BY ORDER OF THE COMMANDER,
354TH FIGHTER WING CC (PACAF)

354TH FIGHTER WING INSTRUCTION 33-201

14 FEBRUARY 2002

Communications

POLICIES AND SECURITY PROCEDURES FOR THE EIELSON METROPOLITAN AREA NETWORK (EMAN) AND SECURE EIELSON METROPOLITAN AREA NETWORK (S-EMAN)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: 354 CS/SCBB1 (2d Lt Rebecca Salter)

Certified by: 354 SPTG/CC
(Colonel David Lawton)
Pages: 7
Distribution: F

This instruction implements Air Force Policy Directive (AFPD) 33-2, Information Protection; AFI 33-115V2, License Network Users and Certifying Network Professionals; AFI 33-119, Electronic Mail Management and Use; AFI 33-129, Transmission of Information Via the Internet; AFI 33-202, Computer Security; AFI 33-204, Information Protection Security Awareness, Training, and Education (SATE) Program; AFI 33-223, Identification and Authentication; AFI 31-501, Personnel Security; AFSSI 5027, Network Security Policy. This instruction includes policies on security for the EMAN, S-EMAN, SafeSuite, E-mail, the Internet, Distribution lists, the "For Sale" board and passwords. Technology has allowed us to communicate and pass on information at higher speeds. This ability also brings with it security risks. Each individual with access to the EMAN and S-EMAN must be vigilant in ensuring the protection of the network and each computer individual system. Each individual must also ensure that privileges such as E-mail, access to the Internet and the "For Sale" board are not abused. This instruction applies to all units assigned to the 354th Fighter Wing and tenant units who access the EMAN and/or S-EMAN.

1. General. This instruction consolidates policies regarding the use and security of the EMAN, S-EMAN, Internet and E-mail. Access is a privilege that can be taken away. Adherence to these policies will help ensure information doesn't fall into the wrong hands.

2. Security.

2.1. Access to the EMAN. All personnel requiring network access must have a completed National Agency Check (NAC) or equivalent.

2.1.1. For new military members:

2.1.1.1. Unit commanders may grant interim access based on verification that the required investigation has been initiated.

2.1.1.2. Information Assurance (IA) Awareness training must be conducted and documented prior to granting access.

2.1.2. For new civilian employees, contractors, summer hires, and volunteers:

2.1.2.1. Unit Security Managers (USM) will submit an AF Form 2583, *Request for Personnel Security Action*, to the 354th Security Forces Squadron (SFS) requesting a Local Files Check (LFC).

2.1.2.2. The 354 SFS will conduct the LFC and inform the USM of the results.

2.1.2.3. If the LFC is favorable, the USM will prepare a letter for unit commander signature granting interim access to the EMAN until the NAC or further clearances are favorably completed. This letter will be addressed to the NCC Communications Service Center and will accompany the Eielson Metropolitan Area Network (EMAN) access form to the Communications Service Center.

2.1.2.4. IA Awareness training must be conducted and documented prior to granting access.

2.1.2.5. System Administrators and Workgroup Managers must implement measures to limit access to only information required to conduct assigned duties.

2.1.2.6. Supervisors and commanders must ensure increased monitoring of the individual's Automated Information System access.

2.1.3. Any violations of security regulations will result in denial of access to the EMAN.

2.2. Internet Security SafeSuite (ISS) Network Scanning and Vulnerability Reporting Policy. PACAF requires all of its bases to use ISS Internet Scanner to perform network vulnerability scans. ISS is the Air Force's network scanning tool of choice and is part of the Base Information Protect initiative.

3. E-mail and Internet Use. E-mail and the Internet are for official use, with limited personal E-mail use additionally authorized. Official use of E-mail and the Internet is described as, "use required in performance of assigned duties." Using E-mail or the Internet for other than official or authorized purposes may result in adverse administrative or disciplinary action.

3.1. Base policy authorizes personal E-mail use for brief personal communication such as checking in with colleagues or friends for morale and welfare purposes. Personal E-mail is used to facilitate communication that would normally take an individual away from their workcenter, but can be performed through the use of E-mail. Specific restrictions and unacceptable uses include:

3.1.1. Pornography, profanity, hate/racist literature, chain letters, large broadcasts, and group mailings.

3.1.2. Sending abusive, offensive, harassing, or intimidating material to or about others that violates Air Force standards of behavior. This includes, but is not limited to, humor considered in poor taste or offensive, and political or religious lobbying.

3.1.3. Sending or receiving E-mail for personal or commercial financial gain.

3.1.4. Use that adversely affects performance of official duties.

3.1.5. Use that overburdens the communications system.

3.1.6. Sending or distributing copyrighted materials (including cartoons) unless approval is obtained from the author or publisher.

