MCUB-IMD 16 February 2012

MEMORANDUM FOR Information Systems and Local Area Network Subscribers

SUBJECT: Acceptable Use Policy, User Agreement, Information Systems Security Statement, User Responsibilities, and User ID Receipt (Automated Information System and Network Access)

Introduction. Team Winn members and all others using AMEDD Automated Information Systems (AIS) have a responsibility to assess the sensitivity of Army data and to ensure its security. Ultimately, **Information Assurance** (what we used to call computer security) **is each individual's responsibility**. The user must be alert to possible breaches in security and adhere to DoD security regulations. The security practices below are not all-inclusive, but are intended to remind the user and heighten individual awareness toward securing Army Automated Information Systems (AIS). Remember that the computers, software, network, e-mail, data, etc. all belong to the Army. These guidelines are found, in greater detail, within AR 25-1 (Army Knowledge Management and Information Technology), AR 25-2 (Information Assurance), AR 380-5 (Department of the Army Information Security Program), AR 380-67 (Personnel Security Program) and DoD 5500.7-R (Joint Ethics Regulation)

1. UNDERSTANDING. By signing this document (physically or electronically), you acknowledge and consent that when you access Department of Defense (DoD) information systems, locally or remotely:

-You are accessing a U.S. Government (USG) information system (IS) (as defined in Committee on National Security Systems Instruction (CNSSI) 4009) that is provided for U.S. Government-authorized use only.

-You consent to the following conditions:

- The government routinely monitors communications occurring on this information system, and any device attached to this information system, for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network defense, quality control, employee misconduct investigations, law enforcement investigations, and counterintelligence investigations.
- At any time, the government may inspect and/or seize data stored on this information system and any device attached to this information system.
- Communications occurring on or data stored on this information system, or any device attached to this information system, are not private. They are subject to routine monitoring and search.
- Any communications occurring on or data stored on this information system, or any device attached to this information system, may be disclosed or used for any U.S. Government-authorized purpose.
- Security protections may be utilized on this information system to protect certain interests that are important to the government. For example, passwords, access cards, encryption or biometric access controls provide security for the benefit of the government. These protections are not provided for your benefit or privacy and maybe modified or eliminated at the government's discretion.
- You verify you understand that you have the primary responsibility to safeguard the information contained in the Winn Army Community Hospital Fort Stewart-Hunter Army Airfield Army Medical Department Network aka "the network," and, in turn the United States' Non-secure Internet Protocol Router Network (NIPRNET) from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use.

2. ACCESS. Access to this network is for official use and authorized purposes and as set forth in DOD 5500.7-R (Joint Ethics Regulation), AR 25-2 (Information Assurance), Army network policy and accreditation, or as further limited by Federal, Department of Defense, Department of the Army, US Army Medical Command, Regional Medical Command, Medical Department Activity, or other associated unit policy. Your individual logon ID is to provide YOU with access. Not your friend or spouse or visiting cousin, or the guy who can't remember his password. Don't share your individual logon ID or password or the use of your CAC and PIN. Inappropriate activity under <u>your</u> logon is <u>your</u> responsibility. One network user, one logon. Remember that network access is a separate process from CHCS, AHLTA, ESSENTRIS, DMLSS or MEDPROS (etc.) access.

3. REVOCABILITY. Access to Army resources is a revocable privilege and is subject to content monitoring and security testing. Continued access to network resources requires annual Information Assurance training through the Information Assurance Training Center, https://ia.signal.army.mil/.

