PennState
New Kensington

Acceptable Use and Security Procedure

Procedure Number: PSU-NK-ITS-004
Date: March 2, 2012
Page Count: 7

Purpose:

The purpose of this procedure is to outline the acceptable use of computer and electronic equipment within Penn State New Kensington, hereafter referred to as “campus”, and its facilities. Inappropriate use exposes everyone to risks including virus attacks, compromise of network systems and services, and possible litigation.   Penn State New Kensington computing systems are for business purposes in serving the administrative, academic, and research activities of Penn State New Kensington, University, faculty, staff, and students.

Effective security is a team effort involving the participation and support of every Penn State New Kensington employee and affiliate who deals with information and/or information systems. It is the responsibility of computer users to familiarize themselves with this procedure and conduct their activities accordingly.

Scope:

This procedure applies to faculty, staff, students, contractors, consultants, temporaries, and other workers of Penn State New Kensington, including all personnel affiliated with third parties. This procedure applies to all equipment that is connected to the New Kensington Data Network.

Definitions:

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

Spam - Unauthorized and/or unsolicited electronic mass mailings.

Internet - A worldwide system of computer networks.

Intranet - A private network that is contained within an enterprise.

Extranet - A private network that uses the Internet protocol and the public telecommunication system to securely share part of a business' information or operations with suppliers, vendors, partners, customers, or other businesses.

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.

DHCP (Dynamic Host Configuration Protocol) - A protocol used by devices to obtain network information such as an IP Address in an automated fashion.

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 campus Information Technology staff consisting of the System Administrator, IT Specialist and the Director of IT

Procedure:

General Use and Ownership

1. Electronic equipment purchased by the University should be used to support the University’s mission of teaching, learning, research, and service.
2. It is a requirement that devices connecting to the New Kensington Data Network be configured and operated in a manner consistent with University Policies.
3. To comply with University Policies, State and Federal Law, Penn State New Kensington must be able to trace a device's network activity to an individual user. Any device attached to the New Kensington Data Network must adhere to the configurations herein.
4. Institutional data regardless of classification (public or private) must be used, stored, and archived according to University Policies.
5. Penn State New Kensington reserves the right to audit the New Kensington Data Networks and systems on a periodic basis to ensure compliance with Penn State New Kensington and University policies and security and network maintenance purposes.

Device and Network Security

1. If a device connects to the New Kensington Data Network or University via an authenticated network connection (802.1x, wireless VPN, Remote VPN), the user credentials used to "log in" to the authentication mechanism will be considered the "user of record" for all activity generated by the device.
2. If the device is connected to an unauthenticated connection (i.e. a "standard" New Kensington Data Network connection):

- The device's operating system must be configured to control access to the device with a username *and* password.
- All users of the device *must* be assigned a userid and password that uniquely identifies them. Users must not share their userid and password with anyone.
- Passwords must comply with University Password requirements.
- Shared or "Group" accounts are permitted only when necessary to carry out institutionally assigned responsibilities. Shared credentials must have a designated owner and co-owner, which are jointly accountable for the security of the data, system, or application for which they have been provided access.
- The NK ITS Department must maintain a signed End-User Computing Agreement for each Penn State New Kensington employee and user account.
- The device must maintain a log containing at a minimum, the login date/time and userid of all users when they log in and log out of the device.
- Optionally, the device may participate in a network based Identity Management system (such as Active Directory) to support and provide the appropriate user audit logs.

3. Individuals are not permitted to extend their own authorized computer and network access privileges to others (e.g., Password sharing, connection sharing, or installation of rogue Wireless Access Points).
4. Any network device which handles "Institutional Data" (e.g., Student Records, Financial Data, HR Data, etc.) is required to comply with additional security requirements, including:
   - The device must be configured to comply with University minimum security standards.
   - The content of the device’s Hard Disk drive *must* be encrypted.
   - The device must be connected to the designated New Kensington Data Network access port on the New Kensington Data Network.
   - The device must not allow access to any student, guests or non-Penn State New Kensington staff.
   - The device must not give access to the hard drive(s) where others can read or write files to the location on your hard drive(s).
5. The device must be configured and operated according to University minimum security standards and "Best Security Practices" (e.g. NIST SP800-12).
6. Where applicable, the device must have anti-virus software installed and configured to obtain automatic updates. The anti-virus software must also be enabled and active.
7. Where applicable, the device must be configured to obtain OS updates automatically. It is recommended that the device also be configured to install OS updates automatically. If the device does not auto-install updates, a process must be in place to ensure that all security updates are installed within a reasonable time after release (e.g. less than 2 weeks). Exceptions will be made at the discretion of the Director of IT.
8. University Policy requires a user to operate a University device with the least privileged account required to perform required tasks. If a user believes additional system privileges are required

to perform his/her employment duties, refer to Penn State New Kensington procedure PSU-NK-IT-00Q (Computer Administrative Access Request Procedure). If an exception is granted, the user should operate under a system user (limited user) account at all times unless required to elevate his/her privileges to perform a task.

9. The University is concerned about Intellectual Property Rights. The New Kensington Data Network is maintained to support the teaching, research, and outreach missions of Penn State New Kensington and University. Use of Peer to Peer (P2P) file sharing software should be limited to those occasions where it supports the mission of the University. Routine network maintenance activities occasionally result in the detection of devices participating in P2P networks. Any device found participating in an unauthorized P2P network may be disconnected from the network without prior notice. Any violations of Intellectual Property Rights discovered during routine maintenance activities will be reported to the Office of Information Security (OIS).
10. All systems connected with the New Kensington Data Network infrastructure may only use IP addresses assigned by Penn State New Kensington or the NK ITS Department. IP addresses provided via DHCP must employ a mechanism to ensure that only the intended host receives the IP address or are authenticated and logged so that the user of that IP address during a given period of time can be determined in the event of a security incident.
11. Purchasing of electronic devices (e.g. computers, printers, A/V equipment) must be coordinated with the NK ITS Department to assure equipment is compatible with Penn State New Kensington infrastructure and purchased within university guidelines. Departments interested in purchasing equipment should contact the NK ITS Department.
12. The relocation of a device(s) with the exclusion of laptop computer, from a classroom or office in which it is assigned is prohibited without approval of an ITS staff member.

Information and Data Security

1. Because information contained on portable and remote computers is especially vulnerable, special care must be exercised. Portable and computer systems containing sensitive university data are required to utilize hard drive encryption techniques to protect the data in the event of unauthorized physical access to the system. In addition, the hard drives of all University-owned laptop computers must be fully encrypted.
2. To maintain proper data encryption, all systems storing or utilizing Institutional Data (AD-96), and using a wireless connection must also utilize a Penn State New Kensington approved VPN (virtual private network). Systems transferring sensitive university data over non-secure networks (wired or wireless) must encrypt that data during transmission.
3. Sensitive university data may not be stored on a non-encrypted portable storage device (i.e. portable hard drive, USB key). If the use of a portable storage device is required, consult the Director of Information Technology regarding an approved storage device.
4. Sensitive University data is prohibited from being stored on a personally owned computer.

5. If a computer is left unsupervised, access to the device must be secured. When traveling, laptop computers must be physically secured.

Unacceptable Use

The following activities are prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Penn State New Kensington to engage in any activity that is illegal under local, state, federal or international law while utilizing Penn State New Kensington owned resources.

The lists of prohibited activities presented below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or entity protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Penn State New Kensington.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Penn State New Kensington or the end user does not have an active license is strictly prohibited.
3. It is illegal to export software, technical information, encryption software or technology, in violation of international or regional export control laws. The Director of Information Technology should be consulted prior to export of any material that may be of question.
4. Introduction of malicious programs into the New Kensington Data Network or devices (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.). Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
5. Using an electronic device to engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
6. Making fraudulent offers of products, items, or services originating from any university access or email account. Or, offers of products, items, or services for personal profit from any university access or email account.
7. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or

logging into a server or account that the employee is not expressly authorized to access. The only exception to this is when access is part of a security analysis performed by an authorized Penn State New Kensington or university individual. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information.

8. Port scanning or security scanning without prior approval from the Office of Information Security (OIS).
9. Executing any form of network monitoring which intercepts data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
10. Circumventing user authentication or security of any host, network or account apart from assigned duties performed by the NK ITS Department.
11. Interfering with or unsanctioned denying of service to any user other than the employee's host (for example, denial of service attack).
12. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet apart from assigned duties performed by the NK ITS Department.
13. Providing information about, or lists of, the Penn State New Kensington employees or students to parties outside the University (excluding the Penn State New Kensington directory).
14. Extending your own authorized computer and network access to other individuals through connection sharing such a bridge portal or the installation of a rogue wireless access point.

Email and Communications Activities

1. Sending unsolicited email messages (unrelated to University Business), including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through content, language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters" or "pyramid" schemes of any type.
6. Use of unsolicited email originating from within The New Kensington Data Network or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Penn State New Kensington or connected via the New Kensington Data Network.
7. Posting identical or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Procedure History:

September 19, 2019 – Removed firewall exceptions because we no longer manage a local firewall
February 15, 2018 - Procedure created based off previous campus policy.