

Module 1

Introduction to Workgroup Management

1.1 OBJECTIVES

After this training students will be able to:

- Define Workgroup Management
- Summarize the roles and responsibilities of workgroup managers
- Summarize the legal issues related to Workgroup Management

1.2 OVERVIEW

Welcome to the Air Force Workgroup Management (WM) Course! This course is designed to give you a basic foundation in WM knowledge and skills. This course is structured in a modular format and your instructor will guide you from module to module. We'll start with Module 1, Introduction to Workgroup Management, and work through to Module 12, Information Technology Requirements Planning.

In this particular module, we will discuss how technology led us to the creation of WM, what WM is, what responsibilities a workgroup manager has, what legal precautions workgroup managers need to be aware of, and review WM in the holistic perspective of Enterprise Information Management (EIM).

1.3 TRANSFORMATION TO WORKGROUP MANAGEMENT

Historically, and to a much lesser extent today, an information manager's primary job was to format and type correspondence, messages, publications, and reports for unit personnel. Information managers also ordered, posted, and filed publications; coded, filed, stored, and disposed of records; prepared TDY orders; sorted and dispatched mail; and safeguarded classified material ensuring proper markings and storage. Today, due to the injection of information technology into the workplace, end users now perform many tasks previously accomplished by information managers. Using electronic forms, publications, templates, and features available in desktop software, unit personnel do much of this work themselves. The introduction of electronic workflow, electronic records management, Air Force Messaging Services, the Defense Travel System, and the Common Access Card will further reduce the information managers "traditional" workload and free them to focus on fusing information requirements with information technology.

Refocusing information managers towards integrating information technology, information management (IM), and information networking skills creates a nucleus of professionally trained personnel for centrally managing information and information technology as force multipliers for improving decision-making. Because an enormous amount of the information managed today is stored on networked and stand-alone computers, the IM career field now includes WM as a core function.

However, we must keep focus of the fact WM is a core function and not the only function we perform as information managers. Figure 1-1 illustrates the core functions information managers are accountable for and your

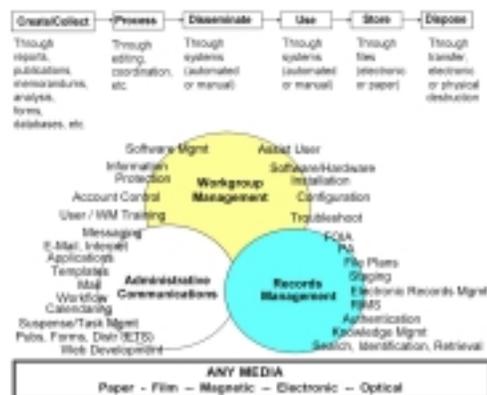


Figure 1-1. Information Life Cycle and Information Management Responsibilities

responsibility to management throughout its life cycle (creation/collection, processing, dissemination, use, storage, and disposal). As an information manager you are charged with learning and exploiting information technology and leveraging this knowledge to improve your organization's business processes to ensure our warfighters receive decision-quality information at the right time and right place.

1.4 WORKGROUP MANAGEMENT DEFINED

As defined in AFI 33-115V1, *Network Management*, workgroup managers normally support a functional community (e.g., work centers, flights, squadrons, or organizations) and are the first line of help customers contact to resolve problems. The workgroup managers will be an Air Force specialty code (AFSC) 3A0X1 (Information Manager), if one is assigned. Workgroup managers are usually not assigned to the Network Control Center (NCC), though are logically an extension of the NCC Help Desk (HD) team. Workgroup managers take direction from the Functional System Administrator (FSA) and NCC. NCC direction takes precedence over FSA direction.

As a workgroup manager you will gain and cultivate a developed knowledge of hardware, software, and communications principles, and install, configure, and operate client/server devices. You will resolve the day-to-day administrative and technical system problems users experience. Contact your FSA or HD if you cannot resolve a customer's problem. This is essentially what we refer to as maintaining the "first 400 feet" of the network.



Figure 1-2. Network Crew Positions.

A workgroup manager is also a valuable member of the network crew force charged with maintaining the Air Force network with the same rigor and discipline as a weapons system. The workgroup manager crew position is 1 of 11 network crew positions (Figure 1-2).

