University of Dayton
PCI System Standards

PURPOSE:
The purpose of this policy is to identify acceptable technologies and associated configuration standards for servers hosted within the University of Dayton's PCI DSS (Payment Card Industry Data Security Standard) environment.

SCOPE:
This policy applies to all University of Dayton departments, to all employees – faculty, staff, contractors, consultants, temporaries, and other workers, and to students responsible for servers and services hosted within University of Dayton's PCI environment.

POLICY:
UD must protect sensitive financial data in all areas, to protect our customers and the university. This is especially true in the environments that process credit card data for the university. In order to promote compliance with the PCI security standard that governs security in these environments, all personnel dealing with these systems must maintain a standard, secure environment. UDit has designed a basic environment in accordance with guidelines established by the PCI security standards council's DSS. The administrators of each system must comply with this basic configuration, as well as maintain security of these systems. This policy addresses many of the specific standards that are a part of this environment.

Architecture/Acceptable Technologies

- WWW – Web applications, services and sites need to employ properly signed X.509 certificates and TLSv1/SSLv3 transport encryption whenever sensitive information is exchanged, carefully vet user input to avoid common malicious exploitation techniques such as SQL Injection, Cross Site Scripting, etc. and use well defined protocols to allow for the granular protection of our resources within the PCI environment. IT staff can leverage use of centralized Apache, IIS, JBoss and Tomcat as well as Squid and Novell proxy/reverse proxy solutions. Web applications in the PCI environment must be behind a web application firewall. All web applications in the PCI environment must be contacted only through reverse proxy servers. All PCI systems may not have any direct contact to the Internet. All access to any external resources must be explicitly defined and justified by a strong business case. These will be restricted by specific firewall rules.
- Encryption – Cardholder data in the PCI environment must be transported and stored in a strongly encrypted form, using accepted encryption standards. All non-console administrative access will be through encrypted means of communication. Insecure services and protocols, such as telnet and FTP, may not be used for any communication in the PCI environment.
- Remote Access – Remote access into the PCI environment will be restricted to connections that are justified by a strong business case. These connections will only be available through the university's VPN system and only available for the time needed. Vendor access for support will only be granted on a temporary basis for the time

needed for each support incident, and will be removed as soon as each support incident is complete.

- Operating System – Even with segmentation, it's critically important that IT staff employ only those operating systems for which we have significant expertise and that have not yet entered a period of extended support or end of life. Prior to implementation, IT staff should verify applications and services work on Windows 2003 SP2+, Solaris 9+, SuSE 10+ or Red Hat Enterprise Linux 4+ or VMware ESX 3.5+. Owners of appliances, often based upon slimmed versions of commercial or free operating systems, need to similarly consider the ease and availability of updates and ability to restrict access.
- Database Management Systems (DBMS) – Databases host the persistent session information and data supporting our services. DBMS access will be restricted to administrators using secure remote access methods and to multi-tier application partners. IT staff will use centralized, backend Oracle or MS SQL in multi-tiered solutions whenever possible for increased security and efficiency.

* Exceptions will be considered when justified by a strong business case. Requests for exceptions must be made through the appropriate authorities.

System Standards

Appendix A lists general system configuration requirements for systems included in the PCI environment.

ENFORCEMENT:

Parties found to have violated this policy may be subject to disciplinary action.

REVISION HISTORY:

ISO 27002 2005 Ref. #10.4.1, #10.6, #12.1
Original: August 2009
Revision:
Responsible Office: UDit

Appendix A –Configuration Requirements for PCI Systems

All personnel with development or operations and maintenance responsibilities for systems hosted within UD's Data Center and processing customer credit card data will ensure systems are configured in accordance with the specific configuration requirements below. These configuration requirements are in accordance with current PCI DSS standards (available at https://www.pcisecuritystandards.org/index.shtml).

General

- Install critical security patches within one month of release for all system components and software.
- Run an approved antivirus solution and be current within 3-5 days.
- Enable and configure the host firewall.
- Ensure audit/security event logging is enabled with restricted access.
- Enable password protected 15 minute timeout on client sessions.
- Ensure all system clocks are synchronized to UD's NTP solution.
- Change vendor-supplied defaults before installing the system on a network, including default passwords and SNMP settings.
- Use central authentication/authorization mechanisms or create a unique user accounts for each individual using the system.
- Disable all unnecessary services and protocols.
- Update CMDB server records promptly when any changes occur.
- Disable all clear text protocols (Telnet/FTP) unless required and documented in UD's CMDB.
- Enable and configure the host firewall to explicitly allow only approved traffic and log dropped packets, if possible.
- Maintain all audit trail history for a minimum of one year, with a minimum of 3 months of logs available for immediate analysis.
- Use two-factor authentication for remote access.
- Install and configure the Sentinel agent for log analysis, and insure that this service is continually operating.
- Install Tripwire for change management and insure that this service is continually operating.
- System will be scanned for vulnerabilities both internally and externally on a regular basis. These scans will be done with, for example, Qualys/Nessus.
- Servers will point to UD's centralized update servers when possible.
- Disallow SSH to root account.