CP – 8.99.1

DAMAGE, LOSS, OR THEFT OF IT EQUIPMENT

Related Board of Trustees Policy: none
OPR: Vice President for Administration
Approval: August 2012
Revision: January 16, 2018

DAMAGE, LOSS OR THEFT OF IT EQUIPMENT

College employees are obligated to protect College information technology (IT) equipment and sensitive College data. This procedure outlines the necessary steps to take in the event of equipment damage, and to minimize the potential threat to network and computer resources resulting from the loss or theft of information technology equipment.

Damage to IT Equipment

Should College-issued equipment become damaged, for any reason, employees must report the damage immediately to the Technology Services department. The equipment will be evaluated by Technology Services personnel to determine whether repair or replacement is needed.

When equipment is damaged beyond repair, it will be securely disposed of in accordance with NC Statewide Information Technology Standards.

Loss or Theft of IT Equipment

If the loss or theft occurs off-campus, report it to the local law enforcement authority first. Next, whether on- or off-campus, report the loss or theft to Campus Security, at 638-7261.

Include in the report to Campus Security, at a minimum, the following,

- Whether the device was on and logged into the College network when stolen
- If the device contained files with sensitive College data
- Encryption and password status of any files, if applicable

The IT department will reset user passwords associated with the device and block access to network resources. Users will then be required to change passwords and any other applicable login credentials, to regain network access.

If there was a potential compromise of sensitive information or exposure of network resources, the Dean of Technology will confer with appropriate College officials and/or legal counsel, coordinate notification of affected individuals, and report the incident to State or Federal agencies as required.

User Security Precautions

When using a college-owned IT device (e.g., laptop, smart phone, iPad, or other) or a personally-owned device to access the College's computer network, or when storing files with sensitive College data on any device, take the following precautions:

- Do not leave devices unattended in a public area or visible in a parked car even "for a moment,"
- Utilize a login password for the device, and
- Store sensitive College data, as much as possible, only on approved College network storage drives rather than on mobile devices or laptops, and access the data using the College's virtual network (VPN) facilities.

Return to Table of Contents