

3. Systems must have a password protected screen saver automatically activated within a short timeout period to ensure that unattended workstations are protected.
- C. Prior to leaving for the day, faculty and staff must:
1. Exit running applications and close any open documents.
 2. Ensure workstations are left on but logged off in order to facilitate after hours updates.
- D. Faculty and staff shall use University workstations for authorized University purposes only.
- E. Only approved personnel may install pre-approved software on University workstations.
- F. All sensitive information must be stored on network file shares.
- G. Laptops shall be secured through the use of cable locks or locking laptops up in drawers or cabinets.
- H. The IT Department shall ensure that all workstations use a surge protector (not just a power strip) or a UPS battery backup.
- I. Faculty and staff shall keep food and drink away from University workstations in order to avoid accidental spills.
- J. University workstations shall have vendor-issued critical security updates and patches installed in a timely manner.
- K. University workstations shall have active and updated anti-malware protection software.
- L. Faculty and staff shall not disable anti-malware protection software.

DESK AND OFFICE AREAS

- M. Faculty and staff who work with sensitive information should have lockable space available for storage