4. UNCLASSIFIED INFORMATION PROCESSING. Our LAN, and by extension the NIPRNET, is the primary unclassified information system for the Fort Stewart Medical, Dental and Veterinary Activities' facilities. It also provides service for other AMEDD-related personnel and functions as required and approved (e.g. SOF at Hunter AAF, Battalion Aid Stations). The NIPRNET, and hence our LAN, are UNCLASSIFIED systems. The network provides unclassified communication to external DOD and other US Government organizations. Primarily this is done via electronic mail and Internet networking protocols such as standard Web access (http), Secure Sockets Layer (https), File Transfer Protocol (FTP), telnet, secure shell, Virtual Private Networks (VPN) and others as required and approved.

a. The NIPRNET, and hence our network, is approved to process UNCLASSIFIED, SENSITIVE information in accordance with AR 25-2, Office of the Surgeon General, MEDCOM, and local automated information system security management policies. A DAA has accredited this network for processing this level of information.

b. Our network, NIPRNET, and the Internet, for the purpose of this document, are synonymous. E-mail and attachments are vulnerable to interception as they traverse the NIPRNET and Internet. Our systems are subject to any number of threats to inbound/outbound data, to include external and internal threats and malware.

5. Common Access Card, Public Key Infrastructure and Army Knowledge Online. Our Military and Civilian (Government, contract, and DOD Affiliates such as volunteers and students) workforce will have a Common Access Card (the military and DOD Civilian ID card), also known as the CAC. The CAC is an important part of the Information Assurance and Information Security of our nation, and also will provide for increased security of patient data, privacy data, and other Unclassified, Sensitive information.

a. PKI. Public Key Infrastructure provides a secure computing environment utilizing encryption algorithms (Public/Private-Keys). The CAC, via PKI, provides a secure computing environment utilizing encryption algorithms (Public/Private Key). The CAC will be used to log on to the network, encrypt sensitive e-mail, and digitally "sign" e-mail when necessary. In order for the CAC to work properly as currently implemented, one will need an Army Knowledge Online (AKO) account.

b. Token/Smart Card (or CAC). The Cryptographic Common Access Card Logon (CCL) is now the primary access control mechanism for all Army users (with very few exceptions). This is a two phase authentication process. First, CAC is inserted in to a smart-card reader, and then a unique user PIN number provides the validation process via "middleware" software. If you don't remember your PIN, it will have to be reset. You can get your PIN reset at the IMD main office (Room 1G03 in the main hospital) during normal duty hours (pending equipment availability). Alternately, you can get your PIN reset at the ID card issuance facility on main post or at Hunter Army Airfield, or at the main post library.

c. Digital Certificates (Private/Public Key). CAC is used as a means to sending digitally signed e-mail and encrypted e-mail.

d. Private Key (digital signature), as a general rule, should be used whenever e-mail is considered "Official Business" and contains sensitive information (operational requirements) or clickable web links (embedded URLs). The digital signature provides assurances that the integrity of the message has remained intact in transit, and provides for the non-repudiation of the message that the sender cannot later deny having originated the e-mail.

e. Public Key is used to encrypt information and verify the origin of the sender of an email. Encrypted mail should be the exception, and not the rule. It should only be used to send sensitive information, information protected by the Privacy Act of 1974, and Information protected under the Health Insurance Portability and Accountability Act (HIPAA).

f. Secure Socket Layer (SSL) technology should be used to secure a web based transaction. DoD/Army Private (Intranet) web servers should be protected by using this technology IAW DoD/Army PKI implementation guidance.

g. Your AKO address is supposed to be your return e-mail address. For that to happen, though, you'll need to log in to AKO and forward your AKO e-mail to your AMEDD e-mail account. That way, anything sent to your AKO can be read from your MEDCOM e-mail account here.

h. Normally, your AKO e-mail address will be your main e-mail address. Your official e-mail (whether it be an AMEDD account here or some other MS Exchange account elsewhere) will pass through your AKO e-mail

account. Be sure you have an AKO account, and that the AKO e-mail address you provide IMD is accurate. If you provide IMD with an inaccurate AKO e-mail address (or if your AKO is in use elsewhere, such as in a Post NEC e-mail account), your e-mail can disappear into oblivion. So don't just make one up -- or guess what it is -- verify your AKO e-mail address.

