Kansas State University

College of Veterinary Medicine

Computing Policies and Procedures Handbook

Approved 18 November, 1999 by Dean's Administrative Council

Last Revision 26 April 2016

Table of Contents

- Introduction page 3

- KSUCVM Computing and Technical Services page 4

- Computing Security page 5

- CVM World Wide Web Policies and Procedures page 6

- CVM Network Policies and Procedures
  - . Introduction page 7
  - . User Accounts page 7
  - . Access to Resources page 11
  - . User Rights and Responsibilities page 12
  - . Abuse of Resources page 15
  - . Network Administrator’s Responsibilities page 17
  - . Enforcement page 18
  - . Reporting Problems page 19

Appendix A. - K-State University Information Technology Usage Policy page 20

Appendix B. – K-State University Electronic Mail Policy page 23

Appendix C. – K-State University Internet and World Wide Web Policy page 26

Introduction

This handbook was created to serve as a guideline for the use of the computing and network resources at the College of Veterinary Medicine at Kansas State University. The policies and procedures contained herein were developed by the college's Technology Advisory Committee (TAC) in cooperation with Computing and Technical Services (CaTS), and are approved by the Dean of Veterinary Medicine and the Dean's Administrative Council. The Technology Advisory Committee is made up of faculty members from each department within the college who serve as their departments' faculty contact person for computing and technology issues. The committee is responsible for initiating any policies or procedures related to computing technology within the college, and recommending them to the Dean and the Administrative Council for approval. ***If you have any questions or concerns about any of the policies or procedures set forth in this manual, please contact your departmental TAC representative.***

Computing and Technical Services (CaTS):

The CaTS web site is located at http://www.vet.k-state.edu/cats

The following support services are available through CaTS:

- Network connectivity/ Ordering new connections
- Computer and Peripheral recommendation and purchasing
- Computer and Peripheral troubleshooting and repair
- Hardware and software installation and support
- Classroom equipment support
- Programming and Internet/Intranet services

For all PC computing needs, please call the CaTS Hotline at 2-4725.

To make a service or support request:

1. **Call the Hotline at 2-4725** The hotline is available weekdays from 8:00am to 5:00pm. Requests can be made at other times, but cannot be acted upon until the next business day.

2. **Explain your request or problem.** If your problem or request cannot be solved over the phone, the request will be entered into the support database and assigned to the next available technician. You may request a particular technician if you desire. If you wish to be present during the technician's visit, you should make that known at this time.

3. **A technician will be in contact with you as soon as possible.**

Non-emergency response to requests after business hours will occur the morning of the next business day.

Emergency requests after hours:

Emergency response after hours is limited to CVM Network outages only. If you cannot connect to a CVM network server or the Hospital Management System (Vetstar/UVIS) after hours:

If possible, try to connect from another machine or office to see if the problem is isolated to your machine or connection. If not, contact one of the following people:

Steve Waldron – Network Administrator	313-0233
DeAnna Jacklovich – Network Administrator /IT Security	313-0235
Nancy Hawkins – Vetstar Administrator	313-0839
Eric Herrman – VetView Administrator	313-4031

COMPUTING SECURITY

SIRT

The **K-State Security Incident Response Team (SIRT)** is charged with providing "services and support dedicated to preventing and responding to information/network security incidents".

The primary responsibilities of SIRT are to respond to incidents in a coordinated manner; define an IT security architecture; implement preventive measures; recommend policy and procedure necessary for the campus to be in compliance with good security practice; and serve as a conduit of IT security information between central IT and the colleges, departments, and units represented by the SIRT.

The CVM SIRT representatives are:

Primary Contact : DeAnna Jacklovich	406 Trotter Hall 313-0235
Secondary Contact: Steve Waldron	406 Trotter Hall 313-0233

Security Policies

Information concerning SIRT's security policies and procedures can be found on the K-State SIRT website at https://www.ksu.edu/InfoTech/security/SIRT/. In addition, the CVM TAC committee recommends and the Dean's Advisory Council approves policies that act to enhance the security of the CVM network and its resources. These policies are updated regularly as needed upon approval from the Dean:

1. CaTS will configure all CVM computers to automatically install Windows updates from the CVM Windows Update Server. This insures that the latest critical patches and updates are available to CVM computers even if Microsoft's servers are temporarily overloaded or unavailable, and allows the updates to be installed at times that are convenient to our users.

2. CaTS will configure all CVM computers with a universal administrative username and strong password. In the event of a failure of the CVM Windows Update Server, the network administrator will be able to use this account in conjunction with Network Security software to push critical updates and patches to vulnerable computers as necessary.

3. CaTS will also configure the universal administrative account to have access via Remote Desktop, so that in the rare instance where procedures #1 and #2 fail, the network administrator can remotely log into a vulnerable machine and manually install critical updates and patches.

Campus and CVM network administrators will scan the CVM network on a regular basis, particularly following the release of any critical updates, to identify un-patched and vulnerable computers. Steps 1-3 will be followed as needed until the identified system has been successfully updated and its vulnerability closed.

CVM World Wide Web Policies

The World Wide Web is a technology that connects computer networks, like the one here at KSUCVM, with other networks throughout the world, and allows these networks to share information (the **Internet**). For the most part, networked users access this information using a graphical interface called a Web Browser, of which Internet Explorer and Firefox are examples. The Web uses a special type of network language that is platform independent called TCP/IP to send information between computers. In order to communicate with a Web source, you must have an IP address, which is a unique number that identifies you on the Internet. At KSUCVM, this number is allocated to you each time you log into our local network.

