UNIVERSITY OF Cincinnati Clermont College **Category:** Information Technology **Applicable for:** Faculty/Staff/Students	*Procedure/Guideline Title:* **System Security** **Effective Date:** 11.16.2016 **Prior Effective Date:** **Enabling Act:** Technology Steering Committee Approval	*Number:* **034.TS.104** **Owner:** Technology Steering Committee **Responsible Office(s):** Technology Services

Background

As an institution of higher learning, UC Clermont both uses information technology and provisions it to the members of the university community. These guidelines have been developed to create a framework that ensures an effective and secure technology infrastructure for all faculty, staff, students and visitors at the college. The primary directive of technology at UC Clermont is to support, promote and enhance the learning process.

As per the University of Cincinnati's policy on Information Technology, all operating units that use information technology shall be responsible for:

- Developing and implementing, when appropriate, additional IT policies, guidelines or procedures specific to their academic or administrative units.

Guidelines

- Central Login Credentials

  UC Clermont utilizes the UC Central login credentials for device and network access. This is done via a "connector" from UC AD domain to UC Clermont's UCCC domain.

- Network Management

  Management done by Technology Services utilizing software products that allow for central management and configuration backups of all network switches.

  Additional management support by UCit Network Operations Center including monitoring of network utilization and traffic ingress and egress.

Physical Security

- Nightly shutdown of lab workstations

  Automated shutdown of all student lab machines at 11:30pm daily
  Automated power on for patch and antivirus maintenance at 6:00 am daily

- Mission critical production servers in secure location

  Servers housed in a single secure location
  Multi door access to server room
  Node room key required for room entry

- Mission critical production servers maintained with fault tolerance
  Virtualized servers hosted on server cluster and data stored on SAN, all of which utilize RAID and system redundancies/

Prevention of unauthorized access

- Enforce user password changes every 180 days.
- Passwords must be at least eight characters long.
- Passwords must contain at least 1 upper-case character, 1 lower-case character and 1 number or special character.
- Passwords may not contain user name or any part of the end user's full name.
- The server will maintain a list of a user's last ten passwords. In order to keep passwords unique end users will not be able to re-use their ten most recent passwords.
- Accounts will be locked out after four failed logon attempts, and will be locked out for 5 minutes. The count of failed logon attempts will be re-set after five minutes.

Detection of security breaches

- Install/maintain desktop anti-virus software.
  Network Associates, McAfee installed on all UC Clermont workstations
- Automation of desktop anti-virus files
  Virus definition files setup for auto update on a daily basis on all faculty/staff/student machines. *Precluded by implementation of McAfee ePO server

  Virus definition files updated via McAfee ePO server on a daily basis on all faculty/staff/student machines
- Automation of server anti-virus files
  Virus definition files setup for auto update on a daily basis on all servers

Use of Information Technology
http://www.uc.edu/content/dam/uc/infosec/docs/policies/Use_of_Information_Technology_Policy.pdf

Contacts
Technology Services 513.732.5216