6. MINIMUM SECURITY RULES AND REQUIREMENTS. You are our first line of defense against misuse or penetration of our network. Personnel are not permitted access to the Network or attached Army Information Systems unless in complete compliance with Army and MEDCOM personnel security requirements for operating in the Unclassified, Sensitive System-High environment. As a network user, the following security rules and requirements apply:

a. Each subscriber must have completed the initial user security awareness training module (included in the HEART and HIPAA training). In accordance with AR 25-2, MEDCOM and SRMC instructions, Initial and Annual Refresher Information Assurance training is to be obtained through APEQS and the Information Assurance Training Center, Provide proof of completion to PTMS. Each subscriber will participate in all DoD/Army sponsored Security Awareness Training and Certification programs (inclusive of threat identification, physical security, acceptable use policies, malicious content and logic identification, and non-standard threats such as social engineering). Each subscriber must understand that the initial training will expire in one year and that you will be required to take an annual refresher training (IAW AR 25-2) and your account will be disabled until you have met this requirement.

b. Each individual, when required, will generate, store, and protect individual logon credentials (passwords, verify codes, or pass-phrases). In accordance with AR 25-2 Best Business Practice 04-IA-O-0001, all user-level, user-generated passwords will be 14-characters (or greater), case-sensitive and be changed regularly. They should be made up of at least 2 each of uppercase and lowercase letters, numbers, and special characters. You will not use your user ID, common names, birthdays, phone numbers, military acronyms, call signs or dictionary words as passwords or pass-phrases. Again, your password is for YOUR use, no one else's. In accordance with changes to AR 25-2, Chapter 4, Section IV, Para 4-12, along with the BBP, passwords should be changed at least every 60 days. Some systems (e.g. AHLTA, Essentris and CHCS-I have other limitations which will be followed for those systems.

c. When using a CAC to logon to the network, you will make sure it is removed prior to leaving the computer that you logged on.

d. Each person will use only authorized hardware and software on the DoD/Army Networks to include wireless technology. **No personally owned hardware, software, shareware, or public domain software to include telephony clients (e.g. Skype) is authorized without written approval by the Chief, Information Management Division.**

e. To protect the systems against viruses or spamming, use virus-checking procedures before uploading or accessing information from any system, diskette, attachment, compact disk, DVD or other media.

f. Do not attempt to access or process data exceeding the authorized information system classification level (Unclassified, Sensitive).

g. Do not alter, change, configure or use operating or programs, except as specifically authorized.

h. Do not introduce executable code (such as, but not limited to, .exe, .com, .cmd, .vbs, or .bat files) without authorization. Do not introduce or write malicious code.

i. Safeguard and mark with the appropriate classification level all information created, copied, stored or disseminated from the IS and do not disseminate it to other persons without a need-to-know.

j. Do not use Army- or DOD-provided information systems for commercial gain or illegal activities.

k. Maintenance will be performed only as specifically authorized, normally by the System Administrator (SA), remotely by the Enterprise Service Desk (800USAMITC), or IMD help-desk personnel.

l. Do use screen locks/passworded screen savers and log off the workstation when departing the area.

m. Immediately report any suspicious output, files, shortcuts, or system problems to the IMD Chief, MEDDAC , WTB or DENTAC IT support persons as appropriate and cease all activities on the system until it's checked. The USAMITC Enterprise Service Desk number is 1.800.USAMITC. DENTAC IT support section is 767.0874.

n. Address any questions regarding policy, responsibility, and duties with regards to the operation and security of Army Information Systems to the IMD Chief, or the appropriate System Administrator or Information Assurance Security Officer.

o. Understand that each Information System is the property of the Army and is provided for official and authorized use. Further understand that each system is subject to monitoring for security purpose and there is no expectation of privacy. Ensure that its use is authorized. Understand that there is no recognized expectation of privacy in official data on the IS and one may have only a limited expectation of privacy on personal data on the IS. Don't store data on the IS you don't want others to see.

p. Understand that monitoring of the network will be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution.

