


<p>CAMPUS POLICY</p>  <p>UNIVERSITY OF COLORADO at COLORADO SPRINGS</p>	POLICY NUMBER: 700-004	PAGE NUMBER: 1 of 7
	CHAPTER: Information Technology	
	SUBJECT: Wireless Networks	
	EFFECTIVE DATE: February 1, 2006	
	SUPERSESSSION:	
OPR: Chancellor VC:	Approved by Pamela Shockley-Zalabak, Chancellor, on February 1, 2006	

I. POLICY

This policy is to help ensure the security and availability of information technology systems and networks and the confidentiality and integrity of electronic information captured, maintained, and used by UCCS. This policy should be used as the foundation document for all standards, procedures, and guidelines that are developed and implemented by UCCS related to information systems and data security.

II. AUTHORITY FOR CAMPUS POLICIES

Authority for the creation of campus administrative policies is found in *The Laws of the Regents*, 1990, Article 3 Section B.8, which states:

The chancellor of the University of Colorado at Colorado Springs shall be the chief academic and administrative officer responsible to the president for the conduct of affairs of the Colorado Springs campus in accordance with the policies of the Board of Regents. The chancellor shall have such other responsibilities as may be required by these *Laws*, the Board, and as may be delegated by the president.

III. PURPOSE

To ensure the technical coordination required to provide the best possible wireless network for the University of Colorado at Colorado Springs (CU-Colorado Springs), the campus' Information Technology Department (IT) will be responsible for the deployment and management of IEEE 802.11 (802.11) and related wireless equipment on the campus. Other departments needing to deploy wireless equipment that uses university resources may do so by coordinating with IT.

This policy provides the structure for a campus-wide solution for the implementation of wireless technologies, which includes centralized determination of identity and authentication to the end of the provision of the appropriate levels of security.

CHAPTER: 700 Information Technology	SUBJECT: Wireless Networks	POLICY: 700-004	EFFECTIVE: February 1, 2006	PAGE: Page 2 of 7
--	-------------------------------	--------------------	--------------------------------	----------------------

IV. DEFINITIONS

The following terms are found in this policy document or its associated guideline documents:

Access Control: A physical, procedural, and/or electronic mechanism that ensures only those who are authorized to view, update, and/or delete data can access that data.

Authentication: A systematic method for establishing proof of identity.

Authorization: The process of giving someone permission to do or have something. System administrators/owners and data custodians define for their systems which users are allowed access to those systems and what privileges are assigned. A system could be an operating system, database, or application.

Availability: The assurance that a computer system is accessible by authorized users whenever needed or as pre-defined.

Common Criteria for Information Technology Security Evaluation: A comprehensive specification (aligned with the ISO IS 15408) that first defines the targeted environment and then specifies the security requirements necessary to counter threats inherent in that environment.

Confidentiality: An attribute of information. Confidential information is sensitive or private information, or information whose unauthorized disclosure could be harmful or prejudicial.

Cookie: A small text file that is sent to a user's computer by the server that the user is visiting. This file can record preferences and other data about the user's visit to a particular site. Cookies often are used for long-term data collection. Short-term cookies might be used for things like authentication in "single sign-on" services.

Cost-effective: To deliver desired results in beneficial financial terms.

Critical Servers: Within UCCS, critical servers are devices needed to support major UCCS administrative services, or they are devices that contain personally identifiable information that has value in and of itself.

Data Custodians: Individuals who have been officially designated as accountable for specific data that is transmitted, used, and stored on a system or systems within a department, college, school, or administrative unit of UCCS.

Decryption: The process of turning unreadable cipher text into readable text.

Encryption: The process of turning readable text into unreadable cipher text.

CHAPTER: 700 Information Technology	SUBJECT: Wireless Networks	POLICY: 700-004	EFFECTIVE: February 1, 2006	PAGE: Page 3 of 7
--	-------------------------------	--------------------	--------------------------------	----------------------

Firewalls: Policy-based filtering systems (composed of both hardware and software) that control and restrict the flow of data between networked computer systems. Firewalls establish a physical or logical perimeter where selected types of network traffic may be blocked. Blocking policies typically are based on computer IP addresses or protocol type of application (e.g., Web access or file transfer). Types of firewalls relevant to this policy include:

- Integrated OS (operating system) firewalls, bundled with the OS (e.g., Windows, Linux)
- Dedicated firewalls protecting labs or server sanctuaries
- Dedicated firewalls protecting individual hosts
- Logical firewalls protecting non-co-located systems

Forensics (Computer): The discipline of dissecting computer storage media, log analysis, and general systems to find evidence of computer crime or other violations.

