CEHD Computer Security and Service Policy

This document is written in support of the following University policies:

- 1-14: Policy for Responsible Computing at the University of Delaware
- 1-15: Information Security Policy
- 1-18: Electronic Mail Management and Retention Policy
- 1-19: Employees' Use of E-Communications Policy
- 1-20: Policy for Wireless Computing at the University of Delaware
- 1-22: Personal Non-Public Information (PNPI) Policy

Support Requests

The Office of Educational Technology (OET) provides computer and network support to CEHD faculty and staff. This support includes setting up computers, virus detection, the installation of virus protection software, automatic operating system and software updates, the installation of operating and productivity tools software, diagnosing printing problems, hardware and software recommendations, and printer installation.

To request computer support for University-owned computers, write to oet-help@udel.edu, use the web form at http://home.oet.udel.edu/oet-help-request-form/, or call (302) 831-8162.

Clients who request service on laptops must bring them to OET's main office in Willard Hall Education Building. Because of the volume of calls and scheduled appointments, technicians cannot respond to unscheduled requests for support.

In addition, OET offers home computer support for a flat fee. Clients must sign a waiver for service on home computers.

Computer, Network and Information Security

All CEHD equipment connected to the University network must be configured by OET at the time of connection to ensure that it is secure and properly configured. In addition, any computer that is physically moved to another location; assigned to a new user; or is to be used by additional users -- in the case of shared computers -- must be visited by OET at the time of these changes.

The Office of Educational Technology will provide an annual base computer inventory for each unit in September, using Google Docs. This document will be shared with an administrative assistant in each unit and will list all computers with KACE installed. It is the responsibility of the unit to notify OET of any inventory changes. In addition, OET will record equipment information, if available, in help call requests and resolutions in OET's help call database.

Each unit should specify its own standard procedures with regard to file storage and retention. They, and not OET, are responsible for ensuring that personal non-public information (PNPI) is not saved on local drives and that all computers, whether or not they are used to handle sensitive information, are regularly updated and protected against attack and infection. See University Information Security Policy (1-15) and Personal Non-Public Information (PNPI) Policy (1-22)

OET's recommendation is that Microsoft Word and Excel be configured to save by default to a network location on an OET file server. Backups of OET file servers are performed as outlined in the CEHD File Storage, Backup, and Retention Policy (PDF).

Specific guidelines regarding mail retention are outlined in University Electronic Mail Management and Retention Policy (1-18) and Employees' Use of E-Communication Policy (1-19).

Every faculty member, full- or part-time staff member, and graduate student in CEHD may receive an OET login and file space. Addition and deletion of faculty, staff and students on OET's network is not automatic. Units need to notify OET when individuals join CEHD and when they leave. In addition, OET will contact each unit at the beginning of the fall and spring semesters to verify if current accounts should remain active.

Computer Recommendations/Purchase

To insure that CEHD computers have the required software and hardware to access University and OET network resources safely and securely and for increased efficiency in computer configurations, contact OET for computer software and hardware purchase recommendations, including wireless access points.

In addition to preserving our security, purchases through OET frequently qualify for discounts.

For home purchase recommendations, contact the Technology Solutions Center, consult@udel.edu, 002B Smith Hall, (302) 831-6000.

Computer Configurations

The currently supported operating systems within CEHD are Windows 8, Windows 7 and Windows Vista and for Macintosh computers, OS X 10.6 or later. All CEHD computers must have current virus protection, firewalls enabled, and current operating system updates. In support of the Policy for Responsible Computing at the University of Delaware (1-14), and to protect the intellectual property of the College, each computer that contacts OET servers must have McAfee Virus Protection and KACE installed for automatic updates of non-Windows software. In addition, Windows computers on the OET network have operating system updates pushed to them.

Wireless Devices

In support of the Policy for Wireless Computing at the University of Delaware (1-20), wireless access points must be configured by University Network and Systems Services (NSS) or OET staff. In addition, wireless printers must be configured by OET staff.

Moving computers

If you need a computer moved, contact University movers to move it to your desired location (OET does not move computers). It is important to remember that once it is moved, schedule an appointment with an OET technician to install the equipment.

Data Security Recommendations

All computer users have the obligation to protect University resources and data. Data protection measures include maintaining password security, locking your computer when you are away from it, safeguarding PNPI, and disposing of computers properly. To safeguard your data, especially in public areas, lock your computer session, when stepping away from the computer.

Disposal of computers

If you plan to dispose of a computer, contact OET. An OET technician will record the computer's network configuration and to wipe the computer of all data using specialized software to insure that your data is not compromised and is completely erased. Do not discard computers that have not been wiped by OET as this creates a security risk for you and your department.

Once your computer is erased, contact University movers to deliver it to UD Surplus or take it to UD Surplus yourself.

If a computer hard drive malfunctions and cannot be erased, OET will deliver the hard drive to University Archives, where the drive will be destroyed. Your unit will be billed for the associated fee.

Passwords

Passwords are considered confidential information and should not be shared or written down. Strong passwords (11 or more characters and a combination of numbers and upper and lowercase letters) should be used for your OET and University network accounts. If you need to share a password-protected computing resource with another staff member, contact OET for assistance.

Under no circumstances should staff and faculty share an individual's login and password. In rare circumstances, anonymous logins on the OET network are created and assigned and are associated with specific computers.

Personal Non-Public Information

Personal non-public information (PNPI) should not be kept on computer hard drives or removable media such as floppy disks, USB flash drives, or zip drives. Examples of PNPI include Social Security Numbers, credit card numbers, and grades in the context of identifiable information such as names. If absolutely necessary, this information should be encrypted and stored on a secure network drive. For encryption solutions, contact oet-help@udel.edu.