The Web, because it is mostly platform and software independent, has information delivery advantages that also make it an ideal way to share information on a local network. When this technique is used, it is called the **Intranet**. Information on an Intranet is still accessed via a Web Browser, and locally relevant information can be delivered seamlessly with information throughout the world. At KSUCVM we have both Internet and Intranet resources.

In order to minimize maintenance efforts and maximize standardization and university compliance, the college's web resources are managed under the following policies and standards defined by federal and state laws, KSU's CITAC, and the college's Technology Advisory Committee:

1. All KSUCVM web pages must meet the requirements set forth in the Standards for K-State World-Wide Web Pages published by the university's advisory committee, CITAC (Appendix C).
2. Web pages are reviewed before being published on the college's Web server.
3. The KSUCVM Web site is designed for the dissemination of professional information. Personal web pages can be created and published through eID accounts on the main campus.
4. Departments or service groups desiring a web page should contact CaTS. Departmental web pages are considered Internet resources whose proper use is described below:

KSUCVM Internet resources:

The KSUCVM Internet consists of resources that are freely accessible to anyone in the world. Therefore, these resources should be limited to informational data about the college, its departments, faculty, students and research activities. The Internet cannot include information that is bound by copyright laws or information that is proprietary in nature. If a department or service group wishes to make information about itself available to the general public, they should contact CaTS and have them create a web page for you. You will need to provide the information that you wish to have included in your web page: text, images, etc.

5. KSUCVM instructors are encouraged to use K-State Online to disseminate course information to students. The KSUCVM Intranet is also available for this purpose. Proper use of these resources is described below:

KSUCVM Intranet resources:

KSUCVM Intranet resources should be limited to information whose intended audience is the students, faculty, and/or staff of KSUCVM. Limiting access to these resources helps to resolve some educational copyright issues and help protect proprietary information. Please contact CaTS if you are an instructor or wish to have information published on the Intranet.

CVM Network Policies and Procedures

1. Introduction

The KSU College of Veterinary Medicine (CVM) network is a local area network (LAN) located in the College of Veterinary Medicine Complex. The CVM network is connected to the KSU campus network, which is in turn connected to worldwide Internet. The CVM network is made up of over 1000 PC workstations and servers. Services provided by the network include distributed file service, file archive, remote printing and remote job execution. The CVM network also provides connection to the services provided by Kansas State University's Computing and Telecommunications Services (CTS), including access to users' campus eID accounts, WWW, and Usenet News. A CVM network account is required to access services provided by the CVM Network.

The policies and procedures stated in this document are the result of efforts to educate the users of the network about the services that are available, what the rules are, and how to more effectively utilize network resources.

2. User Accounts

User accounts are used for access to the College of Veterinary Medicine network services, and for access to the university's network and the Internet. There are three types of accounts: faculty/staff, student, and student worker accounts. The accounts are created on the premise that once a user has an account, that account will be active as long as the user is employed by, or a student of the College of Veterinary Medicine. Each account is assigned to one user who is responsible for all actions of the account.

2.1. Types of Accounts

2.1.1. Faculty/Staff
CVM faculty/staff may be assigned an account for instructional use. Disk space for faculty/staff is provided by the College of Veterinary Medicine. File maintenance is the responsibility of the user.

2.1.2 Student
KSU veterinary students are authorized to have network accounts from the College of Veterinary Medicine. This type of account has limited access to the network resources. The student assigned to the account will be responsible for all network transactions associated with the assigned account.

2.1.3 Student Workers
Student workers are authorized to have network accounts from the College of Veterinary Medicine. This type of account has limited access to the network resources. The student assigned to the account will be responsible for all network transactions associated with the assigned account.

2.2. Account States

Accounts have four distinct states of existence. These states indicate the activity of the account from its creation to its deletion.

2.2.1. Creation
When an account is created, the following items are established:

- A username (also called userid). The network system administrator assigns the username based on a user's eID. The assigned username may not be subsequently changed unless the eID is changed first.

- a unique e-mail address (username@vet.k-state.edu)
- a home directory for storing the user's files
- a user information sheet The user information sheet is printed for each account upon its creation (with the exception of student accounts). The user information sheet contains the username, information to set password, e-mail address, location of the home directory, as well as other information useful to the novice user. The user information sheet may be picked up from the users' department human resource representative or their supervisor shortly after hiring. If this document is not provided they many contact their department human resource representative for further information.

2.2.2. Active

Once the user information sheet has been picked up, the account is considered active. Accounts will remain in the active state until one of the following criteria is met:

- the user has relinquished network privileges (i.e., upon graduation)
- the account or owner of the account has been found violating any portion of this policy
- the owner of the account is no longer employed by or enrolled at KSUCVM
- the user has not logged into the network for a period of 90 days

2.2.3. Disabled

Active accounts are changed to the disabled state prior to deletion. The disabled state is an intermediate step between an active account and a deleted account. In the disabled state, all network access and access to the accounts' electronic mail is denied. Electronic mail addressed to the account will continue to be delivered. Some files may be archived and deleted. An account may be reactivated from the disabled state. If no request is made to return the account to active status within 30 days, the account will be deleted.

