



OFFICE OF INFORMATION TECHNOLOGY

**CAPSTONE
POLICY - IS04**

**UNIVERSITY IT INFRASTRUCTURE
RESPONSIBILITIES AND SERVICES**

RESPONSIBLE ADMINISTRATOR: VICE PROVOST FOR INFORMATION TECHNOLOGY
RESPONSIBLE OFFICE(S): OFFICE OF INFORMATION TECHNOLOGY
ORIGINALLY ISSUED: APRIL 2007
APPROVALS: APPROVED BY THE EXECUTIVE VICE PRESIDENT AND PROVOST:

Neal J. Smatresk

Date

APPROVED BY THE PRESIDENT:

David B. Ashley

Date

REVISION DATE: 15-JAN-09

POLICY REVIEW PERIOD: EACH JULY

SECURITY RESPONSE PRIORITY LEVEL: (NA)

STATEMENT OF PURPOSE

The purpose of this policy is to directly support State of Nevada and Federal privacy legislation, codes and laws, and the foundation of the UNLV implementation of the NSHE Board of Regents Bylaws (Title 4, Chapter 1, Section 27 titled Data Security Policy). To provide management direction and support for information security in accordance with business requirements and relevant State and Federal laws and regulations. This Capstone policy, in concert with Capstone Policy IS01 - *Information Security for Information Resources and Assets* and the other Capstone policies, assists in defining the strategic need and direction for UNLV information security.

ENTITIES AFFECTED BY THIS POLICY

This policy impacts all Academic Colleges, Schools and Departments, and all faculty, staff, students, and contractors at all levels.

WHO SHOULD READ THIS POLICY

This policy should be read by all members of the campus community, all entities that do business with the University, as well as periodic and one-time visitors to UNLV.

POLICY

Networks are the highways of information exchange and security through standards preserves these computing resources. All UNLV organizations and personnel operating or administering IT networks shall meet the mandatory requirements and standards included herein for the network configuration and security of UNLV networking equipment, communications, IP-telephony, and systems. This policy focuses on and assists in ensuring an information technology infrastructure that promotes the missions of the University in teaching, learning, research, patient care, and administration.

SCOPE AND APPLICABILITY: The information infrastructure is a significant and critical asset of UNLV. The University network is a shared resource used to support the University's mission of teaching, research, and public service, and to conduct the University's business. It is accordingly necessary to manage the network in such a manner as to ensure its availability for these purposes, and also, to the extent that elements of the network or services running on it interact with external networks, ensure conformance with responsible behaviors (in the sense of network protocol usage, defenses against hacking, etc.). This Capstone Policy primarily addresses the provisioning of network services and the allocation of related responsibilities to ensure the availability of the network and network services now and in the future. Additionally, the assignment of published network names to network resources must be consistent with University communications standards and strategies.

The Policy applies to all University computing networks/systems and organizations, individual schools, departments, University laboratories, and other University-based entities owning, directing, or operating IT network systems or devices. This Policy has a primary focus on UNLV networks and networking devices, and supporting facilities. External networks holding UNLV information, even when carried out on a privately owned devices that are not managed or maintained by UNLV, are governed by this Policy where applicable.

BACKGROUND: The wide variety of cyber threats to networks have the potential of causing significant business and academic disruption and significant cost in terms of failed services, service recovery, and expiatory costs associated with the potential loss of protected or sensitive information.

The Policy in many cases assigns prerogatives to the Office of Information Technology (OIT) department. The impetus for this is the need to ensure the interoperability of the various network elements and services, the desire to minimize the time needed to diagnose and resolve network problems, and the need to ensure the University's ability to evolve the network infrastructure to meet UNLV needs and to stay in step with changes in external networks (such as the migration from Internet Protocol v4 to Internet Protocol v6).

The policy does not apply to non-UNLV networks or stand-alone UNLV networks except when connected to UNLV networks or holding University information.

In order to manage information networks and security comprehensively, this policy aims to promote the following goals:

- To ensure that use of IT systems is consistent with sound networking and security principles;
- To ensure that IT systems are used for their intended purposes and meet any compliance requirements;
- To ensure the confidentiality, integrity, availability, and superior performance of IT networks;

◆ Note: The focus of this policy is on the security of information technology devices and resources, and not on specifics for the management of data or any particular class of data. For information concerning data, please consult University policies for data stewardship and custodianship, which provide the authority for and guidance towards the development of policy for the preservation and proper management of data in specific functional areas.

