UNITED STATES MARINE CORPS
MARINE CORPS BASE
PSC BOX 20004
CAMP LEJEUNE, NORTH CAROLINA 28542-0004

BO P5230.3B
BMSD
20 OCT 1997

BASE ORDER P5230.3B

From: Commanding General
To: Distribution List

Subj: INFORMATION SYSTEMS MANAGEMENT (ISM) PROCEDURES FOR MARINE CORPS BASE, CAMP LEJEUNE (SHORT TITLE: ISM PROCEDURES)

Ref: (a) MCO P5231.1C
(b) MCO 5271.1A
(c) OPNAVINST 5239.1A
(d) BO P2300.1C

Encl: (1) LOCATOR SHEET

1. Purpose. To detail the responsibilities for management of information systems in Marine Corps Base (MCB), Camp Lejeune organizations.

2. Cancellation. BO P5230.3A.

3. Background

a. Information systems are used extensively in virtually every Base support functional area. Information systems are productivity enhancing tools and continual planning, coordination, and technical review ensures the maximum productivity for information systems in each functional area.

b. Reference (a) provides the Marine Corps' philosophy, policy, and guidance on life cycle management of computer systems. Reference (b) is the issuing authority for the Information Resources Management technical publications which serve as overall technical guidance for Marine Corps management of information systems. Reference (c) is the guiding policy for information systems security in the Department of the Navy. These three publications form the framework within which local MCB, Camp Lejeune ISM policy must operate. Reference (d) is the Standing Operating Procedure for Communications-Electronics and defines the responsibilities of the Base Communications-Electronics Officer.

4. Information. In order to support MCB, Camp Lejeune organizations with information resources and to plan adequately for future growth, the Assistant Chief of Staff, Management Support

Department (MSD) provides assistance for requirements determination, acquisition, design, configuration, installation, maintenance, and upgrade/replacement of all information systems for MCB, Camp Lejeune organizations.

5. Action

a. All MCB, Camp Lejeune organizations will comply with the provisions of this Manual in developing information systems, requesting ISM support, obtaining repair and maintenance services, and purchasing equipment, software, and peripheral devices, and appointing Information Systems Coordinators (ISCs).

b. This Manual sets forth the proper procedures and the prohibited practices for access to and use of Marine Corps computer systems. Unauthorized or prohibited usage, criminal activity, or violations of security procedures by military or civilian personnel may subject them to criminal prosecution or to administrative discipline.

6. Summary of Revision. This revision contains a substantial number of changes and should be completely reviewed.

7. Reserve Applicability. This Manual is applicable to the Marine Corps Reserve.

8. Certification. Reviewed and approved this date.

B. A. GOMBAR
Chief of Staff

DISTRIBUTION: A less Cat IV
plus BMSD (10)

LOCATOR SHEET

Subj: INFORMATION SYSTEMS MANAGEMENT (ISM) PROCEDURES FOR MARINE CORPS BASE, CAMP LEJEUNE (SHORT TITLE: ISM PROCEDURES)

Location: _____

(Indicate the location(s) of the copy(ies) of this Manual.)

ISM PROCEDURES

RECORD OF CHANGES

Log completed change action as indicated

Change Number	Date of Change	Date Entered	Signature of Person Incorporated Change

ISM PROCEDURES

CONTENTS

CHAPTER

1	DEFINITIONS
2	ORGANIZATION AND RESPONSIBILITIES
3	INFORMATION SYSTEMS SECURITY
4	CUSTOMER SUPPORT
5	TRAINING
6	ACQUISITION, INSTALLATION, ACCOUNTABILITY, AND DISPOSAL OF INFORMATION RESOURCES
7	ELECTRONIC MAIL POLICY
8	INTERNET ACCESS POLICY

APPENDIX

A	INTERNET ACCESS AGREEMENT

CHAPTER 1

DEFINITIONS

	PARAGRAPH	PAGE
ABBREVIATED SYSTEM DECISION PAPER (ASDP)	1001	1-3
COMPUTER SYSTEMS SECURITY OFFICER (CSSO)	1002	1-3
DEFENSE MEGA-CENTER (DMC) DETACHMENT	1003	1-3
INFORMATION RESOURCES MANAGEMENT (IRM)	1004	1-3
INFORMATION SYSTEMS AND RESOURCES	1005	1-3
INFORMATION SYSTEMS COORDINATOR (ISC)	1006	1-3
LIFE CYCLE MANAGEMENT (LCM)	1007	1-3
LOCAL AREA NETWORK (LAN) ADMINISTRATOR	1008	1-4
MANAGEMENT SUPPORT DEPARTMENT	1009	1-4
SECURITY POINT OF CONTACT (SPOC)	1010	1-4
TERMINAL AREA SECURITY OFFICER (TASO)	1011	1-4

CHAPTER 1

DEFINITION OF TERMS

1001. ABBREVIATED SYSTEM DECISION PAPER (ASDP). A document that defines the requirement for purchase of information systems equipment, software, and training. The ASDP is used to document the requirement for information system development projects of less than $1M and for Federal Information Processing (FIP) resource acquisitions up to $50M.

