PennState
New Kensington

# Firewall Rule and Exception Procedure

*Procedure Number: PSU-NK-ITS-009*
*Date: September 28, 2017*
*Page Count: 3*

## Purpose:

The purpose of this procedure is to outline the process to request exceptions to firewall rules which secure the New Kensington data network. These rules are in place to protect the University's institutional data and the devices that are connected to the New Kensington campus data network. Exceptions without proper precautions may expose the New Kensington campus to a higher level of risk including virus attacks, compromise of network systems, confidential data, services, and possible litigation.

## Scope:

This procedure applies to employees, students, contractors, consultants, temporaries, and other workers at the New Kensington campus, including all personnel affiliated with third parties and other university departments and locations. This procedure applies to all devices that are connected to the New Kensington campus data network.

## Definitions:

*Device* – A computer, electronic tool or communication apparatus with the ability to connect to a data or communication network.

*Internet* - A worldwide system of computer networks

*Firewall* – A hardware device or software application that is used to monitor and inspect data transmission traveling between data networks (i.e. The Internet and the New Kensington Data Network.) Based on a programmed rule set managed by the NK ITS department, the firewall will either allow or disallow traffic with the aim of preventing unauthorized access to the campus private data network.

*VPN* – (Virtual Private Network) – A technology used to allow a user or network to connect in a secure and virtual manner via open or public communication channels. A VPN grants a remote user (e.g. working from home) secure access to local network services as if he/she were sitting in his/her office.

*IP Address* – A unique network address assigned to a device connected to a network.

*New Kensington Data Network* – The technology infrastructure, hardware, and software installed at the campus which is used to facilitate the flow of digital information between (but not limited to) computers, printers, servers, mobile devices, the Internet, etc. This includes both the wired and wireless networks at Penn State New Kensington.

*NK ITS Department* – The department that oversees IT resources at Penn State New Kensington to include the System Administrator, IT Specialist and IT Director

*Penn State New Kensington IT Council* - a group of individuals that advise the Chancellor on IT strategic planning and governance for Information Technology at Penn State New Kensington

*System User* - an individual that uses a device that is maintained by the NK ITS Department and agrees to the responsibilities outlined in the Computer System Usage Agreement Form.

*Enhanced System User* - an individual that uses a device and has agreed to be responsible for the systems administration aspects of the device as outlined in the Computer System Usage Agreement Form.

## Procedure:

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 University. Thus, the following policy establishes requirements and guidelines before exceptions are established through a firewall protecting individual or groups of computers and servers:

- All exception requests must be made by the system user or system administrator that has the particular exemption need.
- The devices(s) must be administered by a professional information technology staff person. The purpose is to provide campus 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 due to technical reasons will be reviewed on a case-by-case basis.
- Security patches must be installed in a timely fashion (as soon as possible, but not to exceed one week of release by the vendor) by the system administrator. 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 NK ITS Department staff will check computers granted exceptions to ensure that the latest security patches have been installed.
- A device will be disconnected from the network if a security incident occurs. The port(s) granted in the exception will be closed until the computer complies with items 1 and 2 once again.

PennState
New Kensington

## Exceptions

Exception process – Any exception requested for a given device 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 to the Director of IT. Any such requests will be reviewed by the Penn State New Kensington IT Council and a recommendation will be made to the Chancellor. The decision for adoption or denial will be based on security risks associated with adopting the exception and ultimately will be the decision of the Chancellor.

When a System User or Enhanced System User submits a request for exception, the following information should be included:

- The specific need for the exception and port(s) to be opened with justification for each.
- The device name(s) or IP address of the devices(s) for the exception.

A statement to the effect that the owner of the device(s) "understands that the device will be disconnected from the network and the port(s) granted the exception will be closed if a security incident occurs involving the device.

Exceptions may not be granted for a request if the Chancellor considers the proposed exception too vulnerable to attack, or for operating systems and applications without a proven record of adequate security.

## Enforcement

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

## Procedure History:

September 28, 2017 – Procedure created based off previous campus policy.