Patch Management and System Updates

Objectives:

- Ensure the full functionality of implemented systems and applications
- Reduce the risks resulting from possible exploitation of recognized (published) technical vulnerabilities

Controls:

- Obtain timely information about updates and technical vulnerabilities of information systems and applications.
- Evaluate the value of the patch or update in terms of functionality, problem resolution, prerequisite installation, vulnerability avoidance or reduction, vendor recommendations or requirements, potential impact to systems and/or users, etc.
- Implement appropriate measures to address any identified risk.

Asset Information and Ownership

Asset Information: An inventory of the information asset, to include vendor billing and support contacts, version numbers, current state of deployment, expiration and renewal dates, etc.

Asset Owner: Individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the asset. Asset Owners are to timely maintain the elements of Asset Information to ensure information is current. See Appendix A for list of Assets and Owners.

Implementation Guidance

Asset Owners and the supporting organization must take timely and appropriate action in the identification of relevant patches and system updates to ensure the ongoing functionality of systems and applications, and to minimize the risk of exploitation of recognized and announced vulnerabilities. Implementation of the following guidelines will help achieve the stated objectives:

A. Define and establish the roles and responsibilities for system and application patching, vulnerability management and maintenance of Asset Information. This will most often require resources from the Asset Owner, business organization, and the supporting IT organizations.

B. Monitor for notices of recommendations, requirements and/or vulnerabilities. Sources of information include the system and application vendors, user groups, peer organizations, industry-recognized resources, audit functions, etc.

C. Define a timeline for reacting to a notice received or recognized, establishing its relevancy, and determining an initial course of action.

Responsible parties should review within a reasonable timeframe (e.g., two business days) all notices that are received (e.g., email message, etc.) or recognized (e.g., viewed at a vendor's website, etc.) to determine relevancy (Is the notice applicable to NU's implementation?) and what further action is recommended (e.g., ignore, communicate to support teams, schedule for discussion, recommend immediate action, etc.).

D. Assess the benefit or risk associated with implementation, and determine a course of action.
Where patches or updates are deemed relevant, the Asset Owner should identify any benefit (e.g., increased functionality, enhanced security, etc.) or adverse impact (e.g., reduced function, latency, etc.) of implementation, and determine if the recommended course of action would be to implement or "take no action".

E. Develop a recommendation and prioritization for implementation of patches/updates or other compensating controls.
The Asset Owner must decide on how quickly a patch or update should be applied. Examples: a "break-fix" update or resolution of exploitable security vulnerability might receive a high-priority designation for immediate implementation; an update to improve a low-usage function could be scheduled at a future date. Additionally, other or alternative modifications to systems, applications or configurations should be considered/recommended, where complementary and appropriate; examples are: turning services on or off, adding access controls, increasing monitoring activities, etc.

F. Test and evaluate patches/updates for effectiveness and adverse impact.
Implementation of patches and/or updates must be tested and evaluated to ensure they are effective (i.e., function as they are designed) and do not induce undesirable side effects.

G. Invoke change management procedures, as appropriate, to implement relevant patches and updates.

Document Maintenance Log

Date	*Modified By*	*Nature of Change*
22 Jul 2013	D. Kovarik	Document initiation
15 Aug 2013	D. Kovarik	Add Document Maintenance Log; add responsibility for maintenance of Asset Information; add implementation activity, subject to change management procedures.
04 Mar 2015	D. Kovarik	Update "owners"

Appendix A – Assets and Owners

- CATracks – Regan Holt
- FASIS – Kathy Tessendorf
- NUFinancials – Kris O'Brien
- Oracle Real Application Clusters (RAC) – John Walsh
- Student Enterprise System (SES) – Ann Dronen
- Business Intelligence – Luna Rajbhandari