

College of Arts and Architecture

Firewall Exception Policy

1.0 Purpose

The purpose of this policy is to outline the procedure and requirements to request exceptions to firewall rules within the College of Arts and Architecture. These rules protect the academic and administrative computing environment and safeguard college data. Exceptions without proper precautions may expose the College of Arts and Architecture to a higher level of risk including virus attacks, compromise of network systems and services, and possible litigation.

2.0 Scope

This policy applies to employees, students, contractors, consultants, temporaries, and other workers at the College of Arts and Architecture, including all personnel affiliated with third parties using the college's networks. This policy applies to all equipment that is connected to the College of Arts and Architecture network.

3.0 Policy

Although firewalls provide a secure computing environment, they could also restrict certain teaching, research, or outreach activities within the College of Arts and Architecture. Thus, the following policy establishes requirements and guidelines for obtaining firewall exceptions.

3.1. Exception Requests

While a qualified faculty or staff member (who agrees to the terms of the Arts and Architecture Server Security Policy) may administer a server, a department's professional information technology staff person must make all exception requests. These individuals are aware of the security issues and needs within their department as well as whether other internal or external resources may better provide the requested service. Additionally, they also know what information to provide the Firewall Exception Committee.

3.2 Device Administration

The Firewall Exceptions policy offers a mechanism through which college and departmental servers and/or dedicated appliances (e.g. webcams, network attached storage units) can provide their intended services. The device(s) for which the exception is sought should be dedicated to providing only the functions related to the exception. The device(s) must be administered by a qualified individual as defined by the Server Policy. Ad hoc, personal, or research servers should make use of departmental, college, or university resources whenever possible rather than soliciting an exception.

3.3 Software Patching

Server administrators must install security patches for their excepted devices in a timely fashion (as soon as possible, but not to exceed 72 hours of release by the vendor unless the patch prevents the proper function of installed software and no satisfactory work-around can

be found). As part of the auditing process, Arts and Architecture Information Technology will check computers granted exceptions to ensure that the latest security patches have been installed.

3.4 New Devices on the Network

An exception will be necessary at the point of device setup and at any time where a new service is added, even if no new port is being requested. Documentation for these changes must be kept on file to comply with auditing requirements.

3.5 Exception Process

The server administrator is responsible for researching the necessity of the exception as well as the possible security risks associated with making the exception. Administrators not part of IT will then forward this research in electronic form to their department's IT professional, who will fill out the Exception Request and forward it to the appropriate department head for signature, after which it will go to the college's Firewall Rules Exception Committee. All requests will be reviewed by this committee and adopted for the department, the college as a whole, or denied based on the lack of necessity or unavoidable security risks. Lack of necessity will be determined based on the need for the service in question and/or the availability of alternate means to more securely use the service (e.g., tunneling the traffic via a VPN).

Requests for exceptions through the firewall may only be submitted by a departmental IT professional using the Exceptions form. The form will require the following information:

- Documentation of research leading up to the exception request.
- The specific need for the exception and port(s) to be opened with justification for each.
- The Internet name and address of the computer(s) for the exception.
- The name, phone number, and email address of the individual responsible for administration of the computer(s). If staffing changes leave an excepted server unmanaged, the exception(s) may be removed if an unreasonable security risk arises.
- Security measures in force on the system including password policy, auditing policy, antivirus software (if any), and any additional security related software and/or settings of the machine.
- A statement to the effect that the owner of the computer(s) "understands that the computer(s) will be disconnected from the network and the port(s) granted the exception will be closed if a security incident occurs with that computer, contact information for the administrator is not kept current, or security patches are not being applied in a timely manner."

Exceptions may not be granted for a request that the Firewall Rules Exception Committee considers too vulnerable or for operating systems and applications without a proven record of adequate security.

4.0 Enforcement

Any new services or configuration changes resulting in how the excepted device reacts with the firewall must be documented with the Firewall Rules Exceptions Committee.

Undocumented changes will result in removal of the exception until an updated request for exemption is made.

In the event of a security incident on an excepted device, the device will be disconnected from the network and the exception removed from the firewall until the device again complies with items 3.1 and 3.2.

Computer administrators who allow multiple compromises to occur on their systems through failure to comply with 3.2 and 3.3 above will be subject to greater scrutiny and possible revocation of the privilege to request firewall exceptions.

5.0 Revision History

- Policy written and reviewed by iPAS committee April-May 2007.
- Approved by College iPAS Committee May 21, 2007