1002. COMPUTER SYSTEMS SECURITY OFFICER (CSSO). The Head, Information Systems Management Division, Management Support Department, acting as the Computer Systems Security Officer (CSSO) for the Base, maintains and implements the Base Information Security Plan, and is responsible for announced and unannounced security reviews of Base computer systems.

1003. DEFENSE MEGA-CENTER (DMC) DETACHMENT. The DoD information processing organization, based around a mainframe computer, which provides local output support (print, microfiche, tape), performs regional security administration, schedules local production jobs, and provides production analysis and mainframe connectivity support to MCB, Camp Lejeune. This installation is operated by the Defense Information Systems Agency (DISA).

1004. INFORMATION RESOURCES MANAGEMENT (IRM). The planning, budgeting, organizing, directing, training, promoting, controlling, and management of activities associated with the collection, creation, use and dissemination of information and related resources.

1005. INFORMATION SYSTEMS AND RESOURCES. A combination of information, computer, and telecommunications resources, and other information technology and personnel resources which collect, record, process, store, communicate, retrieve, and display information. Any resource which supplies necessary support for an information system project; for development of an information system; or for operation of an information system. These resources may include personnel, equipment, software, facilities, funding, and contractual support for system definition, design, development, deployment, and operation.

1006. INFORMATION SYSTEMS COORDINATOR (ISC). [Formerly known as Information Systems Management Representative (ISMR)]. The official point of contact for development, maintenance, and technical support of information systems within a MCB organization.

1007. LIFE CYCLE MANAGEMENT (LCM). A management approach for acquiring and using information system resources in a cost-effective manner throughout the entire life of an information system.

1008. LOCAL AREA NETWORK (LAN) ADMINISTRATOR. The designated official within an organization who is responsible for maintaining and monitoring access to the organizational local area network (LAN) and the Base Wide Area Network, to include basic network maintenance functions, issuance of user identification and passwords, and related duties. This function is usually performed by the ISC.

1009. MANAGEMENT SUPPORT DEPARTMENT. The MCB Department which has responsibility for communications and information systems and which provides communications/ information systems infrastructure support to tenant commands within the Camp Lejeune/New River complex. MCB equivalent to the G-6.

1010. SECURITY POINT OF CONTACT (SPOC). The designated individual within each organization who is responsible for implementation of security procedures for that organization's information systems.

1011. TERMINAL AREA SECURITY OFFICER (TASO). The designated official within an organization who is responsible for ensuring the organization's compliance with security operating procedures, maintaining mainframe user access identification codes, creating security profiles for access to mainframe systems, assisting users in gaining access to computer applications, and generally monitoring data security within an organization. This function is usually performed by the ISC.

CHAPTER 2

ORGANIZATION AND RESPONSIBILITIES

	PARAGRAPH	PAGE
ASSISTANT CHIEF OF STAFF, MANAGEMENT SUPPORT	2001	2-3
INFORMATION RESOURCES MANAGEMENT AND PLANS DIVISION	2002	2-3
INFORMATION SYSTEMS MANAGEMENT DIVISION	2003	2-3
COMMUNICATIONS-ELECTRONICS DIVISION	2004	2-4
COMMANDING OFFICERS/DEPARTMENT HEADS	2005	2-4
DIRECTOR, DEFENSE MEGA-CENTER (DMC) DETACHMENT	2006	2-5
INFORMATION SYSTEMS COORDINATOR	2007	2-5

CHAPTER 2

ORGANIZATION AND RESPONSIBILITIES

2001. ASSISTANT CHIEF OF STAFF, MANAGEMENT SUPPORT. At MCB, Camp Lejeune the information resources are managed by the Commanding General. Directly responsible to him is the Assistant Chief of Staff, Management Support, who has staff cognizance over telecommunications and information systems. In order to gain maximum advantage from the technological merging of telecommunications and information systems, the Management Support Department (MSD) has been organized to unite all the resources of both disciplines so all customer needs in the areas of information systems, telecommunications, networking, and related issues can be met in the most effective manner. Included in the Management Support Department organization are the Communications/Electronics Division, which oversees telecommunications systems and facilities throughout the Camp Lejeune/New River complex; the Information Systems Management Division, which provides support for stand-alone and networked computer system applications, and the Information Resources Management and Plans Division, which supports information resources master planning and the implementation of technological improvement projects and initiatives.

