THE UNIVERSITY OF UTAH

Version:	Modified By:	Date:	Approved By:	Date:
1.0	Lisa Zaelit	February 7, 2014	Dan Bowden	February 28, 2014
2.0	Kim Stringham	August 12, 2015	Lisa Zaelit	August 20, 2015
3.0	Stu Schrager	May 14, 2018	Lisa Zaelit	May 16, 2018

DEPARTMENT PROCEDURE FOR STANDARD 6 – Develop and Maintain Secure Systems and Applications

Purpose

The purpose for this procedure is to ensure that all system components and software are protected from known vulnerabilities by having the most recent vendor-supplied security patches installed. This is applicable for all Departments using third party software and/or web services.

Procedure

A. Change Control Procedures – Standard 6.4.5

1. Whenever a security patch is implemented or there are software modifications, the following documentation is required. This documentation is to be completed by the Department and retained permanently by the department.
    a. Documentation of what the impact has been because of the change.
    b. Documentation of the approval is required from all authorized parties.
    c. Ensure that any changes have not impacted the security of the system, and document it.
    d. Confirm that all code changes have been tested by the vendor to ensure they are PCI compliant.
        i. For any changes, the vendor should be able to provide documentation to prove that a PCI assessment that shows compliancy is performed after the change was implemented.
    e. Confirm and document that there are back-out procedures for any change made.
    f. All documentation of the above should be sent to Income Accounting & Student Loan Services.
2. Departments will complete a request for change (RFC) through the University's change management system.
    a. All Applicable documentation will be attached to the RFC.