1.5 WM ROLES AND RESPONSIBILITIES

WMs responsibilities are defined in AFI 33-115V1, *Network Management*, but are summarized as follows:

- Performs unit software management (inventories, remove unauthorized software)
- Performs configuration (workstations, printer servers, software, operating systems)
- Processes systems requirements (coordinates/validates user requirements)
- Provides software assistance (inquiries, e-mail group maintenance, dial-up networking)
- Manages individual user accounts (adds/removes mail and domain users)
- Manages organization web pages (creates, maintains, updates web pages)
- Manages system security (software patches, accreditation assistance)
- Manages disk (formats/partitions hard disk, optimize storage)
- Manages file system (client, unit-level file system, shard drive space)
- Performs fault isolation and correction (perform corrections, open/tracks trouble tickets)
- Performs unit-level computer system maintenance (computer and printer maintenance)
- Completes work center WM position certification (completes certification requirements)
- Performs unit computer hardware management (receives/inventories hardware and software, turn-in excess hardware and software)

- Performs Functional Area Records Management (prepares, reviews, maintains file plans; provides interim e-records procedures)

Had you been asked to compile this summary of responsibilities before you reviewed the list, you probably would have constructed a similar inventory of a workgroup manager's roles and responsibilities. But, how many of you would have written down a workgroup manager's records management responsibility?

Sometimes we may think records "is someone else's job," but as a workgroup manager, and certainly as an information manager, this is your job! You should be leading the charge, in concert with your Base Records Manager, to help your workgroup users manage their electronic records. Remember, not only do you need to be technically competent but you also need to couple your information technology know-how with your information management background to improve your unit's processes.

1.6 OVERSIGHT OF INFORMATION OPERATIONS

As the providers of front-line computer support to end users, workgroup managers often find themselves installing peripheral devices or troubleshooting problems on a user's computer. If in the course of authorized duties any type of unauthorized "event" is detected, (e.g., evidence a user is visiting unauthorized web sites, down-loading inappropriate material, etc.,) the workgroup manager should stop what they are doing and notify their supervisor. The supervisor will in turn, notify the unit commander, who may direct the workgroup manager to secure the computer. After reporting the incident, the workgroup manager may continue with their administrative duties.

The decision to proceed further with the information is the unit commanders. The unit commander may choose to consult with the base legal and the wing commander on the proper course of action to pursue. If appropriate, the wing commander will issue the necessary search authorization for access to the data stored on the media.

Unit commanders do not have the authority to direct the monitoring of specific individual's electronic communications--this may constitute an illegal wiretap.

Additionally, contracted network professionals may not direct or supervise any federal employee (military or civilian). For example, a contractor working in the NCC may not direct a workgroup manager to check the cache file on an end user's computer because the contractor suspects the end user has been conducting unauthorized activities utilizing their computer. However, contractors may report any suspicious events through their chain of command.

Here are three common scenarios you may find yourself in.

Scenario 1: While monitoring the network to keep things running smoothly, you notice one user "hitting" a number of non-work related (e.g., pornography, stock market, auctions, etc.) sites. What should you do?

Course of Action: You need to note the information and then report it to your supervisor. They will, in turn, report it to the appropriate investigative authority or commander. Once you have reported the discovery, your responsibilities as to this issue are done until/unless you are tasked to assist the investigating authority in gathering the information.

A key element of the scenario is you are monitoring the network or system to keep things running smoothly. The following Department of Justice (DOJ) statement further details the line between authorized duties and a breach of privacy:

“If they are looking at content with a motive other than to make sure that the system is running smoothly or to protect the rights and property of the system owner, then they have stepped over the line and risk violating the wiretap statute. Even looking at logs when the person does not have the intent to operate or maintain the system, or to protect it, could be a problem (under the pen/trap statute 3121(b).” Richard Downing, DOJ

Scenario 2: Your commander wants you to start real-time monitoring of Airman Steele’s e-mail and Internet accounts because he thinks Airman Steele is wasting time. Can you legally do this?

Course of Action: No. Commander-directed monitoring of an individual’s e-mail and Internet accounts real-time constitutes interception of those materials. This is governed by federal law and requires a specific authorization based on information that a crime is being committed. Your base Judge Advocate General (JAG) and Office of Special Investigation (OSI) should be involved in this process from the very beginning.

Scenario 3: You work in a Field Operating Agency (FOA) that resides in a separate building on your base. Can your FOA commander direct the search and seizure of a desktop computer in your unit?

Course of Action: Your FOA commander may order the computer in your unit to be secured and deny the individual user access to it. Searching a desktop computer is different from searching a shared drive or a network system. Those searches can be done with the consent of the Designated Approval Authority. However, the search of a desktop/laptop computer and the office where the computer is located may require a search authorization. Ask the JAG.