Incident Response Capability: The ability to respond appropriately and completely to any incidents, situational compromises, or threats from any source.

Information Systems: UCCS electronic information systems and data assets. All computing systems, networks, digital information, and other electronic processing or communications related resources or services provided through UCCS.

Integrity: Data or a system remains intact, unaltered, and reliable.

Intrusion Detection: A security management system that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

Non-repudiation: A mutually agreed upon process, secured evidence, or other method of operation that provides proof of receipt or protection from denial of an electronic transaction or other activity.

Off Site: A location separate and distinct from the area in which something, such as a computer, is located-- Frequently referred to when considering backup storage.

Ownership: The term that signifies decision-making authority and accountability for a given span of control.

Perimeter Security: The ability to protect the outer limits of a network, or a physical area, or both.

Personally Identifiable Information: Specific data, elements of non-specific aggregate data, or other information that is tied to, or otherwise identifies, an individual or that

CHAPTER: 700 Information Technology	SUBJECT: Wireless Networks	POLICY: 700-004	EFFECTIVE: February 1, 2006	PAGE: Page 4 of 7
--	-------------------------------	--------------------	--------------------------------	----------------------

provides information about an individual in a way that is reasonably likely to enable identification of a person as an individual and make personal information about them known.

Principle of Least Privilege: Access privileges for any user should be limited to only what is necessary to complete their assigned duties or functions, and nothing more.

Principle of Separation of Duties: Whenever practical, no one person should be responsible for completing or controlling a task, or set of tasks, from beginning to end when it involves the potential for fraud, abuse, or other harm.

Privacy: An individual's right to be left alone; to withdraw from the influences of his or her environment; to be secluded, not annoyed, and not intruded upon; to be protected against the misuse or abuse of something legally owned by an individual or normally considered by society to be his or her property.

Privacy Statement: Sometimes referred to as a privacy policy, a privacy statement is posted on an organization's Web site to notify visitors of the types of information being collected and what will be done with the information.

Risk Management: A comprehensive methodology that strives to balance risks against benefits in a pre-defined environment.

Security: An attribute of information systems that includes specific policy-based mechanisms and assurances for protecting the confidentiality and integrity of information, the availability and functionality of critical services, and the privacy of individuals.

Security Incident: An event during which some aspect of computer security is threatened.

Server Sanctuaries: Within UCCS, these are locations within computing facilities where clusters of sensitive or critical servers can be co-located and around which suitable physical and logical security measures can be implemented.

System: A network, computer, software package, or other entity for which there can be security concerns.

System Administrators: Individuals who support the operations and integrity of computing systems and their use. Their activities might include system installation, configuration, integration, maintenance, security management, and problem analysis and recovery. In addition, managing the computer network is often their responsibility in an inter-networked computing environment.

System Management: The activities performed by systems administrators.

CHAPTER: 700 Information Technology	SUBJECT: Wireless Networks	POLICY: 700-004	EFFECTIVE: February 1, 2006	PAGE: Page 5 of 7
--	-------------------------------	--------------------	--------------------------------	----------------------

System Operators: Individuals within the UCCS community who are accountable for the operational decisions about the use and management of a computing system. (See also *System Owners*.)

System Owners: Individuals within the UCCS community who are accountable for the budget, management, and use of one or more electronic information systems, electronic databases, or electronic applications associated with UCCS. (See also *System Operators*.)

Technicians: Individuals who have technical knowledge about computers, software, hardware, operating systems, and networks (e.g., system administrators, system engineers, or network engineers).

Users: Any individual who has been granted privileges and access to UCCS computing and network services, applications, resources, and information.

UCCS-owned Network: A network where network components (including active elements such as routers and switches, transmission media, and network-attached computers) are owned and operated by UCCS or units of UCCS. A message that travels over UCCS-owned networks is, in general, on an open network and hence requires additional security measures to be considered secure.

