

Miami University Information Security Office: Network Server Management Best Practice

Document Number 20071004

Issued by: Information Security Office

1.0. Best Practice – This best practice covers all devices commonly understood as Servers and all Servers as defined in section 4.1.1 below that contain University Information that is “Sensitive/Confidential”. All such devices shall be properly configured, maintained and administered. All such devices shall be registered with the University Information Security Office (UISF). Units such as division, college, school, department, or regional campus that manage servers will ensure that University Information that is stored on those servers complies with the “Best Practice on Data Sensitivity and Stewardship of Electronic Information.”

2.0. APPROVAL(S) AND DATE(S):

This document was approved as a policy on the dates shown below. On 10/5/2007 it modified to replace the word ‘policy’ with ‘best practice’ and released as a best practice.

Policy Approved by the University Information Security Officer 6/16/2006

Policy Endorsed by the Security Working Group 7/26/2006

Policy Approved by Reid Christenberry 9/28/2006

Released as a Best Practice 10/5/2007

3.0. BACKGROUND AND RATIONALE

3.1. BACKGROUND – The purpose of the Miami University “Network Server Management Best Practice” is to promote proper protection of Sensitive/Confidential University Information and critical resources by providing guidelines for the utilization and management of servers and other Network services.

To protect this information it is necessary to properly protect the data repositories, computers systems, and networks of Miami University that are critical resources of the university. These systems must be protected against unauthorized access, malicious access, and disruption of service; Confidentiality, Integrity, and Availability of data and services must be protected. Active measures are necessary to lessen the opportunity for such incidents.

3.2. RATIONALE -- Rising frequency of security incidents involving network-attached devices significantly increase the probability of data compromise or major disruptions to the internal computer systems of the university. Platforms if not properly configured provide an extremely vulnerable and high risk opportunity for exploitation. Proper management, configuration and verifying security of all such devices that act as servers and have access to “Sensitive/Confidential Information”, along with registration will significantly reduce the potential for damage and also greatly shorten the time needed to identify and isolate equipment that has been inadvertently compromised. Additionally, care taken in building and deployment of servers provides a greater level of protection to other devices connected to the Miami University network. Establishing a central, uniform policy and issuing standards and utilities from a central authority allows for rapid incident response and continuous update of protection methods.

4.0. STANDARDS & PROCEDURES

4.1. STANDARDS

4.1.1. DEFINITION OF SERVERS – A Server is a device that offers services to other systems over a network. These provided services include Web (http) servers, FTP servers, file sharing servers, etc. Most

of these services are not typically offered by end-user workstations. However, if an end-user workstation or other device offers services such as the above and contains “Sensitive/Confidential Information”, then this device is considered a server for the purpose of this document.

4.2. PROCEDURES:

4.2.1 SERVER HARDENING – All servers which fall under this policy shall be appropriately configured, secured and managed according to requirements approved by The University Information Security Officer (UIISO). Guidelines as to how to accomplish hardening and management will be provided by IT Services.

4.2.2. SERVER REGISTRATION – Every server that falls under this best practice will be registered with the UISF. Registration information required will be defined by the UISF. Registration shall also include persons to contact for each instance as well as information as to the physical location of the server. Provision will be made by the UISF for academic environments that involve mass creation of servers

4.2.3. INCIDENT ACTION PLAN – Each server will have as part of its registration an Incident Action Plan that contains information sufficient to begin responding to breaches, compromises or other similar problems. This plan shall contain at a minimum: contact information for people technically capable of securing and responding to the incident; steps that allow the UISF or representative to immediately begin to contain or respond to the incident. Any unit that has a number of similar servers may register a master Incident Plan for all units under their control. The incident action plan must be approved by the UISF.

4.2.4. SERVER PATCH MAINTENANCE -- It is generally required that servers be current in their security patches as consistent with industry best practices for reliability.

4.2.5. AUDITING SERVERS – The unit managing the server is responsible to develop and administer its own procedures for verification of server security configurations. Assistance from the UISF is available for system verification. Failure to meet minimum requirements for server configurations as established by the UISF may result in the server being isolated from the network or other action as appropriate.

4.2.6. COMPLIANCE MONITORING -- As a continuing activity associated with normal network management, the UIISO will periodically scan for network-connected devices. Any device not in compliance with this policy may be isolated from the network or receive other appropriate action until compliance with this best practice is accomplished.

4.2.7 ISOLATION PROCEDURES – The “Responsible Use Of Computing Resources At Miami University” provides for isolating of devices from the networks under certain circumstances. In the absence of an action plan for a device, the UISF or representative will attempt to contact the device manager and failing that take other appropriate action while continuing immediate steps to notify the device manager.

4.2.8. UNIT COMPLIANCE – Division, college, school, departmental and regional campus (hereafter referred to as “units”) IT contacts will provide recommendations to the UIISO for the development and revision of standards and procedures for implementing and monitoring compliance with this policy. The UIISO will review recommendations for changes and rationales for the changes to the Vice President for Information Technology and relevant advisory groups.

4.2.9. ENFORCEMENT AND REVIEW - The UISF is responsible for monitoring adherence to this best practice and its periodic review.