PURPOSE
This document outlines the process UIT staff must follow to ensure technical vulnerabilities on systems are appropriately managed.

SCOPE
This policy applies to all production, development, and test environments.

POLICY
1. Each UIT Director is accountable for monitoring compliance with this policy and addressing any issues of non-compliance for IT resources for which they have day-to-day operational responsibility.
2. It is the responsibility of each UIT Director to ensure ownership of IT resources are identified including situations where multiple groups have day-to-day responsibility or no responsible party has been identified.
3. [Within 90 days after approval of this policy – May 1st] Each UIT Director shall:
   3.1. Identify the IT resources for which they have day-to-day operational responsibility.
   3.2. Ensure IT resources are classified, including:
      3.2.1. Data Classification
      3.2.2. Risk Classification
      3.2.3. System Categorization
      3.2.4. Data Types
   3.3. Develop written operating procedures that:
      3.3.1. Identify the individual(s) responsible for:
         3.3.1.1. Ensuring point-of-contact databasei is up-to-date.
         3.3.1.2. Monitoring technical bulletins and advisories for security alerts.
         3.3.1.3. Patching of IT resources.
         3.3.1.4. Updating the firmware of IT resources.
         3.3.1.5. Remediating identified vulnerabilities.
      3.3.2. Identify reasonable timeframes to address vulnerabilities.
         3.3.2.1. Unless other timeframesii have been approved by the cognizant Director, Level 1 and Level 2 Risk IT resources must have vulnerabilities addressed and patches implemented within 60 days and Level 3 Risk IT resources within 90 days.
         3.3.2.2. (Contact ISPO for information on classifying your IT resource).iii
3.3.2.3. If an IT resource has not been formally classified, it defaults to Risk Level 1.

3.3.3. React to vulnerabilities, which may include:
3.3.3.1. Implementing a patch or firmware upgrade.
3.3.3.2. Turning off services or capabilities related to the vulnerability.
3.3.3.3. Implement compensating control(s).
3.3.3.4. All vulnerabilities with a vulnerability scanner (Qualys) risk score of 4 or 5 must be remediated. All others must be addressed based on risk.

3.3.4. Address required testing and change management procedures.
3.3.5. Ensure external facing IT resources are scanned at least quarterly with software specifically designed to identify web based vulnerabilities.
3.3.6. Ensure documentation is retained consistent with the policy requirements, and made available for audit as requested by ISPO or Internal Audit. Documentation shall include the following and action logs indicating:
3.3.6.1. Who reviewed the appropriate technical bulletins (and when) and what vulnerabilities were identified (if any).
3.3.6.2. What actions were taken and when for vulnerabilities identified in a vulnerability scan or technical bulletin.
3.3.6.3. Who performed each action.

3.4. Implement the procedure(s) identified above.
3.5. Review the scan results on a routine basis (no less than monthly) and address any issues within the timeframes required under section 3.3.

4. Exceptions and Compensating Controls
4.1. In the event that compliance with this policy creates a significant cost that outweighs the benefit, an exception may be requested.
4.2. Attempts to identify and correct the problem must have been made prior to requesting an exception. In other words, the vulnerability scanner is typically not the problem. Rather, it identified a flaw or vulnerability that needs to be addressed.
4.3. Exceptions may come in the form of an exception to all or part of this policy, approval to implement or utilize a compensating control, etc.
4.4. Exceptions, including compensating controls, will be documented and approved by the cognizant Director and CIO and may be escalated to a Data Steward.

5. The Information Security and Privacy Office will:
5.1. Provide assistance upon request for the development of procedures required by this policy, interpretation of this policy, or application of this policy.
5.2. Monitor for compliance with this policy.
5.3. Report on a routine basis to the CIOs and other stakeholders as to the status of compliance.

5.4. Facilitate the exceptions process including review of compensating controls.

5.5. Escalate issues of non-compliance to the cognizant CIO and/or Data Steward.

5.6. Audit each group in UIT to determine compliance.

APPROVAL BODY: UIT LEADERSHIP
APPROVAL DATE: JANUARY 23, 2012

---

i https://db.it.utah.edu/poc/
ii Timeframes must be reasonable and defensible.
iii If you’re not sure what classification your system is, contact ISPO to complete a system classification.
iv See guidance document “H-103 IT Resource Security - Vulnerability Management” for more information on meeting these requirements, including a risk based approach for patching, addressing vulnerabilities, etc.
v http://www.secureit.utah.edu/ispo/exceptions.html