POLICY STANDARDS AND CONTROLS: See the ANNEX for STANDARDS for mandatory baseline Policy Standards and Controls that are required to be implemented to be in minimum compliance with this policy and its objectives. Each UNLV administrative department is responsible for development of appropriate internal procedures and directives to implement and comply with this policy for their organization.

Additional subordinate tiers of information security policies, standards, and directives, will focus on common security standards for low-impact systems and specific technological and application security standards for both moderate-impact and high-impact systems. The structure will provide an emphasis on assuring that:

- Confidentiality of information will be assured;
- Integrity of information will be maintained;
- Availability of information for business processes will be maintained;
- Legislative and regulatory compliance requirements will be met; and
- Business continuity plans will be developed, maintained and tested.

COMPLIANCE: It is the responsibility of the UNLV Provost OIT to administer and maintain this Policy and all related information security policies. Policy compliance requirements are:

1. UNLV management has the responsibility to manage University information, personnel, and physical property relevant to academic and business operations, as well as the right to monitor the actual utilization, but not the content except under pre-approved conditions, of all University assets.
2. Information security reviews and security audits will be conducted annually or more frequently as required. The UNLV Information Security Officer, or appointed designee, will conduct security policy reviews and security audits.
3. In addition to any possible legal sanctions, UNLV employees and students who fail to comply with the policies will be considered in violation of the University's relevant codes of conduct and may be subject to disciplinary action and a level of infraction up to and including dismissal or expulsion, pursuant to Campus policies, collective bargaining agreements, codes of conduct, or other instrument governing the individual's relationship with the University. The level of infraction and recourse to such actions shall be as provided for under the provisions of those instruments.
4. The Policy shall also be maintained and enforced with assistance from the UNLV Provost, UNLV Administrative Code Office NSHE Legal Counsel, NSHE Board of Regents Bylaws, and System Computing Services (SCS).

AUDIT STANDARDS AND CONTROLS: Compliance and effectiveness auditing of this policy shall be accomplished using the appropriate BS 7799.2:200x Audit Check List, dated 8.08.2005 or later, and through a complete review of all related misuse complaints (security incidents) that occurred after the previous audit. The audit shall inspect the in-use security applications, procedures, and processes of

systems supporting this policy, including timeliness of updates, for compliance to the policy. The UNLV ISO, or designee, shall be the ombudsman, manager and principal reviewer of this policy. Proposed adjustments and enhancements to the policy for unforeseen issues shall be presented to the Responsible Administrator of this Policy for approval. An audit report and recommendations shall be sent to the Vice Provost for Information Technology.

DISPUTE RESOLUTION (ENFORCEMENT): The Provost shall have the final authority in resolving disputes concerning the Policy enforcement including the use of domain names, IP address spaces, network devices, and network services.

ROLES AND RESPONSIBILITIES: See the ANNEX for ROLES AND RESPONSIBILITIES for the policy responsibilities of Administrative Officials, IT Providers, and Users.

EXCEPTIONS: (None)

RELATED DOCUMENTS

UNLV IT POLICIES -Information security policy structure is based on:

- ISO 17799/27001 – the International Standard for Information Security, and
- enhanced as needed by the [Federal Information Processing Standards \(FIPS\) Pub 199](#) Standards for Security Categorization,
- the *National Institute of Standards and Technology (NIST) Special Publication 800-series* reports on the Information Technology Laboratory's research related to information security controls, standards, and guidelines.
- The standard reference text for ISO 17799/27001 policy development is the most current edition of *Information Security Policies and Procedures: a practitioner's reference*, Thomas R. Peltier, Auerback Publications or it's replacement.

SERIES IS – CAPSTONE POLICIES GROUP (Tier 1)

Policies that establish the foundation for information security and information assets policies.

<i>IS01</i>	<i>Information Security for IT Resources Policy**</i>
<i>IS02</i>	<i>Information Sensitivity and Classification Policy (with Handbook)**</i>
<i>IS03</i>	<i>Personal Non-Public Information Policy**</i>
<i>IS04</i>	<i>Infrastructure Responsibilities and Services Policy**</i>

SERIES IST100 – INDIVIDUAL PRIVILEGES & RESPONSIBILITIES GROUP (Tier 2)

Policies that address acceptable personal use of the computing services, assets, and networks.

