

Title: Policy for Protection of Publicly Accessible Computers
Effective Date: October 13, 2011
Issuing Authority: Chief Information Security Officer

Policy:

To ensure the safety of Temple's systems and to protect the privacy of the Temple community, this policy outlines Temple University's rules and best practices for protecting computers in publicly accessible areas from the risks associated with shared usage and for safeguarding the login credentials of users on these computers.

Publicly accessible computers include but are not limited to smart classroom workstations, instructor stations, smart carts, lab workstations, kiosks, and other shared computers.

Required Procedures:

All publicly accessible instructor/presenter computers must adhere to the following policies, unless an alternative procedure is approved in writing by the Chief Information Security Officer (CISO):

- adhere to all technology policies as posted on <http://policies.temple.edu>.
- follow the annually published, [shared computer software lockdown procedures](#).
- participate in the centrally managed Computer Services patching process.
- run the university approved anti-virus/endpoint protection software, as outlined in the [Temple University Technology Usage](#) policy.
- attach wired keyboards or the receiver dongle from wireless keyboards to the computer using a locking mechanism. Enable encryption on wireless keyboards.
- install proper secure screws (e.g. snake eye pin screws) on podium/instructor station security panels
- use AccessNet username and password logins assigned via Global Groups from Active Directory. Use of generic and/or local administrator accounts is prohibited, except where access is only provided to the desktop through automatic login on startup and where additional access to any network resources is limited through login/proxy access.

Recommended Classroom Procedures:

- Open rooms only as needed and no more than ½ hour before class begins. Secure rooms, when not in use. Make rounds to inspect rooms to ensure classes haven't been canceled and secure rooms.
- On a daily basis, visually inspect the podiums/instructor stations and computers. Look for signs of tampering on any of the screws and security panels.
- Twice per semester, open each podium/instructor station and inspect the computer.

Recommended Student Workstation Procedures:

It is recommended that all publicly accessible student stations in PC Classrooms, Training Rooms and other stations in labs or kiosks adhere to the following guidelines:

- install extra panel locks as needed on podium/instructor station computers and ensure that the computer cannot slide through the security panel or be turned in its storage area.
- install keyboard locks and lock down procedures on student stations in PC classrooms, training rooms and other stations in labs or kiosks.