2.2.4. Deleted

When an account is deleted, the username will be removed from the network and all files belonging to the user will be deleted. Electronic mail sent to the user will be rejected and returned to the sender.

2.2.5 Retired Faculty/Staff Accounts

CVM faculty and staff who retire are allowed to continue to use their KSU main-campus accounts for electronic mail. When a person retires from KSUCVM, their CVM network account will be disabled and their electronic mail will be forwarded to their KSU main campus e-mail account for a period of 30 days. After this time, the account will be deleted.

2.2.6 Emeritus Faculty Accounts

CVM faculty who retire and obtain emeritus status for KSUCVM are allowed to maintain their email account. Network accounts for Intranet Access will be allowed on a case by case basis and authorized by the TAC committee and the Dean. Emeritus network account status will follow the same guidelines as described in section 2.2.1 – 2.2.4.

2.3. Sharing Accounts

Any abusive activities initiated from your account will be traced back to the owner of the account, and the owner will be held responsible. The behavior of someone with whom you have shared your account becomes your responsibility. It is, therefore, policy that College of Veterinary Medicine network accounts are not to be shared. Each account has one user. If users wish to share information or otherwise collaborate in a group, then the users shall use appropriate file permissions combined with optional group membership to share data.

2.4. Password Selection

Perhaps the most vulnerable part of any computer system is the account password. Any computer system, no matter how secure it is from "hackers", can be fully exploited by intruders who can gain access via a poorly chosen password. It is important to select a password that is not easily guessed and to **not share the password with ANYONE**. Campus policy requires passwords to meet the following guidelines:

- Must be10 characters in length
- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Must contain 5 different characters
- Must not be based on a known word or name
- Must contain 3 of the following four categories:
  1. English uppercase characters (A through Z)
  2. English lowercase characters (a through z)
  3. Base 10 digits (0 through 9)
  4. Non-alphabetic characters (for example, !, $, #, %)

Complexity requirements are enforced when passwords are changed or created.

2.5. Changing Your Password

Passwords must be changed every 180 days. This may or may not coincide with main campus eID password changes depending on when you change your eID password.

You will receive an email message two weeks before it is time to change your CVM password. You will continue to receive the reminder message until you change your password or until your password expires. If your password expires you will be locked out of your email and network account and you will need to stop by 406 Trotter Hall to re-enable your account.

Passwords should be changed using the online CVM Password Management tool. Instructions are available at http://www.vet.k-state.edu/education/cats/resources/password/index.html

2.6. Determining Account Misuse

Often, users are the first persons to detect unauthorized use of their account. If this occurs, please notify the system administrators immediately. There are several ways to detect unauthorized use of your account:

- if strange files appear or disappear in your directories
- if you get mail from someone referring to a mail message you did not send

2.7. Account Requests

2.7.1. Requesting a new account

Users may request a new account by completing the New Account Request form online at http://www.vet.k-state.edu/asp/network-account/

> All account requests require verification of student or employee status before creation.

The application a for new account requires that the user sign an agreement stating that the user understands and will abide by all policies regarding the use of the Kansas State University College of Veterinary Medicine network.

2.7.2. Requesting additional group membership

There are times when a group of users need to work together on projects. If a group of users wishes to share e-mail or file data only among themselves, they can become members of a new group. Requests for new groups can be made with proper justification of the purpose of the group and identification of a user who will be responsible for who the group members will be, and the deletion of the group after the project is completed.

2.7.3. Requesting a new password

Sometimes users forget their password. If this happens, you can use one of the following methods to reset your password:

- You can use the Reset Password option from the CVM password self-service website: https://www.vet.k-state.edu/password. This can only be used if you have enrolled for SecurityQuestions/Answers, or enrolled an email account for Verification Code use.
- The user will need to show valid id at 406 Trotter Hall to have a password reset by a member of CaTS. If a user is not available on campus identification by other means may be possible, and will be determined by the Dean’s office.

3. Authorized Access to Network Resources

3.1. Physical Access to Equipment

Many College of Veterinary Medicine faculty and students have access to network resources. These resources may be printers, workstations, PCs, network wiring or connection equipment, etc. Anything that is connected to the network can be considered a resource. Some of these resources are necessarily kept physically secure. Others may be readily accessible to the public at all times.

3.2. Access to Networked PCs

General access to networked PCs for the College of Veterinary Medicine network users is currently limited to the CVM Library and a few computers in Mosier Hall.

3.3. Access via the Internet

Wide-area access to College of Veterinary Medicine network services is limited to access via the CVM World Wide Web server and FTP servers.

3.4. Adding Resources to the Network

The addition of network resources (as stated in 3.1 above) to the College of Veterinary Medicine network, should be coordinated with CaTS. This includes workstations, microcomputers, networked printers, or any other computing and networking hardware.

3.5. Departmental Network Resource

For access to departmental network resources, a supervisor or faculty/staff resource representative is required to send a request for employee access.

4. User Rights and Responsibilities

4.1. Use of Licensed Software

There is a large quantity of copyrighted and licensed software available for use on the College of Veterinary Medicine network. Typically, most of the applications on the network are for use throughout the college. However, some software may be licensed only to a particular group. Other software may have a "floating node" license that limits the number of concurrent users. Copyrighted and licensed software and documentation may not be duplicated unless it is explicitly stated that you may do so. If you have any doubts about what can be copied, please call the CaTS hotline at 2-4725.