<i>101A</i>	<i>Acceptable Use of IT Resources Policy (Users)**</i>
<i>101B</i>	<i>Acceptable Use of IT Resources Policy (Mgmt & SysAdmin)**</i>

SERIES IST400 – IT OPERATIONS & PROVISIONING GROUP (Tier 2)

Policies that provide for monitoring and logging, provisioning and implementation, assessment and compliance, system administration, remote access, physical security, configuration management, and training and awareness programs.

<i>402</i>	<i>Risk Assessment and Management Policy (with Handbook)**</i>
<i>406</i>	<i>Data Media Sanitization & Destruction Policy (with Guide)**</i>

BEST SECURITY PRACTICES SERIES

- BSP-1 Password Standards For Personal Systems (With Guide)
- BSP-2 IT Server Resources Used For Unrestricted Information
- BSP-3 Password Standards For Servers And Network Devices
- BSP-4 Virus, Trojan, Spyware & Other Malicious Code Prevention
- BSP-5 Reporting Electronic Security Incidents
- BSP-6 What To Do For A Computer Security Incident (For System And Security Administrators)
- BSP-7 Computer Security Of User Systems
- BSP-8 Data Media Sanitization & Destruction
- BSP-9 IT Resources Requiring Compliance Protection For Sensitive, Critical, Or Regulatory Information

The following Best Security Practices are, fully or partially, restricted because of content, have limited distribution to system and security administrators, and are only available via internal UNLV mail by contacting the UNLV Information Security Office for further information and prerequisite requirements.

- BSP-2(R) IT Server Resources Used For Unrestricted Information*
- BSP-3(R) Password Standards For Servers And Network Devices*
- BSP-6(R) What To Do For A Computer Security Incident (For System And Security Administrators)*
- BSP-9(R) IT Resources Requiring Compliance Protection For Sensitive, Critical, Or Regulatory Information*
- BSP-9(R)A IT Resources Requiring Compliance Protection For Sensitive, Critical, Or Regulatory Information (Supplement)*
- BSP-10(R) Critical Network Resources*
- BSP-10(R)A Critical Network Resources Supplement*

CONTACTS

OFFICE OF INFORMATION TECHNOLOGY
Herman W Westfall (HWB), Room 101
(702) 895-3628 / FAX (702) 895-1847

Subject	Contact	Telephone	Email/URL
Policy Clarification	Office of Information Technology	(702) 895-0500	http://www.UNLV.edu/infotech/policy.html
Legal Issues	Administrative Code Officer	(702) 895-1879	- none -
Information Security	Information Security Officer	(702) 895-5284	informationsecurityoffice@unlv.edu
Campus Computing Services	Director of Campus Computing Services	(702) 895-0787	- none -

Enterprise Applications Services	Director of Systems & Applications	(702) 895-1765	- none -
----------------------------------	------------------------------------	----------------	----------

DEFINITIONS

Key Definitions for this policy:

****Intermediate distribution frame (IDF):*** In a UNLV building premises, a frame that (a) cross-connects the UNLV cable media to individual user line circuits and (b) may serve as a distribution point for multipair cables from the main distribution frame (MDF) or combined distribution frame (CDF) to individual cables connected to equipment in other building areas remote from the frame room.

****Main distribution frame (MDF)*** is a distribution frame on one part of which the external trunk cables entering a facility or building terminate and on another part of which the internal user line circuits and trunk cabling to any intermediate distribution frames (IDF) terminate. The MDF is used to cross-connect any outside line with any desired terminal of the multiple cabling or any other outside line. The MDF usually holds central office protective devices and functions as a test point between a line and the office. The MDF in a private exchange performs functions similar to those performed by the MDF in a central office.

****Combined distribution frame (CDF)*** is a distribution frame that combines the functions of main IDF and intermediate distribution frame (IDF) and contains both vertical and horizontal terminating blocks. The vertical blocks are used to terminate the permanent outside lines entering the building. Horizontal blocks are used to terminate inside plant equipment. This arrangement permits the association of any outside line with any desired internal equipment. These connections are made either with wire or with optical fiber cables.

****UNLV IT network infrastructures, IT systems, and related supporting equipment*** are assigned tiers according to the role performed for the University:

- TIER 1 is the UNLV campus and metro-area network(s), including support systems, and hereafter is collectively referred to as the UNLV Enterprise Network system.
- TIER 2 is any system or network that contains Essential or Restricted Electronic Information Resources needed for mission-critical support within the University or required compliance support by act, statute, regulation, or public law.
- TIER 3 is all other general systems or networks.

