Request for Exceptions to Firewall Security
COE–FEP–02

1.0 Purpose

The purpose of this policy is to outline the requirements and procedure to request exceptions to firewall rules within the College of Engineering. These rules are in place to protect the employee and the College of Engineering. Exceptions without proper precautions may expose the College of Engineering 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 Engineering, including all personnel affiliated with third parties. This policy applies to all equipment that is connected to the College of Engineering network.

3.0 Policy

It is recognized that a firewall can restrict certain activities on the network and Internet at large that are necessary to conduct the teaching, research, and outreach functions of the College. Thus, the following policy establishes requirements and guidelines before exceptions are established through a firewall protecting individual or groups of machines:

1. All exception requests must be made by a Department’s professional information technology staff person. These individuals are keenly aware of the security issues and needs within their department as well as are aware of existing servers within the College or their Department that may already have the necessary exception and may better provide the service. Additionally, if an exception request must be made for a machine they are aware of what information the Firewall Exception Committee will need to make an informed decision such as the justification for each port included in the request.

2. The computer(s) must be administered by a professional information technology staff person and should be a system dedicated to providing the services for which the exception is requested. The purpose is to provide College and Departmental servers the accessibility they need to provide their intended services. Ad hoc, personal, or research servers should make use of Departmental, College, or University resources whenever possible rather than solicit an exception. Dedicated appliances or servers that cannot be incorporated into the aforementioned services provided by the Department, College, or University (e.g., a web cam used for providing live video feed of lectures or experiments) due to technical reasons will be reviewed on a case-by-case basis.

3. Security patches must be installed in a timely fashion (as soon as possible, but not to exceed 72 hours of release by the vendor) by the information technology staff. The only exception would be if the patch prevents the proper function of installed software and no satisfactory work-around can be found. Occasionally, the College staff will check computers granted exceptions to ensure that the latest security patches have been installed.

4. A computer will be disconnected from the network if a security incident occurs and the port(s) granted the exception will be closed until the computer again complies with items 1 and 2.

3.1 Exceptions

Exception process – Any exceptions requested for a given interface must be thoroughly researched by the department making the request for both the necessity of the exception as well as the possible security risks associated with making the exception. Upon approval by the department, a request must be made via a Request for Exceptions to Firewall Rules Exception Committee. Any such requests will be reviewed by the College of Engineering and either subsequently adopted for the department, or College as a whole, or denied based on the lack of necessity or because of unavoidable security risks associated with adopting the exception. Lack of necessity would 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. The IT professional must go to https://www.engr.psu.edu/firewall_exceptions and must contain the following information:

1. The specific need for the exception and port(s) to be opened with justification for each.

2. The Internet name and address of the computer(s) for the exception.

3. The name, phone number, and email address of the information technology staff person 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 from the system remaining unmanaged.

4. 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.

5. 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 technology staff person responsible for the computer 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 College Security Committee or Firewall Rules Exception Committee considers too vulnerable to attack or for operating systems and applications without a proven record of adequate security.

4.0 Enforcement

If security measures are mitigated after exception has been granted, the exception can be immediately rescinded.

5.0 Revision History