4.1.1 Non-Work-Related Software

The installation and use of Instant Messaging and/or other non-work-related, processor or network intensive programs (graphical screensavers, internet file-sharing programs, etc.) is not recommended or supported by CaTS. These types of programs allow for the introduction of viruses, and affect the efficiency of computers and the productivity of workers. The damage caused by viruses, and the hardware upgrades necessary in order to reclaim resources used by the unnecessary programs are costly, both monetarily and in support personnel time. If these programs are loaded onto CVM computers and cause computer performance problems that require the involvement of CaTS, they should be removed at the request of CaTS deskside support personnel. If such a request is not acceptable to the employee, the employee's supervisor will be involved in the decision on how to optimize performance of the computer in question for work-related purposes.

4.1.2 Use of Customized Operating Systems

Technical support provided by the college (i.e. CaTS) will be limited to devices using an English-based operating system.

4.2. Use of Storage Resources

The file servers on the College of Veterinary Medicine network have a large, but finite, amount of disk space. If a user consumes large amounts of disk space, others will be affected. There are limits set on the shared data volumes so that this will not become a problem. If you require more space than the allocated amount, departments may purchase more space for their use.

4.2.1. Methods for reducing disk usage

The best way of reducing your disk usage is to delete any unused files. Good candidates for deletion are backup files (i.e. file.bak, file.old, file.tmp). If you have a large volume of picture files (i.e. file.bmp, file.jpg, file.gif), back them up to CD, DVD, or some type of external backup device.

4.2.2. Disallowed files

The following file types should not be transported, stored, printed, or otherwise exist on any of the College of Veterinary Medicine network servers:

- files not used for the purposes of education, research, or extension
- scanned, copyrighted material
- GIF, JPEG, MP3, MP4 or other image/audio files not used for academic purposes

4.3. Use of Printing Resources

Many printers are available to network users for print services. Only those printers operated by CaTS and designated as general use printers are subject to the usage guidelines herein. The following activities should be avoided:

- printing multiple copies of the same document; use copy machines instead

- loading or printing any media for which the printer is not designed to use; prohibited materials include resume paper, transparencies, envelopes, etc.
- any activity which could harm the printer or print server
- any activity which would deny the service of the printer to others

4.4. Use of Archiving Resources

Several methods exist for making permanent archives of data on the network including external hard drives, flash drives and CDs or DVDs.

4.5. Use of Remote Non-Veterinary Medicine Resources

The CVM network is directly connected to the Kansas State University network. There are services provided to CVM users by other divisions of Kansas State University. CVM network users are bound by the policies of the resource provider when using resources outside of the CVM network.

4.6. Use of Electronic Mail

Electronic mail (e-mail) is the primary form of communication between individuals on the network. Users are encouraged to read their e-mail regularly. Electronic mail provides an easy mechanism for exchanging information between users. Most file types can be sent via e-mail, although some types are blocked to avoid the spread of malicious software and viruses. Blocked file types include .exe, .bat, .com, .cab, among others, as well as any compressed archive (.zip) file that contains a file of the restricted file type. Large files (>10MB) should be sent via alternate means. One such method is the CVM Large File Upload and Email server at https://ftp.vet.k-state.edu/aht/ .

5. Abuse of Network Resources

This section serves to provide specific examples of the types of abuses that are covered by Federal, State and local laws, as well as university policy. This list is by no means complete and is subject to change without notice as new ways of abusing resources are discovered and new legislation is passed. Penalties for abuse of network resources include, but are not limited to, temporary restriction of network privileges, permanent restriction of network privileges, and criminal prosecution.

5.1. Theft and Vandalism

Theft and vandalism of network resources will be handled by the appropriate authorities (Kansas State University Police and/or Riley County Police). The College of Veterinary Medicine will pursue and support criminal prosecution of individuals suspected of theft and/or vandalism.

5.2. Unauthorized Use of Network Services

Anyone, for whom an active account does not exist, found using any College of Veterinary Medicine network services, will be referred to the appropriate authorities. For CVM staff, students, and faculty, the individual's department head and dean will be notified. Incidence involving individuals not directly associated with the college will be handled by the KSU Police Department. If direct expenses are incurred by the College of Veterinary Medicine during unauthorized used (i.e., paper, printer supplies, etc.), the College of Veterinary Medicine reserves the right to pursue full reimbursement of those costs from the individual. Use of restricted network services without authorization is considered an abuse of privilege and may result in restriction or denial of network access. Current restricted-use network resources include printers reserved for use by an individual, department or research group, and servers, which have restricted login access.

5.2.1. Breaking into accounts

Any attempt to gain access or to use an account other than by the owner will be considered a violation of network policy. Such attempts include, but are not limited to, gaining access to a user's account while the user is away from a terminal or a workstation, or efforts to determine another user's password by closely watching a login. If you find another user logged on but not near a machine, you should try and locate the user, and, if not found, log the user out immediately.

5.2.2. Cracking passwords

Any attempt to crack or otherwise obtain personal account passwords is prohibited. Storing or transferring encrypted or unencrypted personal account password information is prohibited. Writing, transferring, compiling or running programs designed to guess passwords or otherwise gain unauthorized access to user or system accounts or a password is prohibited. This includes programs or techniques designed to trick users into divulging their password.

5.2.3. Access to information

Unauthorized access to information contained in a user's home directory is prohibited, even if the files are readable and/or writeable. When in doubt, **don't read, copy, or change** other users' files.