Additional Definitions of terms in this and other policies can be found in UNLV OIT document "***Information Security Acronyms, Terms and Definitions***".

ANNEX 1 – POLICY STANDARDS

BASELINE SECURITY STANDARDS AND CONTROLS. The following are the Policy Standards that shall be implemented to be in minimum compliance with the Policy.

POLICY STANDARD: IS04-1 Enterprise Network Defined. The UNLV Enterprise Network is the central routing and distribution network and collectively includes: 1) all on-campus physical distribution facilities, such as IDF's, etc., or authorized subdivided secure portions thereof, that allow physical access to the terminus points of the central network; 2) all distribution devices such as security devices, routers, switches, and similar devices that provide the primary routing, distribution, and security services to the physical terminus points. The Enterprise Network is classified as a Tier 1 system.

The Enterprise Network is the sole responsibility of the UNLV Provost, Office of Information Technology and provides the University with Internet access, common digital access and distribution of email and other information/data, IP telephony, common digital interconnection (cable plant) between and within buildings and organizations, and non-wired access.

Adjunctive Networks are defined as non-Enterprise Network subnetworks that are connect to the Enterprise Network through the use of additional distribution devices or methods. These are authorized subnetworks, frequently provided by or for a UNLV organization or entity, containing internal distribution services and other digital equipment including desktop computers. The Adjunctive Networks may be operated directly by the responsible UNLV organization or entity or they may be operated by OIT on behalf of the UNLV organization or entity. Other Adjunctive Networks may be authorized stand-alone local networks. Stand-alone (non-Internet connected) local networks that contain sensitive data shall not have external non-wired access. All Adjunctive Networks shall comply with all information security policies and standards at all times.

POLICY STANDARD: IS04-2 Domain Names. The following provisions shall be observed:

- All official University services that are advertised and/or accessible via domain name services must use domain names that are owned or effectively controlled by UNLV.
- All such domain names must refer to sub-domains of **unlv.edu**, except where special permission is granted.
- Special permission will be granted only in cases where UNLV is acting as host for a non-UNLV organization or function.
- IT will coordinate the assignment of sub-domain names within the **unlv.edu** domain, delegating the assignment of additional naming within sub-domains as appropriate.
- Domain Name Services (DNS) will be furnished by OIT, except where special permission is granted to a unit or group to run their own Domain Name Server.
 - Such permission is intended to be accorded when there is a reasonable, demonstrated need to run such a service, when the technology level of the platform providing the service is deemed to be adequate, and when the staff responsible for running the service has the appropriate skills, and is available to assist in problem determination.
- Domain names shall not contain words or expressions that reasonable people may believe to be potentially offensive to any group.

POLICY STANDARD: IS04-3 Universal Resource Locators (URLs). The following provisions shall be observed:

- All official University activities that are web-based must be conducted on sites whose domain names are owned or effectively controlled by UNLV.
- All official University activities that are web-based must be conducted on sub-domains of **unlv.edu**, except where special permission is granted. Special permission will be granted only in cases where UNLV is acting as host for a non-UNLV organization or function.
- For the University web site, OIT will coordinate the assignment of qualifiers that occur receding or following the domain name within the URL (i.e., <http://qualifer1.unlv.edu/qualifier2/etc...>), by delegating the assignment of additional qualifiers as appropriate.
- URLs shall not contain words or expressions that reasonable people may believe to be potentially offensive to any group.

POLICY STANDARD: IS04-4 Internet Protocol (IP) Addressing. The following provisions shall be observed:

- All computers and other devices directly connected to the University network must use IP addresses that are assigned to the University and managed by OIT or an authorized delegate.
- OIT will allocate portions of the University IP address space to buildings, organizational units, logical entities, or otherwise, as it deems appropriate, to the end of providing for availability, management, scalability, and future expansion.
- OIT will delegate the management of portions of the University IP address space to groups or organizational units that have the ability and requirement.
- OIT will operate all Dynamic Host Configuration Protocol (DHCP) servers except when special permission is granted to other organizations as appropriate.
 - Such permission is intended to be accorded when there is a reasonable, demonstrated need to run such a service, when the technology level of the platform providing the service is deemed to be adequate, and when the staff responsible for running the service has the appropriate skills, and is available to assist in problem determination.

