

Waycross College

IT Firewall Access Policy

Effective Date: March 31, 2007
Last Revised: October 20, 2006

Status:

- Draft
- Approved

Responsible University Officer

Director of Computer Services

Responsible Coordinating Office

Computer Services

Online Publication

<http://www.waycross.edu/compserv/itpolicy/>

1. Scope

This College-wide policy governs all computer systems connecting to Waycross College networks. All such systems are subject to access rules imposed by the campus perimeter firewall. These access controls are established to mitigate threats from the Internet while allowing network activities necessary in performance of the college mission.

2. Policy

2.1. Default Firewall Rules

2.1.1. Inbound Connections

- Inbound connections are defined as connections originating from the outside and destined for the inside of the firewall.
- By default the firewall will deny all inbound connections. Rules must be created to allow specific inbound connections as defined in the Exceptions to Default Firewall Rules.

2.1.2. Outbound Traffic

- Outbound connections are defined as connections originating from the inside and destined for the outside of the firewall.
- By default the firewall will allow all outgoing connections. Rules may be created to deny specific outbound connection as defined in the Exceptions to Default Firewall Rules.

2.1.3. Standard Traffic Flow

The firewall configuration consists of three active interfaces. The Waycross College LAN is attached to the Interface Port 1 (Internal). The Internet / PeachNet is connected to Interface Port 2 (External). The Student Wireless network is connected to Interface Port 3 (Stu_Wireless). Each interface has been assigned a numerical security level, and listed in the table below.

Security Hierarchy

Level	Description	Interface
100	Waycross College LAN	Interface Port 1
50	Student Wireless	Interface Port 3
0	Internet / PeachNet	Interface Port 2

By default all connection requests from a higher security level to a lower security level will be allowed. By default all connection requests from a lower security level to a higher security level will be denied. When connection requests from a lower security level to a higher security level are required to support the College mission, an access rule must be added to the firewall.

2.1.4. Standard Protocols

- Only secure network protocols shall be used to transfer non-public or sensitive data across the firewall. Any exception must be documented as to why a secure protocol is not being used and the anticipated date of conversion to a secure protocol.
- Standard Accepted Protocols
 - DNS
 - FTP (for non-sensitive data only)
 - HTTP (for non-sensitive data only)
 - HTTPS
 - POP3 (for non-sensitive data only)
 - SMTP (for non-sensitive data only)

2.2. Exceptions to Default Firewall Rules

2.2.1. Document Exceptions

All exceptions to the default firewall access rules shall be documented and maintained in Computer Services.

Requests for exceptions to the default firewall access rules should be submitted in writing to the Director of Computer Services. Requests should include the following information:

- Source IP Address
- Source Contact (Name, Phone, Email)
- Destination IP Address
- Destination protocol and port
- Destination Contact (Name, Phone, Email)
- Reason for requested exception (in support of College mission)
- Signature(s) of affected System / Data Owner(s)

Source and destination IP addresses and ports must be as specific as possible. This will maintain security by ensuring that only necessary systems and ports are accessible through the firewall.

2.2.2. Review Exceptions

All exceptions to the default firewall access rules shall be reviewed at least once per semester. Upon adding or removing a firewall access rule that affects a particular system, all firewall access rules affecting that system will be reviewed. Changes to major systems, including removal from the network, will trigger a review of all firewall access rules related to that system.

The purpose of the review will be to identify firewall access rules that need to be removed or further limited. If questions arise or a change is necessary, the system / data owner will be consulted. Any resultant changes will be documented and performed on the firewall.

2.3. VPN Access

2.3.1. VPN Access for Authorized Users

Virtual Private Network (VPN) access allows a remote computer to have network access as if it were on campus and directly connected to the network. VPN access allows users to access the same network resources they use in the office from off-campus.

Waycross College employees that have a job-related reason to access restricted College systems from off-campus may request VPN access to the campus network. That request should be made in writing to the Director of Computer Services. VPN access will be limited to those employees and job-functions that will provide a benefit to the College by allowing access from off-campus.

2.4. Enforcement

2.4.1. Enforcement of Firewall Access Policy

Firewall rules will be used to enforce the requirements set forth in this document. In the event of an emergency, additional configuration and procedural changes may be made in order to protect the Waycross College Network. Faculty and staff will be informed immediately if these changes are significant or disruptive. Workarounds will be provided for any disrupted services. In the event an acceptable workaround is unavailable, the Director of Computer Services in consultation with the Vice President over the area affected will determine the course of action.