PennState New Kensington

Password Procedure

Procedure Number: PSU-NK-ITS-005
Date: February 15, 2018
Page Count: 2

Purpose:

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the New Kensington Campus Data Network. As such, all Penn State New Kensington employees (including contractors, temporary personnel, and vendors with access to any/all New Kensington campus technology systems) are responsible for taking the appropriate steps, as outlined below, to select and secure personal passwords. The purpose of this procedure is to establish standards for the creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope:

The scope of this procedure includes all personnel who have or are responsible for an account (or any form of data communications access) on any system that resides at or in any New Kensington campus facility, has access to the New Kensington Campus Data Network through local or remote connectivity, or stores any non-public campus information.

Definitions:

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.

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:

Penn State has established rules for creating and securing passwords based on the guidance provided by the National Institution of Standards and Technology (NIST) in Special Publication 800-63b, section 5.1.1. Memorized Secrets. Password rules can be found in the Access, Authentication, and Authorization Management Standard, Section VII Authentication, of University Policy AD-95.

Procedure History:

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