

University of Missouri Point of Sale System Security Guide





University of Missouri Point of Sale System Security Guide

Office of the Treasurer

<http://www.umsystem.edu/ums/departments/fa/treasurer/>

This guide is targeted at Point of Sale systems that verify transactions via the commodity Internet.



University of Missouri Point of Sale System Security Guide

Office of the Treasurer

<http://www.umssystem.edu/ums/departments/fa/treasurer/>

Point of Sale Definitions

Point of Sale Data: Data used in the establishment, processing, and fulfillment of purchases. This includes, but is not limited to

- Customer Name
- Customer Contact Information
- Customer Shipping Information
- Order Details
- Order fulfillment Information

Restricted Point of Sale Data: Data specifically protected by the Payment Card Industry Standard and/or the National Automated Clearing House Association (NACHA), and can not be stored on departmental equipment.

- Credit Card Number
- Credit Card Vendor
- Credit Card Verification Number
- Credit Card Expiration Date
- Check Number
- Checking Account Number
- Check Routing Number



University of Missouri Point of Sale System Security Guide

Office of the Treasurer

<http://www.umsystem.edu/ums/departments/fa/treasurer/>

Security Standards for Point of Sale Systems Verifying Transactions via the Internet

Network Requirements	Notes and Reference Documents	Acceptable Verification Method	PCI Section
POS Terminals shall not be allowed to connect directly to the internet	The network configuration should include a private network for POS Terminals. This network should only allow connectivity to the system's transaction processing server, and any management systems required by the terminals such as WSUS or Norton Anti-Virus servers.	network diagram, network mapping software	1.1.6; 1.2; 1.3; 1.4; 1.5
Server and POS terminals shall be isolated from other hosts by a network layer firewall that allows access to specified ports on a least privilege basis	The network configuration should include a hardware firewall with explicit rules tuned to the services and ports needed by the server. Typically this will consist of web service ports 80 and 443 open to the entire Internet and remote administration ports for SSH or Terminal Services open to specified IP addresses or ranges.	network diagram, network mapping software	1.1.3; 1.2; 1.3; 1.4; 1.5
Server and POS terminals shall be logically connected to the network with an IDS or IPS system between it and the commodity Internet	The network configuration should show the use of a network based intrusion detection or intrusion prevention system between the server and the commodity Internet. This is typically already installed on campus networks as a part of the network intra-structure team's defense in depth.	network diagram, network mapping software	11.4
POS Terminals that utilize a wireless network must use a high level of encryption.	At a minimum the wireless network for a POS system must have a separate hidden SSID, have traffic limited as stated above, and at least use WPA/PSK and if possible use at least OS level IPSEC encryption as well.	Manual inspection of configuration	4.1.1
Physical Security Requirements			
Physical access to the server shall be limited to authorized individuals with physical controls and access shall be monitored 24x7	This requirement must be met by housing the system in a campus datacenter.	physical inspection of facilities	9.1; 9.2; 9.3; 9.4
Data Access Requirements			
Data access shall be limited to authorized individuals on a least privilege basis	Only the bare minimum permissions to accomplish any given task in the system should be granted on an individual basis.	manual inspection of system/application authorization lists	7.1; 7.2;
Authentication is required for systems administration, data manipulation, and access to reports	All individual administrators, data entry personnel or other staff with a business need to access the Point of Sale Data must use at least a unique username and password to access the system. All vendor default passwords must be changed.	manual inspection of access controls	8.1; 8.2; 8.5.8; 2.1
Passwords used in the system must meet common security requirements.	Passwords must be at least 7 characters, include numeric and alphabetic characters. After 6 failed password attempts users should be locked out for 30 minutes or until an administrator intervenes. Passwords should be changed every 90 days and the	Manual inspection of password requirements	8.5.9-15



