1.0 Revision History

<table>
<thead>
<tr>
<th>NORTHERN ARIZONA UNIVERSITY</th>
<th>DOCUMENT NO.</th>
<th>NAU - 730</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Configuration Management Policy</td>
<td>Effective Date</td>
<td>10/23/2013</td>
</tr>
<tr>
<td></td>
<td>Revision Date</td>
<td>10/23/2013</td>
</tr>
<tr>
<td></td>
<td>Revision No.</td>
<td>1.0</td>
</tr>
<tr>
<td></td>
<td>Producer: Information Technology Services</td>
<td>Lanita Collette, University Information Security Officer</td>
</tr>
</tbody>
</table>

2.0 Purpose

2.1 Define appropriate security measures for the setup and configuration of servers deployed at Northern Arizona University, hereinafter referred to as University.

2.2 All servers configured after the effective date of this policy are expected to comply with the provisions of this policy and associated guidelines. Existing servers must be brought into compliance as soon as practical.

3.0 Definitions

3.1 Server: For the purposes of this policy a server is a computer, physical or virtual, that provides access to files, applications, or services by means of a network connection to end-point devices or other servers.

4.0 Applicability

4.1 This policy applies to all servers maintained by University staff, faculty, consultants, or vendors for University business or academic purposes, whether housed at the University or at third party locations.

5.0 Policy

5.1 System Administrators must ensure that servers meet University security configuration guidelines. These guidelines are based on industry standards i.e., those recommended by Microsoft for Windows based servers, or industry standards for Linux servers. National Institute of Standards and Technology (NIST) or other current industry standard best practice guidelines are also considered in setting the guidelines. The guidelines will be maintained and periodically updated for currency and relevance by the Information Security team.

5.2 Adherence to the established guidelines will be assessed by periodic (at least once annually) scanning of the University server inventory by the Information Security Team.

6.0 Roles & Responsibilities

6.1 University Information Security Officer: The University Information Security Officer will recommend web application policy and guidelines to the Information Security Committee.

6.2 Information Security Committee: The Committee will review the web application security policy and guidelines and approve any changes or additions.
6.3 **Systems Administrators:** Any University staff or faculty member, consultant, or vendor who configures and manages servers for business or academic use of University students, faculty, or staff is considered a system administrator for the purposes of this policy, and must follow the policy and guidelines.

7.0 **Compliance**

Persons subject to this policy are also subject to the provisions of applicable University Personnel Policies, the student employment handbook, Arizona Board of Regents policies and conditions of service documents, including provisions for discipline for violation of this policy, as well as applicable sanctions under the law. University affiliates are subject to loss of access to University resources for violation of the policy, as well as applicable sanctions under the law.

8.0 **References**

Arizona Board of Regents: ABOR Policy Manual, Chapter 9 – Information Technology, 9-202 University Responsibilities