System Configuration Policy

Date: 06/02/06	Policy ID: UVAW - 2	Status: Approved

Contact Office: Office of Information Technology

Oversight Executive: Director of Information Technology

Applies to: UVa-Wise Campus and Networks

Reason for Policy: The purpose of this policy it to establish standards and procedures for configuring the College network(s) and systems to minimize the risks of exposing sensitive electronic data to unauthorized access and/or misuse.

Definitions:

Policy Statement: The procedures that follow will help to ensure the confidentiality, integrity, and availability of this sensitive electronic data. Any deviation(s) from this policy will be documented for the business case and for the alternative method of securing the network and data.

Procedures: 2.0 Whenever possible UVa system configuration standards will be used for all builds any variation from this shall be clearly documented.

    2.1 Vendor Supplied Defaults

        2.1.1 Do not use vendor-supplied defaults

- Wireless settings – insure that: default WEP keys and SSID changed; broadcast of SSID is disabled; default SNMP community strings are changed; default access point passwords are changed; and WPA is enabled if available
- Default administrator or user passwords for systems or applications are changed.
- Default vendor accounts are to be removed if not needed. If vendor accounts are required they must be disabled and only activated when necessary then disabled immediately upon completion of the task requiring access.

    2.2 Configuration standards for all systems will be documented by the system administrator(s) and

annually reviewed by the Information Security Officer

2.2.1 Servers containing sensitive information will be limited to only one primary function per server.

2.2.2 All unnecessary and insecure services and protocols are uninstalled or disabled

2.2.3 All non-console administrative access shall be encrypted including entering the administrator's password and SSH, VPN, or SSL/TLS shall be used.

Related Information: See Vendor-Supplied Defaults Policy PCI – 2

Background: Approved by Brian Ward, CIO – UVa-Wise, June 5, 2006