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

354 FW INSTRUCTION 33-102

2 APRIL 2001

Communications and Information

WORKGROUP MANAGER'S ROLES AND RESPONSIBILITIES

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/SCXP (SSgt Shane Flint)

Certified by: 354 SPTG/CC
(Colonel David Lawton)
Pages: 10
Distribution: F

This instruction implements the Workgroup Management guidance outlined in AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*; AFI 33-115V1, *Network Management*; AFI 33-115V2, *Licensing Network Users and Certifying Network Professionals*; AFI 33-114 *Software Management*; and 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*; Information is a resource critical to readiness; it is a force multiplier and catalyst to the realization of the AF Core Competency—Information Dominence. Decisively managing DoD and Air Force information ensures maximum application of information warfare for military force effectiveness. Military and civilian leaders, and their staffs, at all levels of command, and within every organization, must view information as a strategic resource. This instruction applies to all units assigned to the 354th Fighter Wing, and provides specific guidance on Workgroup Management to each unit ensuring that an effective and efficient use of information managers and information systems is maintained.

1. General. This instruction provides guidance for Workgroup Management on Eielson AFB. This gives general instructions on Workgroup Managers (WM) responsibilities, roles, and required training. WMs play a vital role in the maintenance and security one of the Air Force's newest weapons system—the network. This Instruction reinforces the Air Force's efforts to Operationalize and Professionalize the network—"One Air Force, One Network."

2. Workgroup Managers (WM).

2.1. WMs are the first line of help in problem resolution for network users. WM responsibilities belong to the 3A0X1 career field (Information Resource Manager), unless no information resource managers are assigned. They are the only career field which receives 3/7-level workgroup management training as well as continuing information technology training throughout their career. If a 3A0X1 is not assigned, available Air Force specialty codes (AFSC) or civilian occupational series

may perform WM duties once trained and certified by the communications squadron. WMs are usually not assigned to the Network Control Center (NCC), although they are a logical extension of the Help Desk (HD) team. WMs possess developed knowledge of hardware, software, and communications principles, to aid in installation, configuration, and operation of client/server devices. They resolve the day-to-day administrative and technical system problems users routinely experience. Furthermore, they work closely with their Functional System Administrator (FSA), if assigned, or directly with the HD when they cannot resolve customer problems.

2.2. The commander will appoint WMs in writing (See **Attachment 1**). Any unit with more than one WM assigned will identify a lead WM (see paragraph **2.2.1.**). The lead WM is the primary focal point for workgroup management issues within their squadron. If only one 3A0X1 occupational series is assigned, they will be the lead WM for the unit. Any additional WMs will likewise be assigned to the 3A0XI occupational series, civil service computer specialist series, or to an assigned functional system administrator (FSA), i.e., the FSA for PC-III, Standard Base Supply System, Automated Business Service System etc. The only exception to this principle is the 354 LSS, as they have only one 3A0X1 authorized and no civil servant equivalents or FSAs. The 354 LSS may appoint one additional WM, at the commander's discretion, to serve with the lead WM. This additional WM is required to complete and maintain the same level of training and certification as any other WM. Base the decision on amount of WMs to assign on the number of users and client/server devices assigned to an organization. (See **Attachment 2** for a suggested WM model).

2.2.1. Lead WMs. WMs ensure a solid WM program is instituted within the unit/staff agency, provide direction to all other assigned WMs, and maintain primary access to all tools and permissions granted by the NCC. The lead WM will take responsibility for communications with the HD on technical issues and disseminate technical information from the HD to other WMs and users assigned to the unit/staff agency. Lead WMs should/may be assigned as the Computer System Security Officer (CSSO), Unit COMPUSEC Manager (UCM), Organization Computer Manager (OCM), and Terminal Area Security Officer (TASM). Ideally, Lead WMs are fully trained and certified before assuming their responsibilities. If this is not possible, they will be entered into a mandatory training and observation mode upon assignment. Furthermore, they must complete all required training and certification within 15 months of appointment.

2.3. NCOIC WM Training and Development. This position is assigned to the Communications Squadron. The position requires a highly trained/skilled 3A0X1; the individual will bear a major responsibility to provide training for all assigned WMs, and act as the liaison between all assigned IMs and the Communications Squadron. Additionally, this person will provide staff assistance visits to each unit on an annual basis (see **Attachment 3**). This position reports directly to the Base IM Functional Manager (FM) and provides recommendations in regards to training, utilization, and assignment of WMs. Finally, this position will conduct monthly WM meetings.