3.1.7. Using another person's account or identity without appropriate authorization or permission.

3.1.8. Permitting any unauthorized use or access.

3.1.9. Use that creates additional expense to the DOD.

3.1.10. Specific prohibitions for use of personal E-mail includes the following additional restrictions:

3.1.11. No attachments.

3.1.12. Use must be of reasonable duration and frequency, and, whenever possible, made during DOD employee's personal time, such as after duty hours or during lunch periods.

3.2. Unauthorized use of the Internet includes the same restrictions identified for E-mail plus the additional prohibitions below:

3.2.1. Participating in "chat rooms" or open forum discussion unless for official use.

3.2.2. Unofficial access to newsgroups, listservers, electronic groups, and games.

3.2.3. Downloading and installing software from commercial web sites without approval from the Wing Information Assurance Office.

3.3. The basic standards for using E-mail and the Internet are based on common sense, common decency, and civility. Communications that would reflect adversely on DOD or the DOD component are not permitted.

3.3.1. Do NOT send official information over a commercial ISP (i.e. hotmail, gci.net, etc)

3.3.2. To do official work at home (EPRs, OPRs, FOUO, or other items) the following applies:

3.3.2.1. Take the data home on a diskette.

3.3.2.2. Do NOT store any official information on your personal system.

3.3.2.3. Do NOT store Privacy Act information on your personal system.

3.3.2.4. Work off the diskette.

3.3.2.5. Once completed, delete Temp files and confirm no data is stored on your personal machine.

3.3.3. Always check the diskette for viruses prior to use.

3.4. IAW AFI33-119, Para. 2.5, the Wing IA Office will conduct random inspections of stored E-mail communications to ensure compliance with E-mail policy. These inspections will take place during regularly scheduled Staff Assistance Visits.

4. Distribution Lists.

4.1. The 354 FW E-mail distribution lists are a mechanism for 354 FW and tenant units to receive official correspondence from unit commanders and their designees. These distribution lists consist of the following, or any combination of the following with a user's personal distribution list, that results in the receipt of E-mail by these personnel or their organizations:

4.1.1. Eielson Distro A: 354 Fighter Wing and Group Commanders Only.

4.1.2. Eielson Distro B: 354 Fighter Wing Staff Agencies.

4.1.3. Eielson Distro C: Squadron Commanders Only.

4.1.4. Eielson Distro D: Wing Tenant Units.

4.1.5. Eielson Distro E: All of A through D.

4.2. Wing, group, and squadron commanders have the authority to generate or redistribute E-mail received through these distribution lists to members of their organization, and may delegate this authority as required. Unless specifically authorized by their unit commanders, personnel are not authorized to use these distribution lists for the dissemination of information, to include official correspondence.

4.3. Similarly, only members of Eielson Distro E, or their designees, are authorized to use the 354 FW distribution lists to transmit information to these distribution lists or to an entire organization. This prohibition includes attempts to create distribution lists by selecting all members of any organization. Common infractions of this policy include attempts to widely promote fund-raising events; this correspondence is not official and can create a burden on our networks.

4.4. Unit commanders will ensure adherence to this policy.

5. Eielson AFB Electronic “For Sale” Board.

5.1. As a convenience to Eielson AFB personnel who wish to privately sell or purchase merchandise, an electronic “For Sale” board is available in the “Public Folders” of Microsoft Outlook. Advertisements for personal goods may be posted here free of charge. The following rules apply:

5.1.1. Post only those items that are for an individual, one-time sale (e.g., vehicles, computers, furniture, garage sales, pets, etc.).

5.1.2. Advertising commercial or home businesses (e.g., Mary Kay, Avon, Longaberger, etc.) is strictly prohibited.

5.1.3. Do not attach pictures, photos, or video of the item(s) being sold. If the prospective buyer wishes to see the item(s), set up an appointment with them to view the item(s), or provide an Internet link to a picture. The linked page may not be located on the EMAN.

5.1.4. Post the item(s) only once per day.

5.1.5. Do not use the “For Sale” board for comic relief or for bickering/bartering with other people.

5.1.6. Use of profanity or other improper language or terminology is prohibited.

5.1.7. The “For Sale” board is for military members, DoD civilians, their dependents, and contractors assigned to Eielson AFB only. Do not post items for others.

5.2. Use of the “For Sale” board is a privilege, not a right. Abuse of this policy may result in administrative action or the loss of the “For Sale” board on the network.

5.3. Questions about the electronic “For Sale” board should be directed to Unit Computer Security Managers or to the Wing Information Assurance Office at 377-2815.

6. “Government Free Issue” Board.

6.1. The following rules apply to items posted on the “Government Free Issue” board located in Microsoft Outlook:

6.1.1. Post only those items that are for official use only (FOUO).

6.1.2. Do not attach pictures, photos, or video of the item(s) being sold.

6.1.3. Post the item(s) only once per day.

6.1.4. Do not use the “Government Free Issue” board for comic relief or for bickering/bartering with other people.

6.1.5. Use of profanity or other improper language or terminology is prohibited.

6.2. Abuse of this policy may result in administrative action or the loss of the “Government Free Issue” board on the network.