2002. INFORMATION RESOURCES MANAGEMENT AND PLANS DIVISION. The responsibilities of the Information Resources Management and Plans Division are as follows:

1. Provide mid-range and long-range planning support for information systems for MCB, Camp Lejeune and the development and implementation of technology improvement projects and initiatives.

2. Support the Communications/Information Systems Working Group (CISWG), which develops and maintains the Base's strategic master plan for communications and information systems.

3. Provide technical assistance to committees and working groups dealing with telecommunications and information systems planning, to include research and assistance on special topics relating to future trends and technologies in communications/information systems.

4. Provide support for special technology projects, especially those involving other Base organizations and external agencies and provide liaison and coordination functions regarding information technology matters to other Base organizations, tenant organizations, and external agencies.

2003. INFORMATION SYSTEMS MANAGEMENT DIVISION. The responsibilities of the Information Systems Management Division, involve the provision of analytical support to Base organizations in determining requirements for information systems; designing and developing, and installing information systems; reviewing the use of those systems to determine their effectiveness and degree of utilization, as a part

of life cycle management; providing an Information Center to support all MCB computer users; and conducting training to support MCB computer users. The ISMD assists the Contracting Officer in systems procurement by providing procurement data, including prices and sources of supply, for information systems equipment and software. The ISMD coordinates with the Director, DMC Detachment where interface with Marine Corps/DoD-wide systems is required; acts as a focal point for coordinating local information systems management within Base organizations; provides support and required periodic training to ISCs; recommends the approval for purchase of information systems under the limit set by the local Delegation of Procurement Authority for information systems, including modifications and enhancements; maintains and manages a capital investment fund for the acquisition of information systems; and acts as the official point of contact for information systems maintenance and repair. The Information Systems Management Division manages the Base Wide Area Network (WAN).

2004. COMMUNICATIONS-ELECTRONICS DIVISION. The Communications-Electronics Division coordinates communications support to include radio operations, message traffic processing, telephone service, public address systems, and electronic maintenance services to Base and tenant commands located at Camp Lejeune. The Division is also responsible for programming, installing, and maintaining all Outside Telephone Cable Plant, internal building wiring, telephone switches, and telephone instruments. The Division maintains and operates a telephone switchboard, Defense Switch Network access, and commercial off-base access. In addition, the Division is responsible for liaison with communication agencies of other commands, services, and agencies. The Division coordinates the procurements and maintenance of all commercial communications equipment and associated cryptographic operations, frequency management, electronic countermeasures and communication security. The Division also coordinates the use of the Military Affiliate Radio System, provides technical advice and assistance and operational control of stationary citizens' band and amateur radio operations at Camp Lejeune under the purview of the Federal Communications Commission, and coordinates the communications efforts of this Command with the Defense Information Service Agency (DISA).

2005. COMMANDING OFFICERS/DEPARTMENT HEADS. As managers of information systems, it is the responsibility of commanding officers and department heads to:

1. Appoint, in writing, an Information Systems Coordinator (ISC) (formerly known as Information Systems Management Representative (ISMR)) for the organization or department to act as point of contact for information systems and for management of maintenance and repair on microcomputers and peripheral equipment. It is preferable that the ISC have basic knowledge of, and interest in, computer systems and should have an understanding of the operations and functions of the organization.

2. Ensure that ISCs and all personnel involved with information system operation attend the periodic training available from the Management Support Department in principles of system operation and system software.

3. Submit all requests for automated system support, including software and peripherals which are not part of equipment repair, via the ISC, to ISMD for study, requirement documentation, review, validation, and/or submission to higher authority in the event the funding threshold is exceeded. Submit all requests for networking of microcomputer systems, either planned or already in place, to ISMD for review, approval, and technical assistance.

4. Identify funding requirements for acquisition and maintenance of software and hardware.

5. Comply with the provisions of OPNAVINST 5239.1_, IRM Publications in the 5239 series, and Chapter 2 of this Manual in matters involving information systems to include the appointment of a responsible individual to oversee security for any and all information systems present in the organization or department.

6. Ensure that only legal copies of legally-acquired standard software are installed on personal computers and network servers within his/her organization.

