Firewall Configuration Policy

*

Date: 11/11/05	**Policy ID:** UVAW-1	**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 firewall(s), network(s), and system(s) to minimize the risks of exposing sensitive electronic data to unauthorized access and/or misuse.

Definitions: Stateful Inspection - Also referred to as *dynamic packet filtering*. Stateful inspection is a firewall architecture that works at the network layer. Unlike static packet filtering, which examines a packet based on the information in its header, stateful inspection tracks each connection traversing all interfaces of the firewall and makes sure they are valid. An example of a stateful firewall may examine not just the header information but also the contents of the packet up through the application layer in order to determine more about the packet than just information about its source and destination. A stateful inspection firewall also monitors the state of the connection and compiles the information in a state table. Because of this, filtering decisions are based not only on administrator-defined rules (as in static packet filtering) but also on context that has been established by prior packets that have passed through the firewall.

As an added security measure against port scanning, stateful inspection firewalls close off ports until connection to the specific port is requested. (http://www.webopedia.com)

Policy Statement: The procedures that follow will help to ensure the confidentiality, integrity, and availability of sensitive electronic data as well as protecting resources from misuse. 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: 1.0 Firewall configuration standards shall include:

1.1 All changes to the firewall configuration must have the approval of the Information Security Officer and must be tested before instituting the change campus-wide.
1.2 Firewall configuration standards must include a documented list of services/ports necessary for administrative and business functions complete with legitimate justification for opening those services/ports.
1.3 Firewall configuration standards must deny all traffic both in-bound and out-bound, except for those listed in the above list of justified services/ports.
1.4 Firewall configurations must include stateful inspection.
1.5 Additional firewalls must be in place between any wireless network and systems storing sensitive data.
1.6 Firewall configuration standards and documentation will be annually reviewed by the Information Security Officer.

Related Information: See Firewall Configuration Policy PCI – 1

Background: Approved by Brian Ward, CIO – UVa-Wise, June 2, 2006