POLICY STANDARD: IS04-5 Ownership and Responsibilities. All internal network devices deployed at UNLV must be "owned" by either OIT or another University authorized operational IT entity or unit that is technically trained and responsible for infrastructure and device administration. The OIT shall be totally responsible for the UNLV Enterprise Network infrastructure deployment and operation including physical security and access control.

Approved configuration guides must be established and maintained by each group, based on academic and business needs and approved by a designated information system security officer (ISSO). Operational IT units should monitor configuration compliance and implement an exception policy tailored to their environment but not in violation with UNLV security policies. Each operational IT unit must establish a process for changing the configuration guides, which includes review and approval by a designated ISSO.

- Network devices are information assets and must be registered within the UNLV enterprise IT management system. At a minimum, the following information is required to positively identify the point of contact:
 - Device contact(s) and location, and a backup contact
 - Hardware and Operating System/Version

- Functions, applications, and data sensitivity (see Policy IS02).
- Device information in the UNLV enterprise management system must be kept up-to-date.
- Configuration changes for production devices must follow the appropriate change management procedures.
- Asset classification and risk assessments shall have been performed.

POLICY STANDARD: IS04-6 Routers and Switches. The following provisions shall be observed:

- Routers and Layer 3 switches will be deployed and managed exclusively by OIT.
- Layer 2 switches will normally be deployed and managed by OIT. Other IT units may be delegated or assigned to operate the devices when appropriate.
- Procurement of network equipment, even if financed outside of OIT, will be the responsibility of OIT, in accordance with established campus standards and negotiated vendor contracts.

POLICY STANDARD: IS04-7 Wireless Devices. The following provisions shall be observed:

- OIT is responsible for deployment, operation and security of wireless networking on campus, and for publishing guidelines on the use of equipment that may interfere with the operation of wireless networking.
- OIT may delegate the right to install and operate wireless access points to other units only under very limited circumstances. When so delegated, the wireless devices and services shall conform to OIT security policies.

POLICY STANDARD: IS04-8 Authentication and Security. The following provisions shall be observed:

- OIT has over-arching responsibility for ensuring the security of the wired and wireless aspects of the campus network, including the connection of remote devices and networks by dial-up or other data communication technologies.
- OIT will allow access only through IP ports and protocols consistent with assignment and usage as specified and/or recognized by the Internet governing bodies and general usage, and known not to be unusually vulnerable to external threats. OIT will publish the list of usable ports and work on a good faith basis to enable additional ports when requested.
- OIT may temporarily, and before giving notice, block normally usable ports under the existence or threat of a known attack until protective measures are taken on computers and/or network devices internal to the campus network.
- OIT has the right to impose reasonable authentication requirements on devices connected to the campus wired and/or wireless networks, and to restrict or manage the connection of remote devices.

POLICY STANDARD: IS04-9 Network Monitoring. The provisions in this standard are subject to the individual privacy provisions mandated in the UNLV Acceptable Use Policy. The following provisions shall also be observed:

- OIT has the right to run software which inspects network traffic and/or device configurations to:
 - analyze network performance and resource utilization,
 - perform intrusion protection and detection,
 - scan to detect and audit security vulnerabilities on network servers and other computers,
 - perform approved security penetration testing for security auditing purposes,

- ascertain the presence of appropriate virus/malware detection software and other security software on network computers,
- scan/monitor to detect the active execution of hacking or virus/worm distribution programs.
- Analysis of packets captured to study performance, utilization, and similar activities will be performed only in the aggregate and will not include human inspection of individuals' data.
 - The capture and analysis of individual packets may be necessary to resolve specific problems or security exposures. In this case, only packet types needed to perform problem determination will be inspected, and affected users will be notified prior to such activities, always assuming that they can be identified before the fact. Inspection of packet contents shall be limited to those fields directly relevant to problem determination.

POLICY STANDARD: IS04-10 Incident Monitoring. The following provisions shall be observed:

- In the case of immediate danger to the availability of the campus network or in any similar situation deemed to present a high risk, OIT may disconnect devices from the campus network without prior notice. However, in such cases, OIT should make a good faith effort to contact the responsible and/or affected parties before such action is taken, and, if unsuccessful, continue such efforts after action has been taken.
- In other cases where undue vulnerabilities and/or violations of this Policy are detected, disconnection of devices shall occur only after multiple notifications have been issued to the responsible parties and only after a reasonable amount of time has passed that would allow for vulnerabilities to be corrected.

