

University of Missouri eCommerce Security Guide





University of Missouri eCommerce Security Guide

Office of the Treasurer

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

This guide is intended for use by those wishing to conduct eCommerce transactions within the University of Missouri. University of Missouri policy grants the Office of the Treasurer full responsibility and authority over financial transactions at the University. This extends to the realm of electronic commerce.

In recent years the major credit card corporations have formed a standard for electronic commerce system security known as the Payment Card Industry Data Security Standard (PCI DSS). The University has contracted with Nelnet to provide a PCI DSS compliant payment processing system called QuikPAY. Front-end applications that use QuikPAY are not required to be PCI compliant; however, to ensure that customer payment and order data is protected, they must meet University eCommerce security standards. Though not encouraged, departments can build a fully PCI compliant infrastructure without using QuikPAY. Applications that do not use QuikPAY must fully comply with the PCI DSS and University eCommerce standards.

The Federal Trade Commission has consistently required merchants who reveal customer order or personal information to refund the purchase price of compromised orders as well as pay regulatory fines. University eCommerce security standards have been created to help mitigate these risks. These standards must be met by all eCommerce systems in order to use the QuikPAY system or be granted a merchant ID.

eCommerce application standards can be met in one of two ways:

- 1) Contract with central IT to use an existing system that has been certified as compliant. (Examples are the Conference Center and IATS Shopping Cart.)
- 2) Develop or purchase a system that meets the University eCommerce standards and is verified compliant by certified IT security staff. This option will generally have a compliance fee associated with it.

For those who choose the second option, the following documents provide guidance in securing eCommerce systems to the University standard. Included are:

- 1) eCommerce Audit Standards (pages 4-7)
 - a. The standards explicitly state the requirements or best practices necessary to be certified for eCommerce activities.
- 2) eCommerce Audit Questionnaire (pages 8-10)
 - a. The questionnaire provides the Office of the Treasurer and auditors necessary information to verify compliance. This questionnaire should be completed and discussed during the audit interview.
- 3) Appendix (pages 11-14)
 - a. Supporting documents for sections 1 and 2

Questions about University eCommerce standards requirements or information in this guide should be directed to the UM System Treasurer's Office.



University of Missouri eCommerce Security Guide

Office of the Treasurer

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

eCommerce Definitions

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

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

Restricted eCommerce Data: Data specifically protected by the Payment Card Industry Standard and/or the National Automated Clearing House Association (NACHA), and can not be transmitted or 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 eCommerce Security Guide

Office of the Treasurer

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

eCommerce Standards for Web Applications Storing eCommerce Data

Network Requirements	Notes and Reference Documents	Acceptable Verification Method
Server 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
Server 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
Physical Security Requirements		
Physical access to the system shall be limited to authorized individuals with physical controls and access shall be monitored 24x7	This requirement is most adequately met by housing the system in a campus datacenter.	physical inspection of facilities when not in dedicated data center.
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
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 eCommerce Data must use at least a unique username and password to access the system.	manual inspection of access controls
Transmission of data shall be via secure protocols	eCommerce 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. eCommerce 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
Granting Permission and Access Levels		
Granting access to eCommerce data shall require organizational supervisory authority	The business owner of the eCommerce system must provide written approval of all new grants of permission of eCommerce data.	inspection of questionnaire
All users who access eCommerce 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
Storage Requirements		
eCommerce data shall be stored on a secure server not an individual's machine	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



University of Missouri eCommerce Security Guide

Office of the Treasurer

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

Training Requirements		
Security awareness training shall be required for all staff with access to administer the system, manipulate data, or generate reports		Inspection of security awareness training records
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
System Security Guidelines		
System Administration and Application Development Best Practices shall be used in development, implementation, and maintenance of the system	<p>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.</p> <p>IAT Services Top 20 Audit Findings http://doit.missouri.edu/security/safeweb/docs/top-20-handout.doc</p> <p>System Security Guidelines Windows Server 2003: http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.mspx Red Hat Enterprise Linux 4 http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/security-guide/ MAC OS X Server http://www.nsa.gov/ia/files/os/apple/mac/1731-007R-2007.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</p>	automated verification of system configuration with vulnerability analysis software, and manual inspection



University of Missouri eCommerce Security Guide

Office of the Treasurer

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

	assistance in finding an appropriate guide.)	
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
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
Copying/Printing		
eCommerce data shall only be printed when a hard copy is required		inspection of internal documents
Copies shall be limited to individuals who are authorized to view the information and have signed a confidentiality agreement		inspection of internal documents
eCommerce data shall not be sent to an unattended printer or left sitting on a printer		inspection of internal documents
Copies shall have a cover sheet indicating that the data is restricted		inspection of internal documents
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
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 eCommerce transactions.	manual inspection of system configuration
Audit Schedule		
The compliance of the entire system shall be verified yearly		inspection of audit databases for completeness and consistency
The compliance of application software shall be		automated verification



