Wake Forest University

Standard

Internet Facing Systems

Director of Information Security

Revision History

Revision	Date	Summary	Editor
1.0	November 19, 2012	Original release	J. Mike Rollins

Introduction and Purpose

The purpose of this standard is to define basic security requirements for any Wake Forest University (WFU) service accessible from the Internet.

Definitions

The Information Security Department is responsible across the University for all aspects of information and data security and complying with laws and regulations related to cyber security.

Information Systems (IS) Security is in the Information Systems Department and is responsible for all information and data security within IS. IS Security is also used as a resource for Information Security

Scope

This document governs all services made available to the Internet. The scope includes systems that are located outside of the campus network infrastructure such as the Graylyn, Hanes Mall Store, vendor hosted or cloud services, etc., and it includes all Internet services.

Standard

A computer or system is Internet facing if there exists at least one computer or system on the Internet that can initiate a connection to a WFU server, laptop or desktop to access an application or service such as web pages; computers and applications supported by third parties; and any other sites or computers that can be accessed remotely. This includes whether the server or desktop actually responds to the communication in any manner or not.

Any person creating or maintaining an Internet facing system must follow these security standards:

1. Registration
    a. Departments must register all Internet facing systems with Information Security. The registration information must include the following: Purpose of system, criticality of system, IP address and Internet name, statement describing the data sensitivity, and 24/7 technical and administrative contact information.
    b. The registration information must be updated annually. Failure to maintain accurate information may result in termination of service. Contact Information Security to update your registration information at infosec@wfu.edu.

2. Minimum Security Measures
    a. The system must be a dedicated system, not a general use system. For example, if a computer is providing a service to the Internet, then it must not be used by any individual to check email, browse the web or be used as a PC for other business reasons.
    b. Security patches for the operating system, firmware, application or service must be evaluated and a risk based decision on which patch to apply must be made within one month of the release of the update. Each security patch must be documented on whether it is installed and the reason why if it is not installed.
    c. When feasible, host-based firewalls shall be installed and configured to prevent unnecessary access from the local network and the Internet.

d. Anti-virus programs must be deployed and kept up-to-date on systems commonly affected by viruses.
e. Perform weekly full disk virus scans.
f. Disable unnecessary network services; this includes any sample applications, example web pages or demonstration programs.
g. Configure Internet services in accordance with vendor security or IS recommendations.
h. Many systems and applications come with default or built-in accounts that have passwords. Where possible, these default accounts shall be disabled and/or have their password changed.
i. Any non-public data must be encrypted during transmission. For example, a web server delivering non-public information should use HTTPS instead of HTTP.
j. Use secure protocols for administration, development or maintenance of the system. For example, use SSH instead of Telnet; use SFTP instead of FTP; use VPN when practical.
k. Use authentication and authorization controls to protect access to non-public information. Examples include user name and password, smart cards and tokens, biometrics, etc.
l. When developing Internet applications, follow industry best-practice guidelines, such as OWASP, and change management procedures.
m. Enable event logging of the operating system and application to a level adequate for incident response and security investigations. All log entries must include time and date. At a minimum, enable logging for login events, logout events and web page access events. Logs shall be retained for 12 months or as required by laws or regulations.
n. After any modification to the application or operating system, the system must be scanned for vulnerabilities. Additionally, each system must be scanned at least on a yearly basis with more frequent scans recommended. Contact Information Security at infosec@wfu.edu to have the system scanned.