POLICY STANDARD: IS04-11 Physical Security and Access Control. Access to UNLV physical networking infrastructure, servers, and other computers operated by an authorized IT organization shall be restricted to authorized IT personnel of that organization. These facilities include: main distribution frame (MDF) closets; intermediate distribution frame (IDF) closets; combined distribution frame (CDF) closets; local area network (LAN) closets; network router and hub rooms; voice mail system rooms; IP telephony rooms; and any similar areas containing communications or networking cabling and devices that must be kept securely locked at all times and not accessed without an authorized IT escort.

All infrastructure equipment controlled by an IT organization must be physically isolated from other equipment not under control by that IT organization. The parent organization shall be responsible to ensure that all UNLV network devices under their control shall be protected by either housing the devices in a dedicated secure closet or a dedicated secure cabinet. Additionally:

- Access to the above areas, rooms, and closets must be protected with physical security measures that prevent unauthorized (non-IT) persons from gaining access without authorized IT escort.
- Access to the areas, rooms, and closets shall be fully and securely logged by the responsible IT organization and access-control logs shall be audited, at a minimum, quarterly by the responsible ISSO.
- Networking or distribution devices are specifically prohibited from operating in uncontrolled (open) desk or office areas.

POLICY STANDARD: IS04-12 Compliance Audits. Information security audits will be performed on a regular basis by authorized OIT security personnel within UNLV. The security audits will be managed by authorized OIT security personnel, in accordance with the *IT Security Audit Policy* and shall include appropriate vulnerability and penetration testing. Information security will filter findings not related to a specific group and then present the findings to the appropriate support staff for remediation or justification. Every effort will be made to prevent audits from causing operational failures or disruptions.

INCORPORATED OTHER STANDARDS AND DIRECTIVES OF THE POLICY: In addition to the core security requirements and standards above, Additional Directives may be incorporated to amend the primary Policy to address, define and promote special IT security standards for unique groups of constituencies or security devices to ensure a secure and reliable information technology infrastructure.

ANNEX 2 –ROLES AND RESPONSIBILITIES

ACCOUNTABILITY:

Administrative Officials (individuals with administrative responsibility for campus organizational units [e.g., control unit heads, deans, department chairs, principal investigators, directors, or managers] or individuals having functional ownership of the infrastructure) must:

- Identify and classify the digital information assets within areas under their control;
- Establish acceptable levels of security risk for resources by assessing factors such as:
 - The level of business criticality or overall importance to the continuing operation of the University as a whole, individual departments, research projects, or other essential activities;
 - How the operations of one or more units would be affected by the loss, unavailability or reduced availability of the assets,
 - How likely it is that an asset could be used as a platform for inappropriate acts towards other devices, persons, or organizations, and
 - Limits of available technology, programmatic needs, cost, and staff support;
- And Ensure that requisite security policies, standards, and safeguards are implemented and monitored for the assets.

Providers (A local infrastructure provider is the organization with principal responsibility for the installation, configuration, security, and ongoing maintenance of the IT device(s) comprising the local infrastructure.) must:

- Be knowledgeable and comply with the current policies, requirements, guidelines, procedures and protocols concerning the administration and security of the University information technology infrastructure resources;
- Analyze potential threats and the feasibility of various security measures in order to provide recommendations to Administrative Officials;
- Implement approved security measures that mitigate threats, consistent with the level of acceptable risk established by Administrative Officials;
- Establish procedures to ensure that privileged or special accounts are kept to a minimum and that privileged users comply with privileged/special access agreements;
- For systems in support of University business administration, establish procedures to implement relevant provisions of other UNLV policies, such as incident response and recovery;
- Communicate the purpose and appropriate use for the assets under their control.

Users (individuals who access and use local infrastructure resources) must:

- Become knowledgeable about relevant University security requirements and guidelines;
- Protect the assets under their control, such as access passwords, computers, and data they download or access.

Other entities with important campus electronic information resource security responsibilities include **Campus Computing Services, Network Operations Center, Systems and Applications**, and miscellaneous other **Information Technology groups** in various departments, schools, etc.

Insufficient security measures at any level may cause infrastructure resources to be stolen, damaged, or become a liability to the University. Therefore, responsive actions may be taken. For example, if a situation is deemed serious enough, devices or subnets posing a threat will be blocked from network access. (The campus "Guidelines and Procedures for Blocking Network Access" specify how the decision to block is made and the procedures involved.)