University of Dayton
Change Management for PCI Environments

POLICY STATEMENT

Modifications to our systems, whether planned or unplanned, can impact our ability to securely deliver services on time, on budget, and in good working order. Additionally, legal and industry requirements governing particular classifications of data may dictate controls. This is the case with systems that process credit card information. Changes to Payment Card Industry (PCI) environments must go through a formal change control process (PCI Requirement #6.4). Note that PCI requirements apply to the entire environment, all components involved in processing, storage and transport of data, not simply the servers and POS terminals. In general, for a change, or enhancement, to be approved, a solid business case must be presented that demonstrates the risk and lost opportunities in not making the change are significantly higher than they are for making the change.

A formal request for Change (RFC) will be required under the following circumstances:

- Modification to the network infrastructure, security controls, hardware, operating systems, applications, database, files, fields, screens, reports, or any other elements.
- Addition of new elements – hardware or software - that utilize or extend delivered system functions including data.
- Requests for deviation from central budget including the addition of products, third party products, services, and hardware.

The Change Control Board may vary depending on the request. Reviewers will consist of UD's PCI Program Manager, UDit's IT Risk Management Officer, UD's Internal Auditor and the owner of the system(s) for which the change is being requested.

PROCEDURE

There is not an exact order in which the process should occur. Evaluations and research may occur before or after the request is prepared. The primary objective of the process is to insure that a valid business case has been prepared that demonstrates a return on investment that is greater than the costs and risks associated with the change and that all PCI requirements continue to be met. Persons requesting a change to a PCI environment will submit an RFC form to the Change Control Board. In some very few cases, application of monthly operating system patches or daily antivirus signature update, for example, changes can be considered pre-approved and will not require submission of a formal change request beforehand. However, server database records should still be updated as soon as possible afterwards to reflect the environment's current status. If there's any question as to whether a change is nominal enough to be considered a candidate for pre-approval, please contact the PCI Program Manager or UDit's IT Risk Management Officer. PCI environments will be tested, as required, quarterly and upon completion of approved changes.

FORM INSTRUCTIONS

CHANGE REQUEST INFORMATION

Information in this section is, for the most part, self explanatory. All except the reference number should be completed by the owner of the system for which the change is being proposed. The reference number will be added subsequently by the Change Control Board.

DESCRIPTION

The physical request will include the background information. This information is a summary of the current situation and general details that have lead to requesting a change. Include any information which may be useful in explaining the need for the change. Submissions should include research information; how other institutions handle similar functions; presentations or product evaluations; and any other materials that may be useful in substantiating the request.

ANALYSIS

Impact: Select PCI requirement(s) that are affected by this change:

- Requirement 1: Install and maintain a firewall configuration to protect cardholder data
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.
- Requirement 3: Protect stored cardholder data
- Requirement 4: Encrypt transmission of cardholder data across open, public networks
- Requirement 5: Use and regularly update anti-virus software or programs
- Requirement 6: Develop and maintain secure system and applications
- Requirement 7: Restrict access to cardholder data by business need to know
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 9: Restrict physical access to cardholder data
- Requirement 10: Track and monitor all access to network resources and cardholder data
- Requirement 11: Regularly test security systems and processes
- Requirement 12: Maintain an policy that addresses information security for employees and contractors

Risks: Describe the risks are associated with making this modification. Examples may include perpetual maintenance requirements, security flaws or expansion of open services.

Cost: Describe items that result in expanded resources including hard and soft dollar expenditures, as well as labor. Items to consider include: software, hardware, services, labor, licenses, staff increases, maintenance, and other recurring costs associated with maintaining the enhancement.

CHANGE CONTROL BOARD DECISION

The Change Control Board will provide a written decision or request for additional information. For auditing purposes, all participating reviewers will initial and the PCI Program Manager will sign and date the completed form.

REVISION HISTORY

ISO 27002 2005 Ref. #10.1, #12.5
Original: Aug 2009
Revision:
Responsible Office: PCI Program Manager