(1) Unethical use (e.g. Spam, profanity, sexual misconduct, gaming, extortion).

(2) Accessing and showing unauthorized sites (e.g. pornography, streaming videos, chat rooms).

(3) Accessing and showing unauthorized services (e.g. peer-to-peer, distributed computing).

(4) Unacceptable use of e-mail include exploiting list servers or similar group broadcast systems for purposes beyond intended scope to widely distribute unsolicited e-mail (SPAM); sending the same e-mail message repeatedly to interfere with recipient's use of e-mail; sending or broadcasting e-mail messages of quotations, jokes, etc., to multiple addressees; sending or broadcasting unsubstantiated virus warnings from sources other than the MEDDAC IAM (e.g. mass mailing, hoaxes, auto-forwarding).

(5) Any use that could cause congestion, delay, degradation or disruption of service to any government system or equipment is unacceptable use (e.g., video, sound or other large files, "push" technology on the internet and other continuous data streams).

(6) To show to unauthorized persons what is deemed proprietary or not releasable (e.g. Use of keywords, phrases or data identification).

q. Do not introduce privately-owned hardware or software to the work area. Personal equipment (IPods, MP3 players, external drives, laptops, etc.) are prohibited on Army networks and from being attached to Army equipment (including PCs) without prior approval of the C,.IMD. All USB/Thumb/Flash-type drives are currently forbidden without specific waivers (requests must be sent via digitally-signed e-mail through channels to Chief, IMD). Be aware: the encryption software for our systems can render your iPOD or other device inoperable.

8. OTHER THINGS TO CONSIDER.

a. **Protect your computer** and the network from software bugs. Log off at the end of your duty day. We have the systems set to automatically update during the evening. If you're still logged in, it might not be able to update as needed, or it might re-boot after an update and you'll lose your data. Normally, you want your PC logged off, but left on at the end of your duty day. BUT, there are exceptions:

(1) Because of the new Data-At-Rest encryption requirement, you should leave your computer (desktop or laptop/notebook/tablet) logged in overnight at least one night per week. All updates won't work unless the system is logged on. So, one night a week log in, lock the workstation, remove your CAC, and let the system stay on overnight.

(2) At least once per week, restart (reboot) your computer. This helps it "clear its throat" and will help it run more efficiently.

b. **Protect against disaster.** Copy your important data files to another drive (floppies are not an option – most of our systems don't even have floppy drives any more; copy them onto a CD or DVD). Update the copies at frequent intervals. Each network account has a corresponding folder (directory) on the network's H: drive. If you go to the H: drive, you should be in a folder named the same as your logon ID. That drive gets backed up regularly. There's limited room there, however, so use it for really important things. Also, realize that during backups, open files (those that are in use) are not backed up. Remember: **backing up data files is a User's responsibility.** If your system crashes and we have to re-do the hard drive, you'll probably lose ALL your data not saved or backed up elsewhere (like CDs, DVDs, or the H: drive). Most of our systems now have either CD or DVD burners, so you can create your own data CDs or DVDs for file backup. Since our space on the network servers is limited, please burn CDs as your backups (using your CDRW) rather than use the H: drive. Blank CD-R or CD-RW disks are available through your section's supply procedures. Contact 800USAMITC for assistance.

c. **Protect your equipment.** Don't eat, drink or snack over your keyboard, computer, terminal or other parts of the workstations you use. Don't put the PC directly on the floor. Use a stand, 2x4s, or an overturned file box. If you leave the PC on the floor, it sucks in dust and dirt. It also tends to get whacked by the buffer and/or glued to the floor when the floors get waxed. The magnets in the motors of the buffers and vacuum cleaners can also play havoc with the system hardware and your data.

d. **Protect your area.** Recognize, politely challenge, and assist people who do not belong in your area.