3. Training. WM training will be provided by the NCOIC of WM Training and Development, in accordance with AFI 33-115V2 and PACAF implementation guidance. WMs will attend a basic Windows NT training course (40hrs), advanced Windows NT training course (30hrs), complete required Computer Based Training (252.5hrs), serve 14 consecutive months in a WM position, and receive training and certification of all required areas in the CFETP before receiving certification in the WM crew position. All inbound 3A0X1s who have completed requirements at their previous assignment will go through a local orientation certification briefing from the NCOIC of WM Training and Development. Upon successful completion, a statement will be annotated on the AF Form 623a to certify qualification in the WM crew

position. The communications squadron or FSAs may provide additional information systems training as needed.

4. Area of responsibility. WMs area of responsibility consists of technical and administrative support of information systems. These areas are separated into four categories: Physical, Security, Records Management, and Administrative.

4.1. Physical Responsibility. WMs are responsible for the client/server (PC's or Workstations) devices assigned to a unit, staff agency, or section (including all peripherals). The line of responsibility stops at the wall connection. WMs have no jurisdiction for any network architecture behind the wall jack to include: switches, hubs, or routers installed by Communications Squadron Network Management personnel. WMs are forbidden to move, power down, disconnect, or otherwise configure any network equipment, except under the explicit instruction of Network Management personnel. Violation of this instruction will jeopardize a WM's certification. Report any suspected network equipment problems to the HD immediately.

4.1.1. Software**.** WMs are responsible for managing the software that is installed on all their workstations. This includes installing, reinstalling, testing, and configuration management of installed software. Also WMs will maintain all documentation, license agreements, and the original media. WMs must ensure that all software installed on computers is approved for use on Air Force domains. Furthermore they will ensure the organization does not use any shareware or public domain software not approved by the Designated Approval Authority (DAA). WMs shall, at a minimum, control all licensed software in a manner to preclude copyright infringements (not including enterprise wide license). WMs will install updates to software, including service packs, security patches, and hot fixes, as soon as they are disseminated for installation. The Wing Information Assurance (IA) office will provide guidance on updates and installation points as they are approved.

4.1.2. Configuration Management**.** WMs are responsible to ensure all workstations are configured in accordance with the approved NCC configuration standards which are provided by the NCC. WMs will coordinate with the NCC when there are questions about configuration of new software or uncommon software that they may use in their organization. Configuration management ensures remotely managed NCC software updates can be accomplished in a timely and secure manner. WMs will maintain instructions for software that requires special configuration.

4.1.3. Reporting Procedures. WMs are responsible for reporting to the HD any problems that cannot be resolved internally. The HD will generate a trouble ticket for calls, and provide WMs with an open and close date along with fix actions accomplished. WMs should provide the help desk with specific information on problems to ensure quick isolation and rectification of the problem. WMs are responsible for following up with the HD if they are not provided with the above stated information or the trouble ticket is not resolved within a timely manner. Cooperation between the WM and HD are critical keys to success for each party concerned.

4.2. Security. WMs are directly responsible for system security. This section is broken into three portions: Computer Security, User Security, and Information Security.

4.2.1. Computer Security. Individual Computer workstations are the weakest link in network security. Workstation security will be closely monitored; security demands the highest priority for WMs…the integrity of your systems depends upon it. The administrator password and account

will only be known and shared by WMs. The default administrator user account should be renamed to provide an added level of security. Passwords will comply with strong password policies; WMs will not add users to the administrator group on PCs. If a user needs special privileges (to run special software or programs) WMs will create a local policy that will allow users to run those programs. Virus scanning software will be on every machine, stand-alone or network. WMs will ensure updated virus definitions are installed on machines in an expedient manner, and report all viruses to IA as outlined in 354FW Instruction 33-101 and AFSSI 5021. WMs will brief all users on the minimum security requirements, and follow up within the area of responsibility to ensure that the minimum measures are applied. All security patches and security updates will be applied immediately, unless otherwise informed by IA. WMs will comply with all additional computer security procedures, not covered here, IAW AFI 33-202.

4.2.2. User Security. Users depend upon WMs to provide day-to-day help with computer related problems. WMs are responsible for ensuring all users have the proper training and clearances to work on computers connected to the LAN. WMs will ensure all users complete the appropriate Security Awareness Training and Education (SATE), have the appropriate security clearance, and complete the Eielson AFB Metropolitan Area Network Form, before sending users to the HD to establish a network account. Details on the training and licensing requirements, and guidance on access to the training will be provided to the users by WMs. Upon successfully completing training, the user is licensed to use the network and granted access to required network resources. User Information Assurance training has been standardized in the Internet-based training (IBT) course. Successful completion of the IBT course satisfies DoD user certification, SATE training, and Air Force network users licensing. If wing IA devises additional training for Eielson AFB, WMs will administer the locally developed training to their assigned personnel and maintain records of the training program using locally developed procedures.