University of Missouri eCommerce Security Guide

Office of the Treasurer

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

verified on each major code revision		of application configuration with vulnerability analysis software
The compliance of the entire system shall be verified on initial deployment		verify risk assessment, asset classification, and other audit documents are on file
The compliance of the operating system shall be verified monthly		automated inspection of system security measures



University of Missouri eCommerce Security Guide

Office of the Treasurer

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

eCommerce 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:

Application Developer

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

Application Information

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



University of Missouri eCommerce Security Guide

Office of the Treasurer

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

Design Documentation Present:

Web Server Information

IP Address(es):

DNS Name(s):

NetBios Name (if applicable):

Operating System:

Operating System Version (include major patch level):

System Dependencies:

Web Server:

Web Server Version:

Database Server Information

IP Address(es):

DNS Name(s):

NetBios Name (if applicable):

Operating System:

Operating System Version (include major patch level):

Database Software:

Database Version:

System Dependencies:

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:

Internal Policy Supports the Following

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

(y/n)

Access to the eCommerce data shall require <Supervisors Name> approval.

(y/n)

All users who access eCommerce data must sign a Confidentiality Agreement.

(y/n)

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

(y/n)



University of Missouri eCommerce Security Guide

Office of the Treasurer

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

All users will be required to attend Security Awareness training.

(y/n)

eCommerce Data will only be printed when a hard copy is absolutely necessary.

(y/n)

Copies will be limited to authorized staff

(y/n)

eCommerce Data cannot be sent to an unattended printer or left sitting on a printer

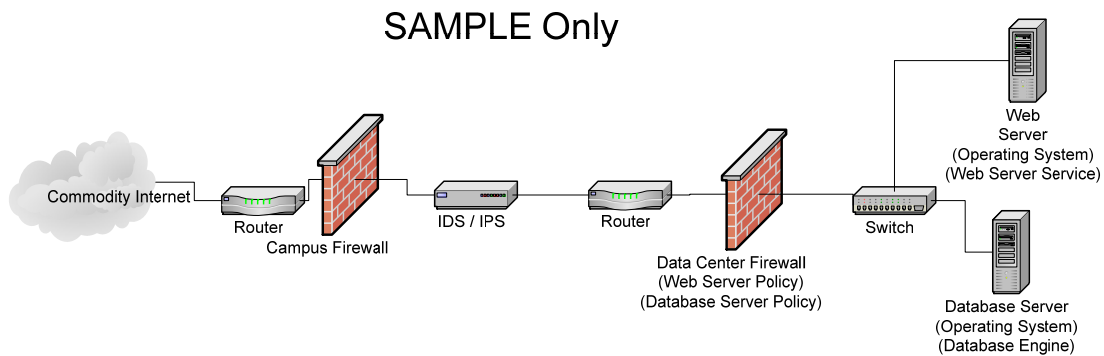
(y/n)

Copies of eCommerce 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 eCommerce Security Guide

Office of the Treasurer

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

Appendix:

Sample Departmental eCommerce 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 eCommerce needs. This system is subject to significant regulation and campus policy. The University Standards for eCommerce require the following procedures to be in place to protect the eCommerce data our system will hold.

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

The Treasurer's Office will be auditing this system and our internal processes on an annual basis, so it is imperative that these procedures are followed at all times.

Sincerely

<Supervisor responsible for the departmental eCommerce system>



University of Missouri eCommerce Security Guide

Office of the Treasurer

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

Information Technology Confidentiality Agreement

As a member of the University community, I potentially have privileged access to many different types of data. Privileged access means I have the ability to view sensitive data or take actions which may affect or give access to computing systems, network communication, or the accounts, files, data, and information of other users. I am aware that the data and information to which I have access are to be treated in a professional and confidential manner.

I certify that I have attended an information session on University Policy as well as appropriate state and federal laws concerning the confidentiality of information and the improper use or release of information and destruction of records.

I understand that if I have questions regarding FERPA, HIPAA or University security and data privacy policies that were discussed at the information session at any time in the future, it is my responsibility to contact the DIT-Information Security & Account Management group (abuse@missouri.edu) in order to ensure that I comply with regulations, processes, and policies.

By signing, I understand that any access granted me is for University purposes and agree to only use such access to perform my assigned job duties. I am responsible for exercising due care to protect this information from unauthorized disclosure, including safeguarding my password(s) and ensuring the data I obtain is disseminated only through approved University channels. Unauthorized access and use/dissemination of data are serious offenses, which may be subject to disciplinary action.

Signed: _____

Print Name: _____

Supervisor: _____

Department: _____

Division: _____

Date: _____



University of Missouri eCommerce Security Guide

Office of the Treasurer

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

Estimated Costs for E-Commerce Security Audits (provided by UM Division of Information Technology (ISAM))

- Initial audit of new eCommerce application: \$975/maximum
 - Hourly rate of \$75

- Re-audit of existing eCommerce application: \$375/maximum
 - Hourly rate of \$75

- PCI Compliance audit of eCommerce system: \$2000/minimum
 - Hourly rate of \$75