

## Campus Computing

### Risk of Loss

Customer Satisfaction

### Contributing Factors

Defective Cabling  
Inappropriate/Inadequate cabling  
Network component failure (eg. Switches, Hubs, Cards, etc.)  
Cables being cut  
Inadequate response from telecom vendor(s)  
Cable not available to establish connection  
Insufficient bandwidth available  
Excessive usage (controlling bandwidth)  
Lack of backup equipment (redundancy) (network or internet downtime)  
Obsolete equipment  
Lack of scheduled maintenance  
Lack of skilled technicians to install and maintain equipment  
Defective equipment  
Inadequate equipment to facilitate operations  
Power spikes and dips  
Interruption in power supply  
Natural and Man Made Disasters  
Mishandling equipment during office relocations/moves  
Equipment overheating and/or exposure to moisture  
Obsolete application/operating systems  
Insufficient file storage (eg. E-mail application-attachments)  
Lack of training  
Lack of manpower to resolve software problems  
Application software does not facilitate tasks at hand  
Under utilization of application  
Lack of standardization - Hardware and Software  
Resources do not match expectations  
Acquisitions of hardware and software not matching long range plans  
Not providing technical assistance

Regulatory

Not developing an Internet privacy policy and statement by 12/01/00.  
Not publishing the Internet privacy statement on CNU's web site in a conspicuous manner by 1/01/01.  
Not making CNU forms available via the Internet to citizens by December 31,2000.

## Regulatory

Not developing procedures to ensure protection of personal data collected and stored which are consistent with the Privacy Protection Act of 1976.

Not incorporating electronic signature technology with the web enablement identified in plans -internal and external transactions.

Utilizing agency-owned or agency-leased computer equipment to access, download, print or store any information having sexually explicit content.

Not informing employees of the restrictions related to access, download, printing or storing information having sexually explicit content.

Publishing web sites (CNU, Faculty, Staff, Students) on university owned servers which contain "indecent" and "patently offensive material".

Utilizing telecommunications equipment to transmit communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age.

Selling or releasing the names or electronic mail or message addresses of any subscriber without the prior consent of the subscriber.

Not documenting security procedures for government databases and communications.

Interception and disclosure of wire, oral, or electronic communications.

Unlawful access to stored communications.

Releasing excluded information.

Not maintaining current information technology plans that have been approved by the CIO.

Searching or seizing materials when individual is not suspected of a crime.

Copyright infringement

## Security

Theft of equipment

Theft/Destruction of proprietary information

Natural and Man Made Disasters

Sabotage

Vandalism

Electronic Eavesdropping

Transmitting illegal or improper information (eg. Hot Mail) via labs

Disclosure of proprietary information (via web, email, etc.)

Downloading or loading viruses

## Operational

Not web enabling business processes (computer center only)

Design of web pages inhibit interaction with target market

Inaccurate information on web pages

Operational

- Untimely update of web pages
- Inadequate web server response
- Not aware of technology available
- Not site licensing widely used software packages
- Not upgrading to most recent version of widely used software packages
- Decentralization of procurement
- Procurement of hardware and software doesn't meet process needs
- Not establishing accountability for all phases of system implementation
- Untimely implementation
- Insufficient resources to implement change
- Ineffective resources to implement system change

Financial

- Not web enabling processes
- Not standardizing basic desktop packages
- Not prioritizing hardware and software applications to coincide with CNU Business Plan
- Acquiring duplicate hardware or software
- Not establishing business partners
- Not availing self for beta testing of hardware or software
- Inadequate student computing fees
- Disproportionate allocation of appropriations and fees among departments
- Application program code changes (HARCO only as it relates to fraud)
- Inability to restore applications and recover information after "system crashes"