4.2.3. License Suspension. If a user engages in conduct inconsistent with the licensing principles, WMs may, with the approval of the user's supervisor, recommend denial of network access. Network suspension is a non-punitive action and the suspension alone, as opposed to the underlying conduct, may not provide the basis for adverse action. Based on the WMs recommendation, the designated approval authority may suspend a users license when deemed necessary in the interest of effective information operations. WMs must submit a written notification of the suspension to include the date and reason for suspension. WMs will submit a copy of the notification of suspension to the NCC for review and/or further action. All other license suspension procedures will be in accordance with AFI33-115V2. Following are some examples of actions inconsistent with licensing principles: installing unauthorized software; failure to maintain an acceptable level of proficiency on a critical program; threatening the security of the network via virus propagation; violation of government E-mail or Internet use policies; hacking or attempting to access unauthorized information; maliciously altering or changing systems files, operating systems, or application software without the consent of the WM.

4.2.4. Information Security. Each user is responsible for securing classified information. All users should ensure that classified information is not shared, distributed, or processed on a system that doesn't meet the minimum classification standards. WMs will ensure all users are aware of the location of workstations authorized to process classified information and provide them with any additional instructions needed to ensure information security. WMs will immediately notify wing IA if a security incident occurs on any information system within their unit. In addition, WMs will

comply with local reporting procedures for classification contamination that is provided by the Wing IA office, and PACAF Pamphlet 31-2.

4.3. Records Management. In accordance with public laws and directives, all official records must be stored and maintained until proper disposition, no matter what media they are recorded on. Electronic records storage is the joint responsibility of WMs, Functional Area Records Managers (FARM), Records Custodians (RC), and users. WMs are responsible to assist the FARM and RC in establishing an electronic records file plan in accordance with Air Force, DoD, and PACAF instructions. The NCC will provide a records storage area for each squadron on a file server, and provide assistance in conjunction with the HD in creating access groups for each squadron. It is the WM's responsibility to create the groups and provide the list of groups to the NCC for implementation. It is also the WM's responsibility to assign the proper individual users to the proper access groups. If possible, the WM will provide the group new users will be assigned to. WMs are responsible for maintaining proper backups of electronic records at on monthly basis as a minimum. Lead WMs will be provided control of the squadron folders for records management; they are responsible for controlling the proper permissions to each group within the squadron. WMs shall assign permissions at group levels and avoid assigning permissions at the user level. The Base Records Manager provides initial training for records management, and can provide further guidance on these procedures.

4.4. Administrative. There are many other areas a WM may be responsible for to include: additional duties, otherwise known as administrative category responsibilities not directly related to WM. The administrative category covers items a WM must specifically maintain to provide a successful WM program within their area of responsibility. The positions listed below are interlinked with one another, and the WM could logically be assigned any of the following:

4.4.1. Computer Systems Security Officer (CSSO). WMs should be assigned as the unit CSSO. (Specific duties are outlined in AFI33-202). In addition, CSSOs should institute internal reporting procedures for users to report virus attacks, suspicious malicious activity, and security violations to the CSSO for subsequent reporting to wing IA. The CSSO will ensure all users are aware of the unit CSSO by posting the name, duty phone number, and reporting procedures in a common area. The CSSO will brief new users about the unit's reporting procedures before approving user accounts and signing off the Eielson AFB Metropolitan Area Network Form. The CSSO will ensure that the 354 FW form 009 is annotated properly and available at all computer workstations.

4.4.2. Unit COMPUSEC Manager (UCM). UCM duties are outlined in AFI33-202. In addition, the UCM should include an initial COMPUSEC briefing to new users, along with an annual briefing. UCMs will receive information and training from wing IA. UCMs will post their name and duty phone in a prominent unit area.

4.4.3. Organization Computer Manager (OCM). WMs logically should be assigned as the OCM. The OCM does not include duties as the ADPE custodian.

4.4.4. Terminal Area Security Monitor (TASM). WMs should also be assigned as the TASM if the unit has classified systems assigned.

4.4.5. The following items are minimum administrative tools a WM should maintain for a successful WM program.

4.4.5.1. Internal Trouble Call Tracking. WMs will maintain a program to internally prioritize and track computer-related problems and provide users with an estimated time of completion for internal trouble calls within their unit. Lead WMs of large squadrons should have a shared

trouble ticket database readily available for all assigned WMs to update, closeout, and verify the status of trouble calls. At a minimum, the database or program should contain the user's name, nature of the problem, building number, room number, date and time of problem, brief description, WM assigned to the problem, and the fix action. Maintaining these minimum categories allows the WM to track trends and share fix actions throughout the squadron or to WMs of other units. After a WM exhausts all available internal resources without success, contact the HD for resolution.