e. **Use only the system(s) you're supposed to use.** You have one PC identified as your primary PC. That's the one with your MS Exchange account installed (Outlook). You may also need to use others. Your use of PC systems is limited to only those PCs in your duty area. "Borrowing" a PC in a friend's work area is unauthorized without approval of the supervisor responsible for that area.

f. **Loss of computer equipment can result in disciplinary action** and you might have to pay for the equipment. Beyond that, however, these systems are likely to have medical data on them, so you could also be liable for a HIPAA violation.

g. **Be sure your output, CDs/DVDs, etc. are marked appropriately** (including SF710 UNCLASSIFIED sticker).

9. INTERNET AND E-MAIL USE. These are taken, in part, from the DoD Acceptable Use Policy in DoD 5500.7-R (Joint Ethics Regulation) section 2-301.

a. Beware of what you download. You're not supposed to load software on Army systems without approval through IMD. This is because it could contain code which will damage software or data on your or other Army AIS or provide data from Army systems to unauthorized recipients.

b. Do not transmit sensitive information via the Internet. Assume e-mail is not secure—just about anyone who makes the effort can read it. Never put in an e-mail message something you wouldn't put on a postcard. By tradition, using ALL CAPS IN AN E-MAIL is considered shouting and is viewed as being in poor form.

c. Never send or forward chain letters over e-mail—it's not only a violation of regulation, but it floods the system with unnecessary traffic.

d. Don't visit places on the Internet that you wouldn't want your mother, spouse, kids, significant other, or boss see you visiting. This includes not only pornography sites but also those sites that incite hatred or incite violence against any group due to their race, religion, national origin, sex, etc., or those that are just plain tacky.

e. DoD guidelines (and common sense) dictate that you limit your Internet browsing ("surfing") to work-related items. DoD also allows for limited "personal" surfing during breaks, lunch, and before or after work. **Your supervisor may or may not allow it, that's up to your supervisor.** The same rules of civility apply. IMD does have Internet usage monitoring software and we do check.

f. Chat rooms are off-limits except for Official Business chat rooms (they do exist, but there are very few of them).

g. Because it uses up so much bandwidth (the capacity of our Internet connections) Streaming Audio and Video is not to be accessed except as part of official business (to include training).

h. Internet Radio, similarly, is not authorized for use because of its bandwidth requirements.

i. Distributed Processing and Parallel Processing computer "sharing" (such as used for the Human Genome Project and Search for Extraterrestrial Intelligence, etc.) is not permitted on Army Information Systems. Although perhaps noble in intent, these distributed processing programs use up bandwidth, processor capacity, and are suspected of being a path for the introduction of malicious software and/or snooping.

j. Peer-to-Peer file sharing programs such as GoToMyPC, Napster, Kazaa, Morpheus, etc. are not permitted on Army systems.

k. Personally-owned computers, laptops, iPods, USB drives, etc., are not authorized on Army systems/networks.

10. IN CASE OF SUSPECTED VIRUS OR CLASSIFIED INFORMATION SPILLAGE. If you think your system has been compromised or infected by a virus, or if you think you've experienced a classified "spillage" incident (accidental introduction of classified material via e-mail, external disk, etc.), don't turn off the computer. Instead, remove it from the network (unplug the network cable) but leave it plugged in, logged on, etc. Notify your supervisor, call the Enterprise Service Desk (800USAMITC) to initiate a ticket, and have someone contact IMD for someone to come and check out the system. Again, **DO NOT TURN THE SYSTEM OFF**, but **DO REMOVE IT FROM THE NETWORK** and contact the ESD and IMD.

