

College of Arts and Architecture Firewall Policy

1.0 Purpose

The College of Arts and Architecture has established the following rules for firewalls in order to better protect private or sensitive data about its faculty, staff, students, and patrons and friends.

2.0 Scope

Firewalls will be installed on all Arts and Architecture networks where required by PCI-DSS standards, the University's Data Classification Scheme, or any other University policy.

3.0 Policy

The initial configuration assumes that all inbound connections from outside the College of Arts and Architecture's secure areas are un-trusted. Exceptions have been made to allow transaction of daily business.

3.1 Incoming Connections

Exception details are available from Information Technology upon request. Exceptions may be sought as outlined in the Exception Policy.

3.2 Outgoing Connections

Conversely, all outbound initiated traffic is allowed with the following exceptions and reasoning:

Service	Port	Reason for restriction
SMTP	25*	Prevents installation of unauthorized SMTP mail servers that may be used as dissemination points for malicious code or spam
Kazaa	1214	Blocks P2P software used primarily to exchange copy written material
Skype	80, 443	Those using Skype must register for an exception. If installed incorrectly, Skype can turn a computer into a "supernode" for the Skype network.

4.0 Enforcement

Any employee attempting to circumvent these rules may be subject to disciplinary action

5.0 Revision History

3/17/08 List of incoming ports and services was removed pending placement of the document behind a secure website.

Working Draft