7. Ensure that the ISMD Administration group is resident on all Admin Lists for all groups, including Server-Name@SERVERS.

2006. DIRECTOR, DEFENSE MEGA-CENTER (DMC) DETACHMENT. The DMC Detachment is the DoD mainframe-based computer support organization which provides local mainframe computer support and production processing support to MCB, Camp Lejeune. The ISMD will:

1. Coordinate with the DMC Detachment on all matters relating to information systems for MCB, Camp Lejeune, where interface is required between local users of automated systems and Marine Corps/DoD-wide systems resident on mainframe computers controlled or accessed by DISA, through the DISA Mega-Center at St. Louis, Missouri.

2. Provide technical points of contact for the DMC Detachment on matters involving access to Marine Corps Data Network/Defense Data Network, uploading/downloading of DMC Detachment-maintained files, and required modifications to Marine Corps/DoD-wide systems.

3. Coordinate with DMC Detachment on all matters relating to local area networks of microcomputers for MCB, Camp Lejeune, where interface with DISA assets are required.

4. Coordinate with the DMC Detachment HelpDesk for mainframe-computer-related trouble calls.

2007. INFORMATION SYSTEMS COORDINATOR (ISC). The Information System Coordinator (ISC), is the point of contact for development, maintenance, and technical support of information systems within his/her organization. The ISC will receive training from the Information Systems Management Division and will be assisted in his/her duties by an ISC Handbook provided by the ISMD. ISCs should refer to the ISC Handbook for detailed information about their responsibilities. ISC responsibilities are generally as follows:

1. Become familiar with basic principles of information systems operation and gain an understanding of the applicability of information systems to operations within his/her organization.

2. Assist in the development of abbreviated system decision papers for procurement of information systems within the organization/department/division.

3. Ensure compliance with system acquisition procedures noted above and contained in Chapter 6 of this Manual.

4. Attend all applicable technical training courses provided by ISMD and schedule applicable personnel within the organization/department for this training as required. Ensure all personnel involved with information systems have received training and are in possession of all manuals and written procedures for their system(s).

5. Screen all information systems project requests to ensure the requests are properly prepared and all required preliminary actions have been accomplished before recommending projects to their commanding officer or department head for approval.

6. Provide continual liaison with ISMD personnel during systems development within their organizations/departments.

7. Authorize creation, change, deletion, or access to data elements maintained in data bases/files for functional areas under their cognizance.

8. Ensure proper data and program backup procedures are being followed and ensure data is properly physically secured.

9. Coordinate information systems maintenance and repair requirements with ISMD in all cases except for those items of equipment which interface with the mainframe computer, such as remote terminals and printers.

10. Make recommendations (with the assistance of ISMD) for hardware or software items which will be added to existing information systems. Maintain inventory of computer equipment and software and provide reports to ISMD of changes to inventory as new items are received.

11. If appointed by the commanding officer/department head, may act as the Security Point of Contact (SPOC) and as Terminal Area Security Officer (TASO) for his/her organization. See paragraphs 3002 and 3003 of this Manual for more information.

12. If appointed by the commanding officer/department head, may act as Local Area Network (LAN) Administrator for the organization, maintaining and monitoring access to the organizational LAN and the Base Wide Area Network (WAN) to include password control and other related duties.

13. If appointed by the commanding officer/department head, may act as point of contact for Commanding General's Inspection Program reviews within the organization as related to information systems management.

14. Depending on the capability of the ISC, may perform preliminary system troubleshooting to determine if a problem is hardware or software related and the best course of action to correct the problem. Contact the Help Desk for assistance whenever necessary.

15. Ensure that the ISMD Administration group is resident on all group Admin Lists, including Server-Name@SERVERS.

CHAPTER 3

INFORMATION SYSTEMS SECURITY

	PARAGRAPH	PAGE
GENERAL	3001	3-3
RESPONSIBILITIES	3002	3-3
MAINFRAME ACCESS SECURITY	3003	3-4
PERSONAL COMPUTER/LOCAL AREA NETWORK SECURITY	3004	3-5

CHAPTER 3

INFORMATION SYSTEMS SECURITY

3001. GENERAL. The growing dependence on computer systems for productivity and efficiency in the work place, have brought new requirements for safeguarding sensitive information and equipment. Accordingly, this Chapter identifies responsibilities and procedures for mainframe, workstation, microcomputer and LAN security.

