Disconnect Policy

Attacks on and intrusions into university electronic resources are continual, serious, and threatening. To prevent catastrophic damage to these resources (including the normal operation of telephone, email, internet, management systems, video, etc.), given the sophistication and speed of intrusive hardware and software, the university must have a capability to immediately address and respond to attacks and intrusions.

The Director of Technology Services (TS) or designee, having the responsibility to maintain and operate the campus infrastructure, has the authority to implement emergency security measures to protect campus electronic resources. These measures may involve shutting off or disconnecting portions of the campus network, blocking certain communication ports, implementing software and/or anti-virus updates, shutting down servers or workstations as a response to immediate threats or attacks to the campus electronic resources.

The Director shall notify senior administration of actions taken in emergency situations, as noted above, as soon as practical. Those units affected by such emergency actions shall be notified and consulted in a timely manner.

Approved by IETCC December 11, 2003