University of Missouri Point of Sale System Security Guide

Office of the Treasurer

<http://www.umsystem.edu/ums/departments/fa/treasurer/>

	user should not be able to choose any of the last 4 passwords used for the account. After 15 minutes of inactivity terminals should lock themselves.		
Transmission of data shall be via secure protocols	Point of Sale data should use a secure protocol for transmission across the network. Most often, this is done over the web using Secure Socket's Layer encryption. Point of Sale data should not be sent via email, except in the case where the customer enters an email address by which they can receive order details.	manual inspection of communication protocols	4.1; 4.2
Granting Permission and Access Levels			
Granting access to Point of Sale data shall require organizational supervisory authority	The business owner of the Point of Sale system must provide written approval of all new grants of permission of Point of Sale data.	inspection of questionnaire	9.2; 9.3
All users who access Point of Sale data shall be required to sign the Confidentiality Agreement	At the time access is granted the business owner must ensure the confidentiality agreement has been signed.	inspection of questionnaire	12
Storage Requirements			
Point of Sale data shall be stored on a secure server not on individual POS terminals.	Staff must be informed of the sensitivity of the data, and that it may not be stored on individual workstations, personal data assistants, or removable media.	network diagram, system description	9
Training Requirements			
Security awareness training shall be required for all staff with access to administer the system, manipulate data, or generate reports	Educate employees on hire and at least annually (for example, by letters, posters, memos, meetings, and promotions)	Inspection of security awareness training records	12.6
Data Disposal Guidelines			
Software shall be used to write over all sectors of the hard drive multiple times when the system is decommissioned	This should be ensured prior to delivery to University procurement for disposal.	inspection of questionnaire	9.10
System Security Guidelines			
System Administration and Application Development Best Practices shall be used in development, implementation, and maintenance of the system	Operating system or development platform specific security guidelines must be followed when developing the system. The following is a list of guidelines appropriate for use for a number of different platforms. IAT Services Top 20 Audit Findings http://iatservices.missouri.edu/safeweb/docs/top-20-handout.doc System Security Guidelines Windows Server 2003: http://www.microsoft.com/technet/security/prodtech/window	automated verification of system configuration with vulnerability analysis software, and manual inspection	2.2;5.6.1



University of Missouri Point of Sale System Security Guide

Office of the Treasurer

<http://www.umsystem.edu/ums/departments/fa/treasurer/>

	<p>sserver2003/w2003hg/sqch00.msp Red Hat Enterprise Linux 4 http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/security-guide/ MAC OS X Server http://images.apple.com/server/pdfs/Tiger_Server_Security_Config.pdf Cold Fusion Server Security Guide http://www.adobe.com/devnet/coldfusion/articles/cf7_security_print.html</p> <p>General Web Application Security Guidelines (applies to all languages deployed to the web) http://prdownloads.sourceforge.net/owasp/OWASPGuide2.0.1.pdf?download PHP Security Guide http://phpsec.org/projects/guide/ C# Security Guide http://msdn2.microsoft.com/en-us/library/ms173195(VS.80).aspx</p> <p>(Note this is not an exhaustive list of all possible system components. If a guide for a specific component is not listed please contact the Treasurer's office to gain assistance in finding an appropriate guide.)</p>		
Remote Administration Requirements			
Restricted to local network and secure VPN pool	The system should restrict access to remote administration services to trusted networks.	automated verification of system configuration with vulnerability analysis software	2.3
Backup/Disaster Recovery			
Backups shall be performed daily		manual Inspection of system configuration	
A minimum of three levels of backup history shall be maintained		manual Inspection of system configuration	
At least one copy of the backup should be stored locally and one should be stored off-site		inspection of internal documents	9.5
Copying/Printing			
Point of Sale data shall only be printed when a hard copy is required		inspection of internal documents	9.6



University of Missouri Point of Sale System Security Guide

Office of the Treasurer

<http://www.umsystem.edu/ums/departments/fa/treasurer/>

Copies shall be limited to individuals who are authorized to view the information and have signed a confidentiality agreement		inspection of internal documents	9.7; 12.6.2
Point of Sale data shall not be sent to an unattended printer or left sitting on a printer		inspection of internal documents	9.6
Copies shall have a cover sheet indicating that the data is restricted		inspection of internal documents	9.7
All receipts shall mask the credit card number.		Inspection of receipt generated by system	3.3
Staff Requirements			
Application development and systems administration duties shall be carried out by separate staff	It is strongly recommended that application staff should receive specialized training or have developed skills in securing computer systems and/or secure programming techniques.	inspection of internal documents	12
Database Requirements			
Databases shall be established on separate physical hardware from front-end systems		manual inspection of system configuration	
Databases shall have full transaction tracking and table level permission	Oracle and Microsoft SQL server are currently the preferred database platforms. Microsoft Access and other desktop database applications are not considered acceptable software for Point of Sale transactions.	manual inspection of system configuration	10
Audit Schedule			
The compliance of the entire system shall be verified yearly		inspection of audit databases for completeness and consistency	11
The compliance of application software shall be verified on each major code revision		automated verification of application configuration with vulnerability analysis software	11
The compliance of the entire system shall be verified on initial deployment		verify risk assessment, asset classification, and other audit documents are on file	11
The compliance of the operating system shall be verified monthly		automated inspection of system security measures	11



