

SECURING UNATTENDED WORK STATIONS PROCEDURES

Related Board of Trustees Policy: BP 8.4

Approval:

Revision:

NC Statewide Technology Standards (ed. August, 2010 Corrections): 20103, 30109, 50705, 50706

Securing Unattended Work Stations

Workstations are safeguarded from unauthorized access, especially when left unattended. Craven configures all workstations to require a password-protected screen saver after a maximum of thirty (30) minutes of inactivity. These time-outs are implemented in the form of password protected screen savers or lock screens that require the user to re-authenticate to access the system. Time-outs are enforced through Active Directory Group Policy Objects (GPO's). Users shall not disable the password-protected configuration specifications established by the College.

Under no circumstances should an employee leave their screen unattended with an actively logged in Datatel session. The session must either be logged out or the computer locked according to the below guideline.

GUIDELINE

Users should lock their workstations when leaving them unattended. This can be accomplished in a number of ways.

1. Press the Windows key (with the windows logo on it) and the L key.
2. Press control-alt-delete and choose "lock computer."

Additionally, users should turn off computers or set them to hibernate at the end of the day or when they will be out of the office for an extended amount of time.

Recorded: November 4, 2011

[Return to Table of Contents](#)