Keep in mind you are not the Internet police. You can be held personally criminal liable (up to 5 years in prison and a \$5000 fine) for violations of the Electronic Communications Privacy Act (<http://cio.doe.gov/ucsp/PublicLaw/ECPA.HTM>), so don’t hesitate to contact your base legal office with any questions or clarifications.

1.7 ENTERPRISE INFORMATION MANAGEMENT (EIM)

As a workgroup manager you will help implement and sustain components covered under the Enterprise Information Management (EIM) umbrella. EIM is a combination of functions and business processes for leveraging information technology to provide cradle-to-grave information management techniques, accountability, and policies. It includes planning, manipulating, and controlling information across the Global Information Grid (<https://www.afca.scott.af.mil/globalgrid/>) throughout its life cycle to enhance aerospace operations. EIM’s primary objective is facilitating standardized, interoperable capabilities to deliver the right information, in the right form, at the right place, at the right time. Figure 1-3 illustrates the 6 major categories of information creation/management and their respective

components...components you will help install, troubleshoot, and sustain. Additional EIM information may be found on the Air Force Communications Agency's web site at <https://www.afca.scott.af.mil/>.

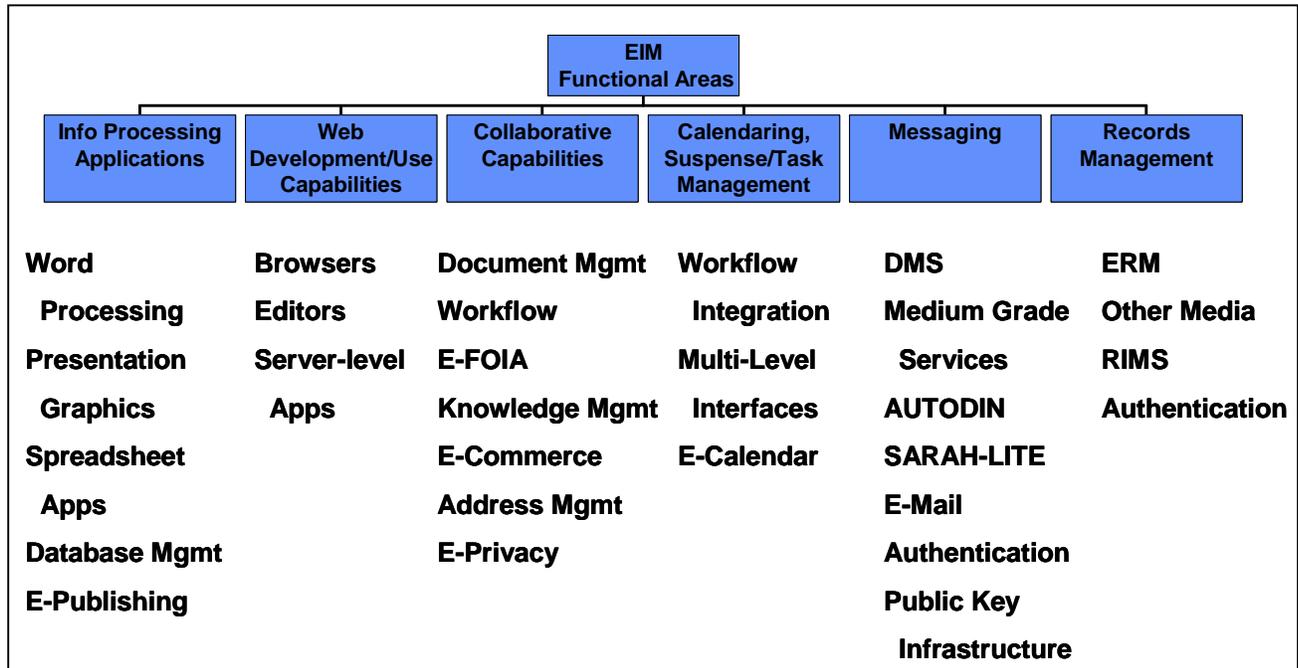


Figure 1-3. EIM Functional Areas

1.8 WM CERTIFICATION

Information managers must possess basic WM task and subject knowledge, and these core tasks are outlined in the 3A0X1 Career Field Education and Training Plan (CFETP) - Part II (Specialty Training Standard).

Workgroup managers are certified and appointed under AFI 33-115, Vol 1, *Network Management* and Vol 2, *Licensing Network Users and Certifying Network Professionals*. Workgroup managers are certified using the Position Certification for Workgroup Management, AF Job Qualification Standard (AFJQS) 3A0X1-225D, following MAJCOM and/or base guidance.

1.9 REVIEW QUESTIONS

1. Workgroup managers are a logical extension of what team?

2. Who do workgroup managers take direction from?

