Addendum to CSUIT Security Policy
for
Warner College of Natural Resources
Version 1.06 - July 2010

Given the ever increasing number of security incidents involving higher educational institutions information technologies, as well as a growing need to protect the computing resources at Colorado State University, the CSUIT security group developed a security policy to address these issues in 2005. The policy has several sections addressing the many areas of information technology. This addendum is designed to be a supplement to the CSUIT security policy, not a replacement. If any item in this addendum is found to be in conflict with the CSUIT security policy, then the stronger security policy takes precedence.

The spirit of this addendum is guided by a "best use" scenario and is intended to be a living document. It is subject to change based on technological advancement, real-time security threats and changes in normal business and/or research practices. There may be instances where applying these policies are cost prohibitive, and those unique cases will be dealt with on a case by case basis by the College of Natural Resources IT Manager. Every individual who either owns or works with a computing device connected to the Warner College of Natural Resources computing environment must conform to these policies.

Section I General IT Security Policies and Guidelines:

2. Personal Computers

A personal computer in the Warner College of Natural Resources is defined as any computing device used by faculty, staff, and students used to conduct day to day business or study and is used primarily by one person.
Examples of personal computers are desktop, laptop, PDA, cellular telephone, tablet PC.

5. Files and File Storage

Natural Resources Computing and Network Services (NRCNS) provides safe and secure file storage for individual users and groups of users. If a separate file storage system or a network attached storage device is required, NRCNS must grant approval prior to connecting the device to the network. Peer to peer file sharing is prohibited.

7. Wireless Networks

CSU has created an effective and secure wireless network infrastructure across campus. Although private wireless networks are not allowed, exceptions can be granted on a case by case basis if the CSU wireless is unavailable. NRCNS must register the device(s) before connecting them to the college network. Any device found on the network that has not been registered, will be disconnected and prohibited.

Section II Mandatory, Minimum IT Security Requirements

1. Operating Systems

Computing devices are subject to the following security policies:

- Only operating systems which provide high levels of security shall be used, and security updates (patches) shall be applied in a timely manner.
- Virus protection is mandatory and must be kept up to date. This includes student computing devices.
- Access to campus resources from remote computing devices via external providers (such as Comcast, Qwest, hotel networks, or any wireless network), shall be secure, e.g. encrypted over a VPN connection terminated on the University's VPN concentrator or accessed vi the secure gateway (https://secure.colostate.edu).

2. Network Security

The Warner College of Natural Resources incorporates a firewall designed to better secure the college computing infrastructure. In general, the firewall will mirror the port blocking rules instituted by CSUIT security policy at the campus border. This will protect the college from vulnerabilities and attacks that could occur from within campus. Additional firewall rules are also in effect and they reflect the CSUIT general security policies as they directly relate to CNR servers, services, PC's and related traffic to and from those devices. Any exemption to these policies will be addressed on a case by case basis.

Governance of These Policies

The Natural Resource Computing and Networking Services (NRCNS) have devised these policies. These policies are subject to change. Any changes to this policy will be reviewed by NRCNS, the Warner College of Natural Resources Computing and Network Services Committee and the Warner College of Natural Resources Dean's Office preceding any modification of the policy.

Service Registration Process (exemption to standard policy)

The CNR IT Manager will review all inquires to register devices and/or services that are restricted by current security policy. The process will be performed on a case by case basis in an effort to satisfy individual business and academic requirements while still preserving the integrity of campus and college level IT security.