University of the Southwest
Compliance Matrix
Payment Card Industry Data Security Standard (PCI DSS)
Revision Date: 6/30/09

Requirement	Compliance Level
Build and Maintain a Secure Network	
1) Build and maintain a firewall configuration	*Compliant* • The University has installed a 3 level intrusion protection system. • The first level is a Cisco 2821 Security Edge Router. The 2821 router maintains line rate throughput under the "IMIX-1" traffic profile with Firewall, Intrusion Detection and Prevention, Access Control Lists, Extended Access, Control Lists, Qualify of Service Classification, Packet Marking/Coloring, and Quality of Service Enforcement (class-based weighted fair queuing). • Level 2 is a Cisco ASA 5500 Series Adaptive Security appliance. The appliance Provides intelligent threat defense and secure communications services that stop attacks before they impact the University network. • Level 3 is a Tipping Point 200 Series Intrusion Protection System. Tipping Point proactively inspects packets as they pass through the IPS to determine whether they are legitimate or malicious.
2) Do not use vendor supplied defaults.	*Compliant* • The University's network is divided into secure VLAN's which segregate all non-university systems onto a separate student VLAN. • The Student VLAN is accessible only to authorized users and systems which comply with the University's network access policies. These systems have direct internal network access to the mail server, portal server, and course management servers. • All university owned systems are allowed access to the Admin VLAN. These systems have direct access to all internal servers. • Currently, only the CAMS database server, Esther, and the Dynamics server, store personal student data. • The Blackboard server has limited student information.

Protect Card Holder Data	
3) Protect stored data	*Compliant* • Student supplied information on applications and information requests are encrypted by Elexio prior to being emailed to the designated University email accounts. • The University stores only the last four digits of credit/debit card numbers. These are stored on the CAMS database server. This server is accessible by internal access on the Admin VLAN only.
4) Encrypt transmission of cardholder data and sensitive information across public networks.	*Compliant* Credit card information is currently only entered through the student portal for online payment of tuition, fees, and housing charges. The web server on which the student portal resides is secured with an SSL certificate from Digicert. The data is then entered and transmitted directly through the Payflow Pro gateway. The PayPal Payflow Pro gateway complies with the Payment Application Data Security Standared (PA-DSS) which supports the PCI Data Security Standard.
Maintain a Vulnerability Management Program	
5) Use and regularly update anti-virus software	*Compliant* In addition to the Cisco 2821, Cisco ASA 5500 and Tipping Point appliances, the University uses Sophos Anti-Virus and Web Security. Sophos Endpoint Security and Control combines anti-virus and client firewall protection with endpoint assessment and control to secure USW desktops, laptops and file servers. Sophos' unified malware detection engine delivers complete protection against viruses, spyware and adware, and controls removable storage devices, instant messaging, games and is prepared to support future expansion of the network to include VoIP should this be adopted by USW. A single console deploys the software, manages policies, and reports on security across all systems connected to the USW network. Sophos Web Security and Control at the gateway blocks spyware, viruses, malware, anonymizing proxies and other unwanted applications enabling comprehensive web-access control for safe, productive web browsing. Sophos Email Security keeps unwanted and malicious

	email out of USW inboxes by blocking spam, phishing attacks, viruses and spyware, and by looking at message content and attachments. The status of the Sophos appliance is monitored internally by USW Technology Services and externally by the Sophos parent servers. No personal data is maintained on the Sophos appliance.
Develop and maintain secure systems and applications: manual or automatic regular reviews of application codes	*Compliant* The Tipping Point intrusion protection system monitors all network servers and provides alerts to the network administrator immediately upon the detection of a suspected intrusion. Reports are generated daily and reviewed by the network administrator.
Implement Strong Access Control Measures	
7. Restrict access to data on a need to know basis	*Compliant* Business office policies restrict access to billing records to only those staff members who are directly working with student or employee accounts.
8. Assign a unique ID to each person with access to the computer system.	*Compliant* A Unique ID is given to each network user, CAMS user, and Dynamics user that restricts electronic access to cardholder data.
9. Restrict physical access to cardholder data	*Compliant* Business office policies restrict access to cardholder data. Only the last four digits of the credit card numbers are kept electronically.
Regularly Monitor and Test Networks	
10. Track and Monitor access to network resources and cardholder data.	*Compliant* The University utilizes the monitoring and logging tools of the Cisco 2821, Cisco ASA 5500 and Tipping Point as well as Active Directory, the Sophos Web and Email Security; Packateer, Bradford Networks and CAMS Enterprise to monitor access to network resources.
11. Test security systems and process on a regular basis.	*Compliant* Security systems and processes will be reviewed and tested on a monthly basis by the Network Administrator. A monthly report will be submitted to the Director of Technology Services.
Maintain an Information Security Policy	
12. Maintain a policy that addresses information security.	*Compliant* An Information Security Policy is in place as of March 31, 2009.