University of Missouri Point of Sale System Security Guide

Office of the Treasurer

<http://www.umssystem.edu/ums/departments/fa/treasurer/>

Point of Sale System Questionnaire

General Information

Site Name:
Merchant ID:
Department:
Campus:
Transactions / \$ per year:

System Supervisor

Name:
Title:
Email Address:
Contact Telephone:
After Hours / Emergency Telephone:
Campus Address:

System Administrator

Name:
Title:
Email Address:
Contact Telephone:
After Hours / Emergency Telephone:
Campus Address:

POS Vendor Contact

Name:
Title:
Email Address:
Contact Telephone:
After Hours / Emergency Telephone:
Campus Address:

Custom Application Developer

Name:
Title:
Email Address:
Contact Telephone:
After Hours / Emergency Telephone:
Campus Address:



University of Missouri Point of Sale System Security Guide

Office of the Treasurer

<http://www.umssystem.edu/ums/departments/fa/treasurer/>

Custom Application Information

Application Description:
Language:
Version:
IDE:
Authentication Mechanism:
User Roles:
Application Entry Points:
Development Status:
Development Schedule:
User Documentation Present:
Design Documentation Present:

Transaction Server Information

IP Address(es):
DNS Name(s):
NetBios Name (if applicable):
Operating System:
Operating System Version (include major patch level):
System Dependencies:
POS Server Software:
POS Server Version:

POS Terminal Information

Operating System:
Operating System Version (include major patch level):
System Dependencies:
POS Terminal Software:
POS Terminal Version:

Physical Information

Server Building:
Server Room:
If not data center describe physical security measures:

Backup Information

Backup software:
Backup server (if remote):
Backup versions kept:
Backup copies kept:
Backup storage locations:



University of Missouri Point of Sale System Security Guide

Office of the Treasurer

<http://www.umsystem.edu/ums/departments/fa/treasurer/>

Internal Policy Supports the Following

Access to the system is limited to authorized individuals on a least privilege basis.

(y/n)

Access to the Point of Sale data shall require <Supervisors Name> approval.

(y/n)

All users who access Point of Sale data must sign a Confidentiality Agreement.

(y/n)

Point of Sale data will only be stored on the secure server and not an individual's machine.

(y/n)

All users will be required to attend Security Awareness training.

(y/n)

Point of Sale Data will only be printed when a hard copy is absolutely necessary.

(y/n)

Copies will be limited to authorized staff

(y/n)

Point of Sale Data cannot be sent to an unattended printer or left sitting on a printer

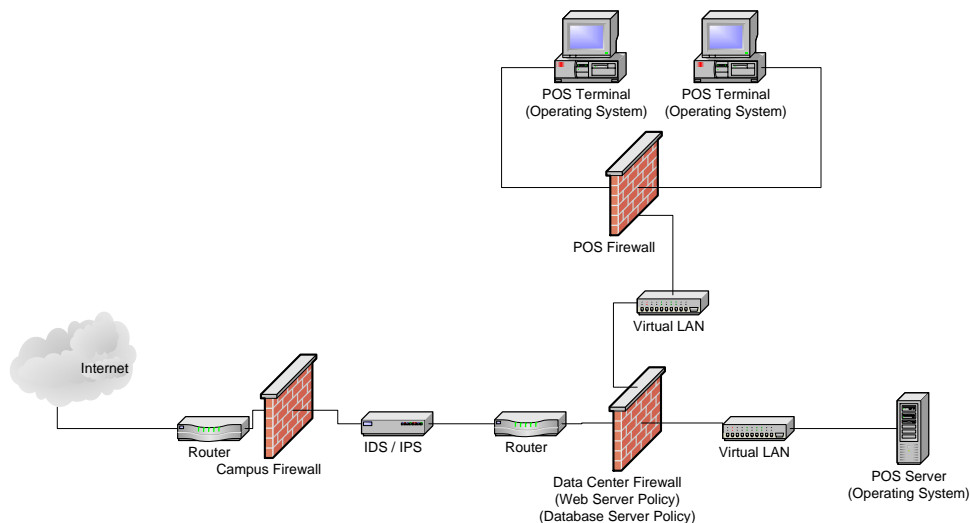
(y/n)

Copies of Point of Sale Data need to have a cover sheet indicating that the data is restricted

(y/n)

(note distribution of a memo / email similar to the one in Appendix 1 is sufficient to meet this requirement)

Network Diagram





University of Missouri Point of Sale System Security Guide

Office of the Treasurer

<http://www.umssystem.edu/ums/departments/fa/treasurer/>

Appendix:

Sample Departmental Point of Sale Memo

A message with the same major bullets should be sent by the Supervisor responsible for the system to all those who access the system.

