FSCOT Agenda

August 15th, 2006

FSCOT Meeting
August 15, 2006 1-3:30 p.m.
Location: Hale Library – Room 503 Deans Conference Room
Polycom IP address: 129.130.36.1 (for Salina call in)

Attachments:

1. Proposed revisions to section .050 of PPM 3430 "Security for Information, Computing and Network Services

Guests:

Harvard Townsend – Chief Information Tech Architect/Head of SIRT
Royce Gilbert – LAN Technologies Manager/Project head of Trend Micro Project

1. Draft Proposal of revisions to section .050 of PPM 3430 "Security for Information, Computing and Network Services (Attachment 1)

2. Policy/Procedures and Implementation of the new Trend Micro Antivirus/spyware software package that is replacing Symantec software this fall (and being implemented now).

3. AVP of IT position search – discussion

ATTACHMENT 1

Proposed Revision to Section .050 of PPM 3430 "Security for Information, Computing and Network Resources"
Date of policy draft: May 11, 2006
Date(s) revised: May 16, 2006, June 1, 2006, June 16, 2006, August 14, 2006
Submitted by: Harvard Townsend, harv@ksu.edu, on behalf of SIRT
Reference: http://www.k-state.edu/policies/ppm/3430.html

Proposed Revision (deletions denoted by strikethrough, additions appear in blue):

.050 Requirements for Information, Computing and Network Security

The following ~~procedures~~ system requirements represent the minimum standard ~~system requirements~~ that must be in place in order to establish and maintain security for University information, computing and network resources.

Initial Network ~~Hook-up~~ Connection:

Each system must be capable of passing a test for vulnerabilities to hacker attacks and relaying of unsolicited email prior to being attached to K-State's information, computing and network resources. System testing will be the responsibility of the Departmental/Unit or University Security Officer.

Password Specification:

~~Systems requiring passwords will specify that they must be changed twice annually, on the first of September and February. Passwords must conform to edits specified in the CNS Policy on User ID & Passwords. Systems that allow remote log-ins over the campus network should have passwords on all accounts. Checking passwords for conformance is the responsibility of the University Security Officer~~.

Password Policy: All passwords on any system, whether owned by K-State or by an individual, directly connected to Kansas State University network must adhere to the following standards when technically possible. This includes devices connected to the campus network with a direct wired connection, wireless, dial-in modem, access by Windows Remote Desktop, use of a Virtual Private Network (VPN), and the like. This policy applies to all passwords – eID, system, user, database, application, etc. Any system that does not comply may have its network access blocked without prior notification. The password standards are maintained by the Vice Provost for Academic Services and Technology (VPAST) or designee. Exceptions must be approved by the VPAST or designee.

Password Standards:

1. Passwords must have a minimum of 7 characters.
2. Passwords must contain characters from 3 of the 4 following categories:
   a. Uppercase letters
   b. Lowercase letters
   c. Numbers

d. Special Characters (for example: !,@,#,$,%,^,&,*, etc. But be aware if traveling outside the U.S. that some symbols, like the U.S. dollar sign, may not be available on international keyboards)

3. Passwords cannot be the same as the K-State eID and not easily guessed (for example: no variants of the K-State eID, dictionary words, family names, pet names, birthdates, etc.).
4. Passwords must be changed at least twice a year (eID password changes are during a designated time at the beginning of the fall and spring semesters).
5. Passwords must be changed significantly and cannot repeat more frequently than every two years.
6. Passwords that are written down or stored electronically must not be accessible to anyone other than the owner and/or issuing authority.
7. The same password used to access Kansas State University Systems (for example, your eID password) cannot be used for accounts or other forms of access to non-K-State systems or applications such as online shopping, banking, etc.
8. Passwords cannot be shared unless explicitly permitted by the issuing authority. eID passwords cannot be shared under any circumstances.
9. Anyone who believes their password has been compromised must immediately notify their departmental or college IT support, or the IT Help Desk to evaluate possible risks.
10. Default passwords in vendor-supplied hardware or software must be changed during initial installation or setup.
11. The eID password must never be transmitted over the network in clear text (i.e., it must always be encrypted in transit). It is also strongly recommended that other types of passwords be encrypted in transit.

Unattended Computers

To protect against unauthorized access to data on computers left unattended, the following precautions are required:

- Enable password protection on the screen saver for all university computers with the exception of special-purpose computers designed for public access, such as information or registration kiosks, public computers in the library, or computer labs where locking is undesirable due to the risk of a user monopolizing a shared computer. The length of time before the password-protected screen saver comes on should be set to 20 minutes or less. For lab situations, it is recommended that computes be set to automatically logout after at the most 30 minutes of idle time.
- Never leave your computer unattended and unprotected. Before leaving your computer, lock the display or log out in a manner that requires a password to gain access.

~~**Virus Protection Software**~~**:**
Protection from Malicious Software and Intrusions:

~~Each attached system will be required to boot-up with active virus protection. The software used may be either one provided by the University, or one of the user's own choosing. In either case, the virus protection software must be no more than 1 update behind the current version and the virus definition files should be no more than 1 month old (or updated to respond to a specific virus alert).~~ Malicious software, or “malware”, comes in many forms – viruses, worms, Trojan horses, denial of service attacks, botnets, spyware, adware, spam relays, etc. All pose a security risk, some of which are a very serious threat to the confidentiality, integrity, or availability of K-

State's information and technology resources. Appropriate precautions must be taken to protect K-State systems and information from compromise by malware. To that end, K-State may require the installation of essential security software on computers connected to the K-State campus network or accessing K-State information and technology resources. The following sections define specific requirements for antivirus, spyware/adware, personal firewalls, and e-mail. Assuring the validity of ~~virus~~ malware protection software ~~will be~~ is the responsibility of ~~the Departmental/Unit or University Security Officers~~ each user, the department/unit security representative, and the K-State Security Officer.