5.2.4. Modifying files

Modifying files anywhere on the system without consent of the file's owner is prohibited. This includes writing or modifying files that have file permissions set to allow modification or writing. This also includes creating new files, renaming, or deleting existing files in directories that may have directory permissions set to allow creation or modification of files. When in doubt, **don't write**.

5.2.5. Receipt and distribution of copyrighted material

Use of network services for the receipt, distribution, or use of copyrighted software or material without the express consent of the copyright owner is prohibited.

5.3. Personal and Pecuniary Use of Resources

The use of CVM computing and network resources for personal or pecuniary purposes is prohibited.

5.4. Licensing and Copyright Infringement

Most software packages and applications are licensed and/or copyrighted. Most licenses and copyright agreements specifically prohibit copying or unauthorized use of the software or data. When in doubt, **don't copy**.

5.5. File Storage

Many gigabytes of disk storage are available to users on the CVM network, although despite that fact, it will eventually all be used. User accounts are set up such that each user has a home directory for storing files. There is also disk space available for network storage of departmental shared data. Since there is a limited amount of disk space free, all users are encouraged to control their disk usage by archiving and deleting old or unused files. Users should also try to avoid duplicating files that are available elsewhere on the network. Disk quotas must be enforced on all home directories.

5.6. Electronic Mail and Instant Messaging

Electronic mail (e-mail) and Instant Messaging (IM) are communications tools used by network users. Due to the design goals of the Internet, these forms of communication are not very secure and should not be used to transfer sensitive or confidential information. In addition, many Instant Messaging programs contain security flaws that can be exploited by hackers and malicious code who use these exploits to gain access to a machine.

The College of Veterinary Medicine follows the Information Technology Usage Policy (Appendix A) and the Electronic Mail policies outlined for Kansas State University (Appendix B) with the following amendments:

5.6.1 Appropriate Use of “massmail”

The use of “massmail” and other distribution lists within the College of Veterinary Medicine should be limited to messages that are related to college and/or university issues. Questions concerning the appropriateness of distributed messages will be resolved by the Dean of the College of Veterinary Medicine.

5.6.2 Use of “Instant Messaging” Programs

The use of Instant Messaging programs within the College of Veterinary Medicine is limited to the program(s) approved by the CVM Technology Advisory Committee. In addition, the approved IM program(s) should not be used to read or send e-mail, or to transfer files of any type between users. Users desiring to communicate via IM should be using machines that have the approved antivirus software installed and active, along with the current antivirus signatures.

5.7. Violation of Remote Site Policy

Users of remote sites or remote site services are bound by the rules and policies of the remote site. If you do not know the remote site's rules and policies, adhere to those outlined in this document.

5.8. Other Forms of Abuse

5.8.1. Malware and SPAM

Anyone knowingly attempting to proliferate, write, or distribute malicious software or SPAM in any form will be remanded for criminal prosecution.

5.8.2. FTP

Using FTP to transfer files to or from remote sites that violate the policies of the remote site is prohibited. In particular, transferring files which are extremely large, contain material offensive to either site, contain information to be used for pecuniary interests of any party, or contain monetary or sexual solicitations is prohibited.

6. Network Administrators' Responsibilities

Network Administrators are held to a higher standard than the average user because they have the capability and responsibility to maintain system integrity. In any networked environment, such users are given super-user access that allows them to read, write, or execute any file on the system. Thus, systems administrators must be entrusted with the security and privacy of all data on the network.

6.1. Privacy Considerations

Network Administrators have access to users' private information. Systems administrators are required to protect the confidentiality and integrity of this information.

6.2. Liability

Network Administrators are not liable for any loss of data or loss of service on the CVM network.

6.3. Investigation of Violations

Network Administrators are charged with investigating violations of CVM network policy. During such investigations, the Network Administrator may have complete access to all data on the CVM network as needed for the investigation.

7. Enforcement

7.1. Temporary Access Restriction

An individual account's access to the College of Veterinary Medicine network may be temporarily restricted due many reasons, including:

- maintenance or servicing of network resources
- investigation of College of Veterinary Medicine network policy violation

Temporary access restrictions are intended to be short lived and usually require the account's owner to contact the Network Administrator for reactivation. Note that investigations of network policy violations may require any number of potentially affected accounts to be temporarily restricted. The owner of the account may not be the object of the investigation if, for example, it may be suspected that a third party has cracked the user's password.

7.2. Permanent Access Restriction

The Dean of Veterinary Medicine or the affected users' department head must approve permanent access restrictions. All accounts assigned to a user may be restricted and future network privileges denied.

8. Reporting Problems

8.1. Physical Security

Physical security is the most important part of system security. Obviously electronic security means nothing if the whole machine is stolen. Users should be aware of what networked machines are in their vicinity and keep an eye out for any suspicious activity. Doors to laboratories should be closed and locked if there are no more users in the lab.

8.1.1. Theft and vandalism

Theft and vandalism should be reported to the Kansas State University Campus Police as well as College of Veterinary Medicine Computing Group.

8.2. Electronic Security

Electronic security is also the responsibility of all users. Users should periodically examine their files for unusual activities. Contrary to popular belief, Network Administrators are not omniscient nor are omnipresent, so suspicious activities often reported first by wary users.

8.2.1. Notification of local system administrators

Violation of College of Veterinary Medicine network policy should be brought to the attention of the Network Administrator as soon as possible. Depending on the nature of the violation, electronic mail or telephone call is the best method of alerting the Administrator.