6.3. Questions about the electronic “Government Free Issue” board should be to Unit Computer Security Managers or to the Wing Information Assurance Office at 377-2815.

7. Passwords. The 354 FW policy on passwords is designed to ensure the integrity of the network by frustrating hacker “crack” attempts while keeping the user in mind. Password complexity will be enforced by the operating system, i.e., the system will not allow you to use a password that violates the wing standard.

7.1. Your password must be:

7.1.1. At least eight (8) characters long.

7.1.2. Contain at least one lowercase letter, one uppercase letter, one numeral in any position other than the first or last position and one special character (i.e. non-alphanumeric) in any position other than the first or last position.

7.1.3. Contain five unique (non-repeated) characters.

7.2. Your password must not contain:

7.2.1. More than four continuous letters of your name (first, middle or last) or office symbol, neither backwards or forwards.

7.2.2. More than four continuous letters of your username, neither backwards or forwards.

7.2.3. Three repeated characters

7.2.4. More than four continuous letters the same as any of your last five passwords.

7.2.5. Anything that “looks” like a word, even using special characters.

7.2.6. Any set of three keys close to each other on the keyboard.

7.3. Things to remember when changing your password:

7.3.1. You must change your password every 90 days.

7.3.2. You must wait at least 1 day before changing your password again.

7.3.3. The operating system will search an electronic hacker dictionary for words and names (forward and backward) within your password, the presence of which will cause your proposed password to be rejected. Even if you place special characters between the letters of a word (i.e., “d*o*g”), the password checker may reject it.

7.3.4. You may try as many times as necessary to obtain a valid password; the system will not lock you out simply because it rejected your password change attempt, no matter how many times it rejects the password you entered.

7.3.5. Do not write your password down, especially where it can be accessed around your desktop. Inspectors – and hackers--have discovered passwords written on post-it notes attached to computers, under keyboards and in desk drawers.

7.3.6. **Never** give your password to **anyone**. No one, to include communications squadron personnel, your supervisor, nor your commander, has the need to know your password.

7.3.7. The NCC runs a password-cracking program on a regular basis. If a user’s password is cracked, that account is locked until the user provides identification to his or her Workgroup Manager or the Communications Service Center, at which time the password must be changed to meet the standard.

7.3.8. If you need assistance in developing a valid password or clarification of these rules, work with your Workgroup Manager. If he/she is not available, call the Communications Service Center at 377-COMM.

8. Computer Maintenance Procedures. Maintenance of computers on the EMAN is provided by the unit Workgroup Manager (see 354 FWI 33-102). Users should contact their Workgroup Manager to resolve their day-to-day problems with their computers. The following are unauthorized user computer procedures:

8.1. Open computer cases and remove or tamper with internal components.

8.2. Swap or cannibalize parts from one computer to another computer.

8.3. Add computers to the domain or remove computers from the domain.

8.4. Install any application software on a computer (contact a Workgroup Manager).

8.5. Format or partition hard drives on any system.

8.6. Install operating systems on any system.

8.7. Hold administrative control on any system in the organization.

8.8. Remove or modify virus-scanning software.

8.9. Manipulate or change file/shared permissions on shared network resources to include but not limited to printers, shared folders, shared files and other peripheral devices.

8.10. Hack\Crack or attempt to access unauthorized information.

8.11. Violation of any of the above may lead to license suspension from the EMAN in accordance with FWI 33-102.

9. S-EMAN Accounts.

9.1. All personnel requiring access to the S-EMAN must fill out a NSA Form G6521or its equivalent web-based form found on the Eielson intra-web (**https://intraweb/**). This form must be signed by the user's Terminal Area Security Officer (TASO). The TASO will verify the user's clearance information, ensure a valid "need to know," and that the user is authorized to access the information. The form will also state the S-EMAN areas that you require access to (i.e. Theater Battle Management Core Systems (TBMCS), Classified Tactical Aircrew Scheduling Airspace Management System (TASAMS), E-Mail, and Internet).

9.2. All EMAN policies are applicable to use of the S-EMAN. In addition, users must take extra care to ensure secret information is not compromised by following established handling, marking, and storage procedures.

9.3. If access to TBMCS or TASAMS is required, a training class must be attended. This class can be scheduled by calling 377-5093. On the appointed day of training, you will need to bring the form, G6521, to the C2 systems work-center in the basement of Amber Hall, room B-80. Once training has been completed, a user account for the necessary system will be created.

9.4. If only Email and Internet access are required, there is no need to attend the training class. Simply come to the C2 systems work-center with the proper paper work and a user account will be created.

BOB D. DULANEY, Brig Gen, USAF
Commander