Access Control Policy for KSC Computers and Data



Keene State College Policies and Procedures

Access Controls Required for KSC Computers and Data

Section Menu

Overview

Control access to information, computer systems and resources used for the transaction of USNH business shall be protected from theft, malicious destruction, unauthorized alteration or exposure, or other potential compromise resulting from inappropriate or negligent acts or omissions.

The USNH System Access Control Policy will increase protection for computers and data resources used in the transaction of USNH and Keene State College business. Given that security is a combination of policies/standards, business practices and technical controls, KSC will rely on all three to ensure our compliancy with the USNH System Access Control Policy. It is the responsibility of every KSC employee to comply and practice safe computing practices as outlined by USNH and KSC policies, standards and procedures.

Workstations

KSC employees must take responsibility and appropriate measures to prevent access by unauthorized persons. All Windows workstations will automatically lock with a black screen after 20 minutes of inactivity. All Macintosh computers will be configured to sleep mode after 20 minutes of inactivity. All lab and classroom computers will log the user out after a period of inactivity. NetID passwords will be required to unlock the screen. The only computers exempted are workstations that have been identified as public access kiosks.

To protect campus resources from theft, malicious destruction, alterations or other inappropriate or negligent acts, all KSC computers and network printers must be physically locked down. Laptop users must be particularly

conscientious of locking down the computer when you are not in your office. Use the lock provided to you by the IT Group. If you cannot locate your laptop lock, please contact the HelpDesk.

Data Security

All data on all computers or electronic storage devices (including, but not limited to desktops, laptops, servers) shall be wiped clean of files and data prior to transfer to surplus. Our current surplus vendor uses Department of Defense standards for wiping all hard drives.

Passwords

All KSC employees must log into the KSC network using their NetID. All KSC NetID passwords are set to expire every 6 months. KSC employees should create their password keeping in mind that it is important to create a strong, complex password. You should never share your passwords with anyone or have them easily accessible by having them written down on a piece of paper.

Protecting Social Security Numbers

Never send Social Security Numbers through email unless they are encrypted. Never print or share Social Security Numbers that have all of the numbers visible. Never publicly display Social Security Numbers. If you don’t really need that information, don’t use it. Always shred important information when you no longer need it or dispose of those documents through lock boxes around campus.

Accessing KSC Data from Home or on the Road

If you are accessing sensitive data from home or during travel, it is your responsibility to provide the same level of security that would be provided within the KSC environment. Your computer should be set to install all patches and run an automatically updated anti-virus product.# Access Controls

Required for KSC Computers and Data