8.3. Recovery of Deleted Files

User home directories are incrementally backed up onto tape every working day, and complete backups are performed weekly. To request restoration of deleted files, Contact the CaTS Hotline with the following information:

- exactly which file(s) need to be restored; include the directory in which the files were located (i.e. Z:\Files, or O:\File1\Important\document\work\due\today)
- the date and time the file(s) were created
- the date and time the file(s) were last modified
- the date and time the file(s) were deleted

If located on tape, the files will be restored and placed back in their original location. Note: files that are restricted under the College of Veterinary Medicine network policy will not be restored.

Any corrections, additions, or suggested changes to this document can be e-mailed to CaTS at cats@vet.k-state.edu or to your TAC representative.

Information Technology Usage Policy

http://www.k-state.edu/policies/ppm/3420.html
Revised September 2, 2010

.010 Preface

"Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, the right to privacy, and the right to determine the form, manner, and terms of publication and distribution. Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community." The EDUCOM Code.

.020 Background and Purpose

This document constitutes a university-wide policy for the appropriate use of all KSU computing and network resources. It is intended to provide effective protection of individual users, equitable access, and proper management of those resources. These guidelines are intended to supplement, not replace, all existing laws, regulations, agreements, and contracts which currently apply to those resources.

Access to KSU networks and computer systems is granted subject to University policies and local, state, and federal laws. Appropriate use should always be legal and ethical, reflect academic honesty and community standards, and show restraint in the consumption of shared resources. It should demonstrate respect for intellectual property; ownership of data; system security mechanisms; and individuals' rights to privacy, freedom of speech, and freedom from intimidation, harassment, and unwarranted annoyance.

The University is not responsible for unacceptable or unethical use of the information technology environment including computer and computer networks or electronic communication system.

.030 Appropriate Use

Appropriate use of information technology resources includes instruction; independent study; authorized research; independent research; and official work of the offices, units, recognized student and campus organizations, and agencies of the University.

Authorized use of KSU-owned or operated computing and network resources is consistent with the education, research, and service mission of the University, and consistent with this policy.

Authorized users are: (1) faculty, staff, and students of the University; (2) anyone connecting from a public information service; (3) others whose access furthers the mission of the University and whose usage does not interfere with other users' access to resources. In addition, a user must be specifically authorized to use a particular computing or network resource by the campus unit responsible for operating the resource.

Acceptable conduct in and use of this environment must conform with: existing University policies, guidelines, and codes of conduct; KSU's Web, E-Mail, Intellectual Property and Information Resource Policies; Kansas Board of Regents policies and guidelines; the usage guidelines of other networks linked to KSU's networks or computer systems, and existing local, state and federal laws.

Therefore, any misuse or violation of KSU's information-technology environment will be judged in accordance with those published policies and rules of conduct, including, but not limited to, the KSU Student Handbook, the Student Governing Association Conduct Code, the University's Policy Prohibiting Racial and/or Ethnic Harassment, the University's Policy Prohibiting Sexual Harassment, the Faculty Handbook and the University Policy and Procedures Manual.

It is your responsibility to be aware of the potential for and possible effects of manipulating information, especially in electronic form, to understand the changeable nature of electronically stored information, and to continuously verify the integrity and completeness of information that you compile or use. You are responsible for the security and integrity of University information stored on your individual computing desktop system.

.040 Confidentiality and Privacy

Authorized access to data or information entails both privilege and responsibility, not only for the user, but also for the system administrator. In general, the university will treat information stored on computers as confidential. However, there is no expectation of privacy or confidentiality for documents and messages stored on University-owned equipment. Additionally, e-mail and data stored on KSU's network of computers may be accessed by the university for the following purposes:

a. troubleshooting hardware and software problems,
b. preventing unauthorized access and system misuse,
c. retrieving business related information,*
d. investigating reports of violation of this policy or local, state or federal law,*
e. complying with legal requests for information,*
f. rerouting or disposing of undeliverable mail.

* The system administrator will need specific approval from the Vice Provost for Academic Services and Technology or the appropriate designee to access these items. The extent of the access will be limited to what is essentially necessary to acquire the information.

To the greatest extent possible in a public setting individuals' privacy should be preserved. However, privacy or confidentiality of documents and messages stored on University-owned equipment cannot be guaranteed. Users of electronic mail systems should be aware that, in addition to being subject to authorized access, electronic mail in its present form cannot be secured and is, therefore, vulnerable to unauthorized access and modification by third parties.

.050 Examples of Prohibited Use

Use of KSU network and computer systems is conditioned upon compliance with this and other university policies and all applicable laws. Though not exhaustive, the following list is provided to emphasize that these activities are NOT allowed on KSU networks or computer systems:

a. using facilities, accounts, access codes, privileges or information for which you are not authorized;
b. sharing your eID password with others;
c. viewing, copying, altering, or destroying anyone's files without explicit permission from that individual;
d. representing yourself electronically as another user;
e. unlawfully harassing others;
f. creating and/or forwarding chain letters;
g. posting or mailing obscene materials;

h. game playing that interferes with academic or administrative use by others;
i. making, distributing, or using unauthorized copies of licensed software;
j. unauthorized copying, reproducing, or redistributing others' text, photos, sound, video graphics, designs or other information formats;
k. obstructing others' work by consuming large amounts of system resources, such as disk space, CPU time and etc.;
l. unauthorized testing of systems and/or resources, such as using program loops, introducing destructive software e.g., "virus" software or attempting system crashes;
m. running or otherwise configuring software or hardware to intentionally allow access by unauthorized users;
n. attempting to circumvent or subvert any system's security measures;
o. advertising for commercial gain;
p. distributing unsolicited advertising;
q. disrupting services, damaging files or intentionally damaging or destroying equipment, software or data belonging to KSU or other users;
r. using computing resources for unauthorized monitoring of electronic communications;
s. destroying public records in violation of KSU's Retention of Records Policy (PPM Chapter 3090);
t. violating any KSU or Kansas Board of Regents policy or any local, state or federal law.