4.4.5.2. Information Systems Database (ISD). WMs will have an ISD available at all times. The ISD will contain vital information on each computer assigned to a WM. The following information is the minimum to maintain within the ISD: building and room number of the computer; computer host name; stand alone or network; make of the computer, processor speed; amount of physical memory; accreditation expiration date; special software; special configuration requirements; operating system; and security or service patches installed. WMs are responsible for maintaining the ISD for their assigned area of responsibility. Lead WMs are responsible to provide information to all flight level WMs for creation, standardization, and maintenance of unit-level ISD.

4.5. **WM and User Interface.** Lead WMs should ensure users know their assigned WM via posted signs with names and contact numbers in a public access bulletin board. Workgroup management is a customer service-based duty. As such, WMs must accept responsibility as the primary contact for user information and education concerning standard information systems and associated software. WMs will train users on basic application software fundamentals to ensure users can effectively interface with respective standard software applications.

5. Web Page Development and Maintenance. Web page development is important to every squadron. Web pages will be maintained by 3A0X1s and/or WMs (this position is normally referred to as the page maintainer) trained on Hyper Text Mark-up Language (HTML) to maintain web pages at every level. When a 3A0X1 is not assigned, the commander may designate another AFSC to maintain unit web pages. All web pages must be in accordance with DoD policy and AFI33-129. Updated web pages ensure that users will use this form of information on a regular basis; maintainers should ensure constant currency of their web pages and coordinate with the web administrator for posting any changes.

6. NCC WM Coordination. The Lead WM will work closely with the NCC on issues that affect a large number of users in their organization. Some issues a WM will coordinate with the NCC are: any changes to user or global groups; institution of log on scripts within the organization; and any changes to user or organizational E-mail accounts. WMs will not receive permissions or privileges that can affect other units other than their own on the Eielson Domain. At a minimum the NCC will provide a WM group that allows for the most liberal privileges available for a WM to accomplish their work without affecting other users or units on the domain. The NCC will provide access to troubleshooting aides (like Microsoft Tech Net) to assist trained and certified WMs in the performance of their duties. WMs should also coordinate with

the NCC when new or unusual software is added to systems to ensure configuration management issues are covered, and ensure updates will not affect program operation.

KENNETH M. DECUIR, Brig Gen, USAF
Commander

Attachment 1

SAMPLE APPOINTMENT LETTER FOR WM

DATE

MEMORANDUM FOR 354 CS/SCX/SCMH

FROM: Your Organization

Subject: Appointment Letter for Workgroup Managers (WM)

1. The following individuals are assigned as WMs for the (organization).

Name & Rank	Duty Phone	BuildingNumber	Position ID
SSgt John Doe	XXX-XXXX	4444	Lead WM
SrA Jane Doe	XXX-XXXX	4441	WM

2. These individuals will be the point of contact for all users assigned to (organization) on computer maintenance, security, and configuration. The assigned WMs understand their duties and will work closely with the Help Desk and NCC to resolve computer-related problems and issues. Please add these members to the (organization) WM Group.

Signature Block of Commander

Attachment 2

THE WORK GROUP MANAGER MODEL

Squadron Level

Below is a workstation-to-user ratio for the following suggested model, considering at least a one-to-one user-to-workstation ratio. However, in some cases, there could be as much as a five-to-one user-to-workstation ratio, especially in large squadrons.

Number of Workstations/Users	Time dedicated to WM/Other Duties
10-70 Workstations/Users	40%/60% or less
70-140	70%/30%
140-220	1 Full time WM
220-300	2 Full time WM
300-400	3 Full Time WMs

Flight Level

Below is a workstation-to-users ratio for the following suggested model, considering at least a one user to one workstation ratio. At the flight level, the possibility of many users utilizing a single workstation is much more common.

Number of Workstations/Users	Time dedicated to WM/Other Duties
20 or less	10%/90%
20 to 40	30%/70%
40 to 60	50%/50%

Attachment 3

WM STAFF ASSISTANT VISIT & SELF INSPECTION CHECKLIST

1. Are unit WMs appointed by the unit commander and does the NCC WM list reflect this appointment?

2. Is the Lead WM identified if there is more than one WM assigned to the organization?

3. Do Lead WMs have internal reporting procedures for WMs within the organization?

4. Does the Lead WM have a software control program instituted for the control of installed software on unit workstations?

5. Are assigned workstations configured to standard configuration management guidelines as directed by the NCC?

6. Are strong administrative passwords enforced for local administrator accounts (eight upper/lower case alpha characters with at least one numeral and special character)?

7. Are any users added to the administrative group on workstations?

8. Is virus-scanning software installed on all workstations within the organization and are permissions assigned to user groups?

9. Are there posted forms identifying the unit's WM, CSSO, and UCM?

10. Does the WM have an electronic records program in place for the organization?

11. Has the WM implemented an internal trouble-call tracking program?

12. Does the WM maintain an Information Systems Database of all unit systems?

13. Are IMs responsible for developing and maintaining unit web pages if assigned?