To Whom It May Concern:

The <System Name> is being developed to meet the department's Point of Sale needs. This system is subject to significant regulation and campus policy. The University Standards for Point of Sale systems require the following procedures to be in place to protect the data our system will hold.

- Access to the system is limited to authorized individuals on a least privilege basis.
- Access to the data requires <Supervisors Name> approval.
- All users who access Point of Sale data must sign the Confidentiality Agreement.
- Point of Sale data will only be stored on the secure server and not the Point of Sale or individual computers.
- All users will be required to attend security awareness training.
- Point of Sale data will only be printed when a hard copy is absolutely necessary.
- Copies will be limited to authorized staff.
- Point of Sale data cannot be sent to an unattended printer or left sitting on a printer.
- Copies of Point of Sale e data need to have a cover sheet indicating that the data is restricted.

The system will be audited on an annual basis, so it is imperative that these procedures are followed at all times.

Sincerely

<Supervisor responsible for the departmental Point of Sale system>



University of Missouri Point of Sale System Security Guide

Office of the Treasurer

<http://www.umsystem.edu/ums/departments/fa/treasurer/>

University of Missouri Access and Confidentiality Agreement

As a faculty or staff member, consultant, volunteer or student at the University of Missouri you may learn of, or have access to, confidential information. This agreement will help you understand what confidential information is and what your responsibilities are.

Confidential information includes, but is not limited to:

- Student or personnel information--employment records, social security numbers, grades or other personally identifiable student information, performance evaluations, disciplinary actions, etc.
- Patient information--medical records, physician-patient conversations, admittance information, patient/member financial information, other personally identifiable health information, etc.
- Third party information—information protected by non-disclosure agreements or other contractual obligations.

In certain circumstances, the following may also be considered confidential information:

- University of Missouri information-- financial and statistical records, job applications, unpublished strategic plans, internal reports, memos, contracts, peer review information, communications, proprietary computer programs, source code, proprietary technology, etc.
- Copyrighted material and other intellectual property
- Third party information--computer programs, client and vendor proprietary information, source code, proprietary technology, etc.

Confidential information is valuable and sensitive. It is protected by law and by University of Missouri policies ([Collected Rules and Regulations, §110.005](#), [Business Policy Manual, §108](#).) The intent of these laws and policies is to assure that confidential information is used only as necessary to accomplish the organization's mission. You are required to conduct yourself in strict accordance with applicable laws and University policies regarding confidential information. As a condition, and in consideration, of your access to confidential information, you agree to:

1. Use confidential information only as needed to perform your legitimate duties
 - a. Only access confidential information which you need to know
 - b. Do not divulge, copy, release, sell, loan, review, alter or destroy any confidential information except as properly authorized
 - c. Do not otherwise misuse or treat carelessly confidential information.
 - d. Understand that you will be held responsible for your misuse, careless or wrongful disclosure of confidential information



University of Missouri Point of Sale System Security Guide

Office of the Treasurer

<http://www.umsystem.edu/ums/departments/fa/treasurer/>

2. Safeguard and prevent disclosure of your password and/or access code or any other authorization that enables access to confidential information. You will be held responsible for any failure to safeguard such passwords, codes or authorization.
3. Report activities to your supervisor that you suspect may compromise the confidentiality of information. Reports made in good faith, including your name, will be held in confidence to the extent permitted by law.
4. Abide by your obligations under this Agreement even when you are no longer affiliated with the University.
5. Understand that you have no right or ownership interest in any confidential information referred to in this Agreement.

I understand and agree that any violation of the responsibilities explained in this agreement will subject me to discipline, possible termination of employment or legal liability. I understand and agree that my privileges hereunder are subject to periodic review, revision and, if appropriate, renewal and that the University may revoke my access code, other authorization or access to confidential information at any time.

I further understand and agree that I have no right or ownership interest in any confidential information that I may have access to as part of my affiliation with the University and that my obligations to keep such information confidential will remain in effect even after my affiliation with the University ceases.

Faculty/Staff/Consultant/Student/Volunteer Signature

Date

Printed Name



University of Missouri Point of Sale System Security Guide

Office of the Treasurer

<http://www.umsystem.edu/ums/departments/fa/treasurer/>

Estimated Costs for Point of Sale Security Audits (provided by UM Division of Information Technology)

Audit Type	Hourly Charge	Average Time
Point of Sale E-commerce Audit (initial and yearly follow-up)	\$75	10-15 hours