Technology Security Audit Procedure

Procedure Number: PSU-NK-ITS-007
Date: February 15, 2018
Page Count: 2

Purpose:

To provide the authority for members of the NK ITS Department and the Office of Information Security (OIS) to conduct a security audit on any technology system located on Penn State New Kensington campus property in accordance with University policy AD-95.

Examples of situations which an audit is justified include:

- Ensuring integrity, compliance, confidentiality and availability of information and resources.
- Investigating possible security incidents and ensure conformance to University security policies.
- Monitoring user or system activity where appropriate (e.g. system compromise is suspected, policy violations are suspected, and complaints have been received).
- Ensuring validity of user accounts.

Scope:

This procedure covers all computer and communication devices owned or operated by the Penn State New Kensington campus. This procedure also covers any computer and communication devices that are present on the Penn State New Kensington premises and/or the New Kensington Data Network, but which may not be owned or operated by the New Kensington campus.

Definitions:

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

Office of Information Security (OIS) - a group of individuals that are part of Penn State Information Technology Services (ITS) that is responsible for protecting the Penn State community from threats to our IT resources.

PennState New Kensington

Procedure:

When requested, and for the purpose of performing an audit, any access needed will be provided to members of the Office of Information Security (OIS) and NK ITS Department personnel in line with University policy AD-95. Users and/or support personnel must ensure that any hardware or software installed for the purposes of filtering traffic such as a firewall appliance or personal firewall software allow unrestricted traffic to and from all systems authorized to conduct security audits at the campus level. At no time shall anyone other than those authorized at the campus or University be permitted to scan computers or devices connected to the New Kensington Data Network or wireless network.

This access may include:

- User level and/or system level access to any computing or communications device
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on the Penn State New Kensington equipment or premises
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and log traffic on the New Kensington Data Network.

Enforcement

Anyone found violating this procedure will be subject to disciplinary action by the administrative unit, the campus, or the University.

NK ITS Department or the Office of Information Security (OIS) personnel will immediately block network access to any system found to be scanning systems in violation of this procedure. Individuals found to be in violation of local, Commonwealth or Federal regulations or laws will be referred to the University Security Office for case disposition.

Procedure History:

February 15, 2018 - Procedure created based off previous campus policy.