UNIVERSITY of DAYTON

Change Management for PCI Environments

Effective Date: August 2009

Approval: December 17, 2015

Maintenance of Policy: Chief Information Officer

PURPOSE: Changes to Payment Card Industry (PCI) environments must go through a formal change control process.

SCOPE: This policy applies to all University of Dayton departments, faculty, staff, students, organizations, and individuals who, on behalf of the University of Dayton, handle electronic or paper documents associated with credit or debit card receipt transactions or accept payments in the form of credit or debit cards. The scope includes any credit or debit card activities conducted at all University of Dayton locations.

This policy also applies to all external organizations contracted by University of Dayton departments, faculty, staff, students, organizations and individuals to provide outsourced services for credit or debit card processing for University of Dayton business.

POLICY:

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.

REFERENCE DOCUMENTS:

1. ISO 27002 2013 Sec. #12, 14.2, 18.1
2. PCI Change Management Form

APPLICABLE REGULATIONS:

1. Payment Card Industry Data Security Standards (PCI DSS)

POLICY HISTORY:

Approved as Amended

December 17, 2015

Approved in Original Form

August 2009

POLICY (continued):

- 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.

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.

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.