Virus Protection

- Any university-owned computer must use the university-supplied antivirus software configured in a managed mode.
- Student-owned computers in K-State residence halls must use the university-supplied antivirus software configured in a managed mode.
- Users of K-State's Virtual Private Network (VPN) or dial-up modem service must use the university-supplied antivirus software configured in a managed mode.
- All other computers accessing the K-State campus network or information technology resources must be running active, up-to-date virus protection software.
- Antivirus software must be activated when the computer boots up and remain active at all times during its operation.
- Real-time file scanning must be enabled where files are scanned for malicious anomalies before they are written to the hard drive.
- Virus definition files must be up-to-date with the most current version available from the vendor.
- The version of the virus protection software must be no more than one version behind the current version offered by the vendor or the version endorsed by K-State, and must be supported by the vendor.
- Checking for and installing updates to virus definition files and antivirus software must be automated and performed at least daily.
- Comprehensive virus scans of all local hard drives must be performed at least weekly.

Spyware/Adware Protection

- All computers connected to the campus network must run active spyware/adware protection software.
- Spyware/adware definition/detection rules must be up-to-date with the most current version available from the vendor.
- Scans of all local hard drives for spyware/adware must be performed at least weekly.

Personal Firewall Protection

- All computers using the university-supplied security software (which includes virus, spyware, intrusion, and firewall protection) must have the firewall enabled.
- Any other computer connected to the campus network must run a personal firewall. Microsoft Windows Firewall is an acceptable personal firewall.

E-mail Protection

- All campus e-mail servers must provide antivirus protection that detects and mitigates infected e-mail messages.
- Infected messages must be discarded or quarantined, not returned to the sender.

Security Patches

All systems connected to the campus network and the applications and databases running on those systems must have the latest security patches available from the respective vendors applied. Any system or application with known vulnerabilities for which a patch is not available must take appropriate measures to mitigate the risk, such as placing the system behind a firewall. Kansas State University may block access to the network for systems that have not been patched.

~~**Local Area Network (LAN) Operating Systems/ Electronic Mail Servers**~~**:**
College/Departmental Systems

~~Units or~~ Colleges, ~~D~~departments, or other K-State units may institute their own distributed computing system, as these provide valuable specialized services to ~~K-State~~ users. These servers, in order to protect the University resources to which they are connected, must be kept no more than ~~1 update~~ one version behind the current vendor-supported version of the operating system and application software and comply with all security requirements and standards set forth in this policy.

Campus units with qualified IT support staff may run their own security management environment with the university-supplied security software that provides virus, spyware, intrusion, and firewall protection. The unit security management system must be configured to provide reports to the central security management system to facilitate comprehensive campus-wide reporting. In the absence of qualified IT support staff, units must use the central security management services for malware protection.

Assurance of server protection is the responsibility of the Departmental~~/Unit~~ Security ~~Officer~~ Representative.

Enforcement

Enforcement of these policies and associated standards is the responsibility of the Vice Provost for Academic Services and Technology (VPAST) or designee. Any device directly connected to the campus network (i.e., with a direct wired or wireless connection, dial-in modem, access by Windows Remote Desktop, use of a Virtual Private Network (VPN), and the like) may be remotely or directly scanned and assessed by designated VPAST information technology or security staff at any time to determine compliance with security policies and standards, or detect anomalous activities, vulnerabilities, and security compromises. Firewalls must be configured to permit this remote scanning function. Scanning may only preformed to the extent necessary to detect and assess the risk. Any system that does not comply with security policies and standards, is susceptible to a known vulnerability, or is compromised may have its network access blocked immediately and without prior notification to protect the integrity of other systems and data.

K-State's Security Incident Response Team (SIRT) has defined procedures for restoring network access after the vulnerable or compromised system has been repaired

(see http://www.k-state.edu/infotech/security/SIRT/Procedures/compromise.html). SIRT will determine whether the repair will require the computer to be reformatted and the operating system and all software and data re-installed, depending on the nature of the compromise.

Key Personnel and Responsibilities:

Security Administrator: The University employee responsible for protecting information, computing and network resources. Responsibilities include assisting with University-wide policies, controls and procedures; monitoring adherence to policies; coordinating responses to security incidents; and providing education on the ethical use of information, computing and network resources.

K-State Security Officers: Technical personnel in central information technology units who have been assigned the additional responsibility of monitoring the state of information, computing and network security at the University level. Responsibilities include detection of problems, exchange of information about hazards and incidents with organizations outside the University, and communication of alerts and remedies to departmental/unit security representatives.

Departmental Security Representatives: The key technical personnel in colleges, departments and university support units. Their responsibilities include supporting and maintaining security for computing, networking or database resources for their respective units.

Deans and Department Heads: Responsibilities ~~will~~ include authorizing access to computer systems in their units, ensuring that System Users understand and agree to comply with University and unit security policies, and ensuring that the technical and procedural means are in place to assist in maintaining the security procedures outlined above.

System Users: Responsibilities include agreeing to and complying with all applicable University and unit security policies and procedures; taking reasonable precautions, including personal password protection, maintenance and file protection measures, to prevent unauthorized use of their accounts, programs or data; representing themselves truthfully in all forms of electronic communication; respecting the privacy of electronic communication; and respecting the physical hardware and network configuration of University-owned networks.