V. PROCEDURES

A. Rationale and Purpose of Policy:

Wireless in the Local Area Network using the IEEE 802.11 standard is a fast emerging technology. 802.11 wireless technologies are by nature easy to deploy, but highly sensitive to overlapping frequencies. Because of these characteristics, all wireless use must be planned, deployed, and managed in a very careful and centralized fashion to ensure basic functionality, maximum bandwidth, and a secure network.

Current 802.11 wireless technologies deploy a very low power signal in a frequency band divided into only 3 non-overlapping channels. The primary purpose of these channels is not so much to provide separate networks, but to ensure that adjacent access points with slightly overlapping areas of coverage do not interfere with each other. In the normal case, it is necessary to use all three channels in an integrated fashion as a single unified network in order to achieve an optimal design. It is therefore not feasible to allow individuals to install their own access points without centralized coordination, due to the resulting signal interference and greatly degraded performance to the common wireless network.

B. Scope:

The Wireless Policy provides guidelines regarding the following:

- * The central deployment by IT of 802.11 and wireless equipment.

CHAPTER: 700 Information Technology	SUBJECT: Wireless Networks	POLICY: 700-004	EFFECTIVE: February 1, 2006	PAGE: Page 6 of 7
--	-------------------------------	--------------------	--------------------------------	----------------------

- * The provision of wireless service by IT for campus departments.
- * The management by IT of 802.11 and related wireless equipment.

C. Policy:

1. IT deployment of 802.11 and related wireless equipment

The University of Colorado at Colorado Spring's Information Technology Department (IT) will be solely responsible for the deployment and management of 802.11 and related wireless equipment on the campus. No other departments may deploy 802.11 or related-wireless equipment without coordination with IT.

2. Provision of wireless service by IT

IT will offer a standard wireless deployment plan that will meet the needs of most CU-Colorado Springs departments wishing to construct and operate departmental wireless services. Departments requiring a different wireless deployment plan may contract with IT to have IT construct and operate either a standard or, if the spectrum is available for it, premium wireless services. IT will work with departments to accommodate any special needs they may have within the technical constraints of the wireless technology, understanding that all requests may not be technically feasible.

3. Management by IT of 802.11 and related wireless equipment

IT will ensure that all wireless services deployed on campus will adhere to campus-wide standards for access control. IT will manage the wireless equipment in a manner that ensures the greatest interoperability and roaming ability for all departments wishing to use wireless technology, and, will centralize the process of determining identity, authentication, and appropriate levels of security for access to and use of wireless technology. IT reserves the right to minimize interference to the common wireless network, and will work with departments to reconfigure or shut down any departmental wireless networks that interfere with the common wireless network.

D. Procedures and Guidelines:

IT will advise IT Council on wireless plans, deployment strategies, and management issues.

Any department wishing to work with IT to deploy wireless access must contact IT by web form (<http://www.uccs.edu/~it/wireless/request/>) to begin the process.

In the case of existing wireless technology deployments that use the same or interfering spectrums, IT will work with the departments in question to move wireless equipment to the common wireless network.

All sensitive data being transmitted across a wireless network should be encrypted (see Data Sensitivity Guidelines, link coming soon).

CHAPTER: 700 Information Technology	SUBJECT: Wireless Networks	POLICY: 700-004	EFFECTIVE: February 1, 2006	PAGE: Page 7 of 7
--	-------------------------------	--------------------	--------------------------------	----------------------

Additional guidelines and best practices relating to the deployment and use of wireless technologies can be found at www.uccs.edu/~it/wireless.

E. References:

The Office of the Chancellor will be responsible for this policy and for any appeals of IT decisions relating to wireless deployments. This policy will be reviewed yearly by that office. Changes will be authorized by the approval of the Chancellor's Executive Committee. IT will review LAN wireless access standards on a yearly basis and recommend changes to this policy as needed.

Appendix A—Policy Routing

This policy was approved by the Information Technology Council.

VI. RESPONSIBILITY

- A. The chancellor or designee is responsible for ensuring that all campus policies are current, compliant with all statutory requirements, case law, and consistent with other applicable standards, including the *Laws of the Regents*, and the University of Colorado Administrative Policy Statements.
- B. The director of IT, the IT Advisory Council and IT Leadership Team shall be responsible to:
 - 1. Review and update the security policy annually.
 - 2. Ensure their staff and colleagues are made aware of all applicable University and campus policies.

VII. ATTACHMENTS: