Administrative Access Request Procedure

Procedure Number: PSU-NK-ITS-00Q
Date: September 28, 2017
Page Count: 4

Purpose:

To comply with university policy, employees assigned a university-owned laptop and desktop computer have limited access to install new software and change computer system settings. In addition to university policy, this procedure is an industry best practice as it pertains to computer security. At times, enhanced system user privileges are required to perform one's job duties. This procedure establishes the steps necessary to request enhanced system user privileges on a university assigned laptop or desktop computer.

Scope:

This procedure applies to faculty, staff, students, contractors, consultants, temporaries, and other workers of the New Kensington campus, including all personnel affiliated with third parties. This policy applies to all devices that are connected to the New Kensington campus network.

Definitions:

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

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.

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

Personally Identifiable Information (PII) – is information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual. PII data is commonly exploited by criminals to steal an individuals' identity. The combination of a name and the following sensitive information are common examples; Social Security Numbers (SSNs), credit card

numbers, Driver's License numbers, passport numbers, Personally Identifiable Health Information (PHI), salary and tax information related to individuals, details of University budgets, tenure or promotion information, staff employee review information, password or other system access control information, human subject information, admission and financial aid information and donor information.

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.

Procedure:

The employee requesting enhanced system user privileges to a university-owned computer must provide a written statement submitted to the Security Liaison/Director of IT explaining why the requested privileges are needed to perform his/her position responsibilities.

The Security Liaison/Director of IT will consult with individual's supervisor to ensure they support the request. The department supervisor and Director of Information Technology will share their recommendation with the Chancellor for approval. Final approval from the campus Chancellor is required to fulfill the request for elevated system privileges.

Granting Access

When a University employee is granted elevated system privileges, he or she must sign an updated End User Computing Agreement acknowledging the additional liabilities they are accepting as an enhanced system user (system administrator) of their computer system.

Enhanced system users (system administrator) privileges are provided to the user to perform system changes. The user, however, should operate under a system user (limited user) account at all times unless required to elevate his/her privileges to perform a task.

When an employee is granted enhanced system user privileges they accept responsibility for any changes they make to the system as well as agree to have system management, software inventory, and antivirus software installed on the system. NK ITS Department is responsible for patching the operating system and all software applications that were provided with the base image, unless otherwise noted. The enhanced system user is responsible for patching all software they install. Users who are granted enhanced system user privileges must comply with all University policies. Software aimed at scanning electronically stored data for Personally Identifiable Information (PII) may be required. Scans will be conducted regularly and results are sent to a central server hosted by the Office of Information Security (OIS). Anti-virus software must be installed, running, and updating regularly as per campus procedure PSU-NK-ITS-006.

Enhanced system users are prohibited from modifying their system configuration in a manner that would prevent their system from communicating with the University's system management, software inventory, PII, and antivirus servers/systems. Users granted enhanced system user privileges are

required to maintain appropriate software licensing documentation for any software they install over what NK ITS Department provides/manages on the base software image. Documentation should be readily available for audit to ensure compliance with terms of issuance. Lack of proper licensing documentation will result in the system's removal from the New Kensington Data Network, and, if necessary, notification of the violation to the appropriate authorities.

Loss of Elevated System User Privileges

The following incidents may be cause to revoke the elevated system user privileges granted via this procedure. If an incident occurs, NK ITS Department personnel will investigate the incident and escalate it to the Office of Information Security (OIS) if required. Otherwise, a report will be created and shared with the user, supervisor, and campus Chancellor. A meeting will be scheduled to review the findings and determine appropriate sanctions and/or removal of privileges.

Incidents that can result in the loss of the elevated system user privileges include:

1. Computer Compromise – A computer is compromised by virus, malware, Trojan, or other malicious software application.
2. The computer system in question is not being maintained (via system patches and upgrade) per campus and University policy. An un-patched system is susceptible to compromise.
3. Network security scans find an unprotected or system vulnerability that is not patched or protected.
4. Scans for Personally Identifiable Information (PII) provide positive results.
5. The system in question is not compliant with software licensing requirements.
6. Violation of this procedure, campus or University policy.

If the incident places University resources in danger of compromise, the suspected computer will be removed from the New Kensington Data Network and/or confiscated without warning.

If a computer compromise occurs which includes the possible exposure of PII, the response to the incident will be conducted in line with campus procedure PSU-NK-ITS-014 University Institutional Data and Personally Identifiable Information.

PennState
New Kensington

Procedure History:

October 1, 2019 – PII scanning is no longer required on all systems with admin rights, just those roles that OIS has identified.

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