In cases of doubt, users bear the burden of responsibility to inquire concerning the permissibility of external network uses, prior to execution. Such questions should be directed to the Vice Provost for Academic Services and Technology.

.060 Reporting Violations

All users and units should report any discovered unauthorized access attempts or other improper usage of KSU computers, networks, or other information processing equipment. If you observe, or have reported to you, a security or abuse problem, with any University computer or network facilities, including violations of this policy, you should notify the Vice Provost for Academic Services and Technology, the Director of Computing & Network Services or other appropriate administrator.

.070 Sanctions

Persons in violation of this policy are subject to the full range of sanctions, including the loss of computer or network access privileges without notification , disciplinary action, dismissal from the University, and legal action. Some violations may constitute criminal offenses, as outlined in Kansas statutes and other local, state, and federal laws; the University will carry out its responsibility to report such violations to the appropriate authorities.

Unit heads have the authority to deny access, for unauthorized use, to KSU's computers and network systems under their control.

.080 Questions

Questions regarding this policy should be sent to the Chief Information Officer at its@k-state.edu .

Appendix B – K-State University Electronic Mail Policy

http://www.k-state.edu/policies/ppm/3455.html
Revised September 2, 2010

.010 Introduction

This Policy clarifies the applicability of law and certain other University policies to electronic mail. Users are reminded that all usage of KSU's information technology resources including electronic mail is subject to all University policies including the Information Technology Usage Policy found at http://www.ksu.edu/policies/ppm/3420.html.

.020 Policy

The University encourages the use of electronic mail and respects the privacy of users. Nonetheless, electronic mail and data stored on the University's network of computers may be accessed by the University for the following purposes:

For items a-g, the extent of the access will be limited to what is reasonably necessary to acquire the information and/or resolve the issue.

a. troubleshooting hardware and software problems,

b. preventing unauthorized access and system misuse,

c. retrieving University business related information, *

d. investigating reports of alleged violation of University policy or local, state or federal law,*

e. complying with legal requests (e.g.; court orders) for information, *

f. rerouting or disposing of undeliverable mail,

g. addressing safety or security issues.

** The system administrator will need written approval, including e-mail, indicating the extent of access that has been authorized from the Vice Provost for Academic Services and Technology or the Vice Provost's designee, to access specific mail and data for these purposes.*

To the greatest extent possible in a public setting individuals' privacy should be preserved. However, there is no expectation of privacy or confidentiality for documents and messages stored on University-owned equipment.

Users of electronic mail systems should be aware that, in addition to being subject to authorized access, electronic mail in its present form cannot be secured and is, therefore, vulnerable to unauthorized access and modification by third parties. Receivers of electronic mail documents should check with the purported sender if there is any doubt about the identity of the sender or the authenticity of the contents, as they would with print documents. Users of electronic mail services should be aware that even though the sender and recipient have discarded their copies of an electronic mail record, there may be back-up copies of such electronic mail that can be retrieved.

University electronic mail services may, subject to the foregoing, be used for incidental personal purposes provided such use does not interfere with University operation of information technologies including electronic mail services, burden the University with incremental costs, or interfere with the user's employment or other obligations to the University.

Registered student and campus organizations such as the College Republican Club or the Young Democrats may use their membership listservs to notify members of meetings, speeches, or rallies. Faculty members may use electronic systems for course-related discussions of political topics. Individuals may use e-mail to exchange ideas and opinions, including those dealing with political issues. The latter is generally considered an incidental use of the e-mail system. However, University information technology resources, including e-mail, may not be used to support partisan political candidates or party fundraising. This statement is consistent with Kansas law and Board of Regents policy on political activity. (See Kansas law and Board of Regents policy printed at the end of this policy.)

Electronic mail may constitute a public record like other documents subject to disclosure under the Kansas Open Records Act or other laws, or as a result of litigation. However, prior to such disclosure, the University evaluates all requests for information submitted by the public for compliance with the provisions of the Act or other applicable law. In addition, electronic mail may constitute University records subject to the University's Retention of Records Policy (PPM, Chapter 3090). As such, they may need to be retained for longer than an e-mail system is capable of retaining them. It is the responsibility of the sender/recipient to determine if a particular e-mail message constitutes a university record.

If an e-mail message is a university record (as defined in PPM, Chapter 3090) it is subject to the same retention period as the paper equivalent. E-mail messages which require long-term retention should be either retained electronically on retrievable media or printed, including all header and transmission information, and filed with their electronic or paper equivalents by the sender/recipient. K-Staters should not consider back-up media on the central system as permanent archival storage (e-mail back up media are only available for 30 days).

Incidental personal electronic mail which is not subject to the Retention of Records Policy may be destroyed at the user's discretion.