11. THE LAST PAGE OF THIS MEMORANDUM IS A RECEIPT FORM.

a. By signing the receipt, you acknowledge and consent that when you access Department of Defense (DoD) information systems there is no expectation of privacy. As stated in the logon banner:

You are accessing a U.S. Government (USG) information system (IS) that is provided for USG-authorized use only. By using this IS (which includes any, device attached to this IS), you consent to the following conditions:
--The USG routinely intercepts and monitors communications on this IS for purposes, including, but not limited to, penetration testing, COMSEC monitoring,, network operations and defense, personnel misconduct (PM), law enforcement, (LE), and counterintelligence (CI) investigations.
--At any time, the USG may, inspect and seize data stored on this IS.
--Communications using, or data, stored on, this IS are not private, are subject to routine monitoring., interception, and search mad may be disclosed or used for any USG-authorized, purpose.
--This IS includes security measures (e.g., authentication and, access controls) to protect USG interests--not for your personal benefit or, privacy.
--Notwithstanding the above, using this IS does not constitute, consent to PM, LE or CI investigative searching or monitoring of the content, of privileged communications, or work product, related to personal, representation or services by attorneys, psychotherapists, or clergy, and, their assistants. Such communications and work product are private and, confidential.

b. As stated in the user agreement:
--Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.
--The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.
--Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.
--Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.
--A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.
--These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.
--In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (ie., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege

or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

-All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

12. VERIFICATION. Your signature on the receipt page (last page) of this memo is verification that you've read this memo, recognize your responsibilities, and understand that unauthorized access to, or improper use of Army AIS is a violation of law and/or regulation. As such, these violations can result in administrative action and/or prosecution under Federal law (or, if in the military, the Uniform Code of Military Justice). Conviction can result in fines, imprisonment, termination of employment or discharge from military service, or a combination thereof.

13. SANCTIONS. REFUSAL OR FAILURE TO SIGN THE RECEIPT WILL RESULT IN TERMINATION OF NETWORK AND OFFICE AUTOMATION SERVICES.

14. FOR FURTHER INFORMATION. Point of contact for this memorandum is IMD, (912) 435-5962.

ARTHUR N. KIRSHNER
Chief Information Officer and
Chief, Information Management Division
USA MEDDAC, Fort Stewart, GA

1. This is the receipt for the subject memo and is to be completed and turned in with your account request sheet. Keep the memo itself for reference and use. Keep the rest of the AUP for your periodic review and reference.

2. Signing this receipt is verification that you've read this memo and understand that unauthorized access to, or improper use of Army AIS systems or networks is a violation of law and/or regulation. As such, these violations can result in administrative action and/or prosecution under Federal law (or, if in the military, the Uniform Code of Military Justice). Conviction can result in fines, imprisonment, termination of employment or punitive discharge from military service, or a combination thereof.

3. Refusal or failure to sign the receipt will result in termination of Network, AHLTA, CHCS, Essentris, other network resources and general Office Automation services. Similarly, you can lose access for failure to complete your HIPAA initial or refresher training, or your annual Information Assurance Awareness Training.

4. Please sign this page and return it to IMD with your account request form, and retain the other pages of this memo for your records and as a reference. Thank you.

5. Please check your personal information in Exchange periodically and provide IMD with updates as changes occur – rank or civil service grade, office symbol or location, duty phone, supervisor, etc.

6. Don't forget your annual IA training and HIPAA refresher training.

STATEMENT

I understand that repetitive violations of this Acceptable Use Policy and User Agreement or AR 25-2 security measures will result in the loss of my network access privileges.
I further understand that in the event of such loss of privileges I will receive a written counseling statement from my first line supervisor, and in order to lift this restriction a memorandum from my first-line supervisor will be required.
Such a request will be routed via the Division/Department Chief to the C, IMD.

Signature
(Please Print Below)

Date

Last Name

First Name

Middle Initial

MCUB-IMD 16 February 2012

Protect patient privacy
Use it for work
Don't share your logon
Don't load things or plug things in without permission
Don't "surf" where you wouldn't want your momma to see
Back up your own stuff onto CD or DVD.
Be responsible.