSU Billings will monitor the policy implementation within the aforementioned timeline.

Recommendation #2 – Concur

MSU Billings will ensure encryption of data as soon as possible once a new credit card processing provider has been finalized and all communications lines with said provider are open.

Thank you for your time and efforts in this matter.

Sincerely,

Ronald P. Sexton, Ph.D.
Chancellor

MONTANA
STATE UNIVERSITY

June 5, 2009

RECEIVED
JUN 09 2009
LEGISLATIVE AUDIT DIV.

Ms. Tori Hunthausen
Legislative Auditor
Legislative Audit Division
Room 160, State Capitol
P.O. Box 201705
Helena, MT 59620-1705

Dear Ms. Hunthausen:

Enclosed you will find Montana State University's response to the recommendations outlined in the narrative segment of the final report on the Information Systems audit of the Payment Card Industry Data Security Standard and Related Controls.

Montana State University appreciates the efforts of the Legislative Audit Division in regards to this audit and its identification of areas for continued improvement.

Sincerely,

Geoffrey Gamble
President

Enclosure

Office of the President
211 Montana Hall
P.O. Box 172420
Bozeman, MT 59717-2420
www.montana.edu

Tel (406) 994-2341
Fax (406) 994-1893

MONTANA STATE UNIVERSITY
Response to Legislative Audit Division Recommendations
Payment Card Industry Data Security Standard and Related Controls

The security of credit card data, as well as other personally identifiable information, is of great concern to Montana State University (MSU). MSU has long had a credit card data security policy in place. Management intends to implement recommendations to strengthen its policy as soon as possible, has already implemented certain improvements, and will implement the remainder by June 30th, 2009. Specific to the recommendations of the legislative auditor:

RECOMMENDATION #1

We recommend the four agencies comply with the contract by:

A. *Developing and implementing specific payment card data security policies which include:*

- *Cardholder data retention*
- *Storage of sensitive authentication data*
- *Securing (masking) primary account numbers*
- *Restricting access to cardholder data*
- *Completing and tracking an inventory of all point of sale devices*

B. *Formally communicating specific payment card data security policies to staff to increase awareness at the department level.*

C. *Formally monitoring the implementation of payment card data security policies.*

MSU concurs with the recommendation.

A. MSU will:
   a. Clarify in its policy that data retention, storage, and access must be in compliance for all credit card payment forms as well as for credit card receipts. The policy currently specifies such for credit card receipts but is silent as to the handling of payment forms filled out by students (or staff, in the case of telephone payments).
   b. Specifically describe in policy what constitutes secure storage.
   c. Ensure that the machine that does not mask account numbers is retired, and that any remaining data from such machine is destroyed.
   d. Maintain an inventory of all point of sale devices.

B. MSU will formally communicate the requirements of its revised payment card data security policy to staff to increase awareness at the department level at its fall 2009 training workshops as well as through email communications to staff and through the campus-wide policy review process.

C. MSU management and internal audit will formally monitor the implementation of payment card data security policies.

RECOMMENDATION #2

We recommend the four agencies ensure all point of sale devices encrypt cardholder data as required by the Payment Card Industry Data Security Standard.

MSU concurs with the recommendation.

MSU will ensure that all of its point of sale devices encrypt cardholder data as required by the Payment Card Industry Data Security Standard.

serving you with pride

Montana Department of Transportation
2701 Prospect Avenue
PO Box 201001
Helena MT 59620-1001

Jim Lynch, Director
Brian Schweitzer, Governor

June 9, 2009

RECEIVED
JUN 09 2009
LEGISLATIVE AUDIT DIV.

Tori Hunthausen, Legislative Auditor
Legislative Audit Division
State Capitol Room 160
Helena, MT 59620-1705

Subject: Payment card industry data security standard and related controls

Dear Tori,

Thank you for giving the Montana Department of Transportation (MDT) an opportunity to respond to the information systems audit performed by your office for payment card industry data security standard and related controls.

We have attached our response including a management action plan. I appreciate your staff's effort, cooperation, and professionalism during this audit. MDT is committed to complying with state and federal laws, and implementing and maintaining effective accounting controls.

If you have any questions or comments regarding this audit, please feel free to contact me.

Sincerely,

Jim Lynch
Director

attachments

copies: John Blacker, Deputy Director
Mike Bousliman, Chief Administrative Officer
Larry Flynn, Administration Division Administrator

Montana Department of Transportation

LAD Audit Recommendations and Agency Responses

Recommendation #1

We recommend the four agencies comply with the contract by:

A. Developing and implementing specific payment card data security policies which include:
   - Cardholder data retention
   - Storage of sensitive authentication data
   - Securing (masking) primary account numbers
   - Restricting access to cardholder data
   - Completing and tracking an inventory of all point of sale devices

B. Formally communicating specific payment card data security policies to staff to increase awareness at the departmental level.

C. Formally monitoring the implementation of payment card data security policies.

Response

Concur

The department was not informed by The Department of Administration (Dof A) or aware of the PCI DSS requirements. DofA needs to inform MDT and other agencies when there are any changes to term contract requirements that impact the agencies. MDT has installed electronic card readers in both the records retention and mailroom areas to control physical access to the records. MDT will work with DofA to establish procedures to comply with the recommendations above and will communicate procedures to staff and monitor those procedures. MDT will continue to monitor and implement any changes to policies.

Recommendation #2

We recommend the four agencies ensure all point of sale devices encrypt cardholder data as required by the Payment Card Industry Data Security Standard.

Response

Concur

MDT will work with the new credit card vendor to ensure all point of sale devices are encrypted.

Management Action Plan - LAD Audits
MDT Information Systems Audit
Payment Card industry Data Security Standard and Related Controls 6/9/2009

Audit Recommendation #	Management View	Corrective Action Plan	Responsible Area	Target Date
Recommendation #1 We recommend the four agencies comply with the contract by: A. Developing and implementing specific payment card data security policies which include: • Cardholder data retention • Storage of sensitive authentication data • Securing (masking) primary account numbers • Restricting access to cardholder data • Completing and tracking an inventory of all point of sale devices B. Formally communicating specific payment card data security policies to staff to increase awareness at the departmental level. C. Formally monitoring the implementation of payment card data security policies.	Concur	The department was not informed by DofA or aware of the PCI DSS requirements. DofA needs to inform MDT and other agencies when there are any changes to term contract requirements that impact the agencies. MDT has installed electronic card readers in both the records retention and mailroom areas to control physical access to the records. MDT will work with DofA to establish procedures to comply with the recommendations above and will communicate procedures to staff and monitor those procedures. MDT will continue to monitor and implement any changes to policies.	Mike Bousliman, Chief Administrative Officer, Larry Flynn, Administrative Division Administrator	12/31/2009
Recommendation #2 We recommend the four agencies ensure all point of sale devices encrypt cardholder data as required by the Payment Card Industry Data Security Standard.	Concur	MDT will work with the new credit card vendor to ensure all point of sale devices are encrypted.	Mike Bousliman, Chief Administrative Officer	12/31/2009