Faculty, unclassified professionals, and classified employees may not suppress publication of (e.g., unlist) their University Computing ID in the on-line white pages, K-State Phone Book or other official publication of Kansas State University. Exceptions for special circumstances must be approved by the Vice Provost for Academic Services and Technology (VPAST) or official designee.

E-mail is considered a formal communication by the University with faculty, staff and students. Faculty, staff and students are expected to check their e-mail on a frequent and consistent basis in order to stay current with University and/or faculty-student related communications. For more information regarding official correspondence see the policy on Official Electronic Correspondence with Faculty, Staff and Students at http://www.ksu.edu/policies/ppm/3460.html.

Violations of University policies governing the use of University electronic mail services may result in restriction of access to University information technology resources in addition to any disciplinary action that may be applicable under other University policies, guidelines or implementing procedures, up to and including dismissal.

In January of each year the Vice Provost for Academic Services and Technology will report to the Faculty Senate regarding cases dealt with that year. For privacy purposes all names will be omitted.

.030 Related Kansas Law and Board Of Regents Policy

Kansas Statutes Annotated (K.S.A.) 25-4169a. Use of public funds, vehicles, machinery, equipment and supplies and time of certain officers and employees to influence nomination or election of candidate prohibited; exceptions; misdemeanor.

(a) No officer or employee of the State of Kansas, any county, any unified school district having 35,000 or more pupils regularly enrolled, any city of the first class or the board of public utilities of the city of Kansas City, Kansas, shall use or authorize the use of public funds or public vehicles, machinery, equipment or supplies of any such governmental agency or the time of any officer or employee of any such governmental agency, for which the officer or employee is compensated by such governmental agency, to expressly advocate the nomination, election or defeat of a clearly identified candidate to state office or local office. The provisions of this section prohibiting the use of time of any officer or employee for such purposes shall not apply to an incumbent officer campaigning for nomination or reelection to a succeeding term to such office or to members of the personal staff of any elected officer.

(b) Any person violating the provisions of this section shall be guilty of a class C misdemeanor.

Kansas Board of Regents Policy and Procedures Manual (15F, section d): In the interest of the fullest participation in public affairs, personnel are free to express opinions speaking or writing as an individual in signed advertisements, pamphlets and related material in support of or opposition to parties and causes. There will be the commensurate responsibility of making plain that each person so doing is acting for himself and not in behalf of an institution supported by tax funds drawn from citizens of varying political and economic views.

.040 Questions

Questions regarding this policy should be sent to the Chief Information Officer at its@k-state.edu.

Appendix C – K-State University Internet and World Wide Web Page Policy

.010 Introduction

Kansas State University (KSU) information resource management policies govern all access to KSU computers and networks. These policies are established and maintained under the immediate authority and direction of the Vice Provost for Academic Services and Technology.

.020 Access

Access to the Internet and the World Wide Web from KSU computers and networks is restricted to specially authorized registered users for academic, research, learning and administrative purposes. Public access to Kansas State University (KSU) computers and networks may be available from the Internet/World Wide Web or from within specially designated public facilities, such as the K-State Union or KSU Libraries.

.030 Official KSU Web Page

Any web page or other type of file on any computer which presents itself in any way as an Official KSU Web Page or Official KSU File must comply with KSU information resource management policies and procedures. Specific responsibilities for the creation and maintenance of the contents of Official KSU Web Pages and Official KSU Files are defined in KSU information resource management policy and procedures. These responsibilities require the use of reasonable and appropriate means of protecting KSU private information, proprietary information, and intellectual property.

.040 Unofficial Web Page

Any registered user may create an unofficial web page or unofficial file on a computer which is owned and operated by KSU or one of its affiliated units as long as it complies with KSU information resource management policies and procedures. All such page contents must be for purposes as defined by the instruction, research or service missions of the university. Individuals, units, or groups creating unofficial web pages and files are responsible for and may be held accountable for the contents. KSU assumes no responsibility for the content of any unofficial web page or file. KSU reserves the right to restrict the quantity and availability of KSU computing and network resources for the purpose of creating, maintaining, and viewing unofficial web pages and files.

.050 Internet Domain

KSU departments and student organizations registered with the Office of Student Activities and Services may register an Internet domain that represents an identifiable entity within that department or organization, such as an institute or research lab, or the student organization itself. Registration of all KSU Internet domains will be managed by a designee of the Vice Provost for Academic Services and Technology. Registration of personal domains, such as johnsmith.org, by individual faculty, staff, or students is not supported. Any domain representing a K-State entity is owned by the University unless specified otherwise in a contract or agreement, with the exception of domains for KSU affiliates such as the Alumni Association, KSU foundation, and Department of Intercollegiate Athletics.

.060 Removal

KSU reserves the right to remove, without notice, any web page or file (Official or unofficial) from any computer which is owned and operated by KSU or its affiliated units which does not comply with KSU information resource policies and procedures.

.070 Use of University Name

Use of Kansas State University's names (i.e. Kansas State University, K-State, KSU), trademarks, official logos, or other intellectual property and creative works is governed by KSU intellectual property and creative works policies.

Unauthorized presentation of any web page or file as an Official KSU Web Page or Official KSU File or any unauthorized or illegal use of KSU computers and networks is prohibited.

.080 Questions

Questions regarding this policy should be sent to the Director of Academic Services at academicservices@k-state.edu.

Issued 5/28/2002