3002. RESPONSIBILITIES

1. Commanding Officers/Department Heads

a. Commanding officers/department heads will ensure equipment and data under their control is secured subject to the provisions of OPNAVINST 5239.1_ and this Manual, to include prevention of unauthorized access and protection against environmental hazard or damage. Commanding officers/department heads will appoint a Security Point of Contact (SPOC) for information systems under their control and furnish the name and organizational address of the SPOC to the Information Systems Management Division, Management Support Department.

b. Commanding officers/department heads will ensure information system(s) and all related equipment under their control is/are uniquely identified for purposes of theft deterrence; will take action to prevent the illegal copying of software and/or the violation of copy protection and copyrights by any information system user under their authority; will take action to prevent the illegal use of game software on government-owned information systems equipment (personal computers, terminals, workstations, etc.); will ensure the current version of anti-viral software is installed on all PCs in their organization; and will ensure the current warning message against unauthorized access is loaded on all microcomputers in their organization. Individuals who misuse or violate security requirements for computer hardware and software will be subject to disciplinary action.

2. Security Point of Contact. The Security Point of Contact (SPOC) for each information system will be responsible for implementation of security procedures appropriate to the system, and will act as focal point for all security information regarding his/her system(s). The SPOC will be contacted in case of any security violation involving the information system. The SPOC will be responsible for assignment and maintenance of passwords for information systems within his/her organization. Detailed instructions for performance of this function can be obtained from the Security Section, Defense Mega-Center Detachment for mainframe-based information systems; and the Head, Information Systems Management Division for microcomputer-based systems and local area networks.

3. Head, Information Systems Management Division. The Head, Information Systems Management Division, Management Support Department, acts as the Computer Systems Security Officer (CSSO) for all information systems supporting MCB activities, and will prepare, maintain, and implement the Base Information Systems Security Plan. The CSSO in coordination with the Office of the Base Inspector will conduct formal,

announced, and informal, unannounced security reviews of all Base microcomputer systems to assess the compliance of Base activities with applicable regulations, to report to higher headquarters as required, and to recommend remedial actions and measures where necessary. The CSSO will conduct periodic training (at least once annually) in security measures relating to microcomputer systems for Information Systems Coordinators, Security Points of Contact, and other interested parties.

3003. MAINFRAME ACCESS SECURITY

1. Terminal Area Security Officer (TASO) Information

a. Commanding officers/department heads are responsible for appointing Terminal Area Security Officers (TASOs) for their organizations. TASOs are responsible for ensuring security regulations are being followed regarding access to mainframe computer systems.

b. The Security Section, ISMD is responsible for training Terminal Area Security Officers (TASOs) and for issuance of Central Security Control Accessor Identification Numbers (SCAs)(ACIDs). The Security Section will establish inspection programs to ensure compliance with security guidelines. The Security Section works with the TASOs to ensure proper department level security is established for mainframe-based computer systems, in accordance with published directives. The Security Section may be contacted regarding specific regulations and procedures.

2. Protection of Mainframe Data Bases

a. Major Base Organizations and Data Base Security. Individual organizations have responsibility for the contents of mainframe-based automated files relating to their specific area of operation, and control access to those files. For example, AC/S Manpower is responsible for automated files of manpower/personnel data. AC/S Logistics is responsible for DSSC/Base Property/Base Contracting Automated System/logistics and supply related data. Department heads should be contacted if access to files under their control is required and may grant access to users when requested by the TASOs. The Security Section does not have the authority to grant any user access to data owned by Base organizations.

b. Requesting Access. Users request access to applications through their TASO. The TASO ensures the proper user profile is registered with the mainframe computer system and that the requested access is needed for the user's job performance. The TASO then forwards the request to the appropriate user organization. The following is the minimum information required for all requests:

(1) Name of site(s) where access is requested.

(2) Name of application library and/or datasets to be accessed, if known.

(3) User's name, grade, billet.

(4) Short justification explaining the need for the access.

(5) Point of Contact.

c. Accessor Identification (ACID) Accountability. Users will be identified with a six character code indicating their organizational affiliation. ACIDs are administered and assigned by TASOs. Additional details for assigning ACIDs may be obtained from the Security Section, DMC Detachment or your organization's TASO.

d. Password Control. The passwords associated with user ACIDs authenticate that the person using the ACID is authorized to use it. Users must protect their password from disclosure and to immediately change the password should it be compromised. User passwords expire every 90 days. Administrator ACIDs expire every 30 days. Information regarding fraudulent use or disclosure of passwords may be found in IRM Publication 5239-06, Data Access Security.

3. Classified Processing. All classified processing will be handled in accordance with BO P5510.6_ and BO P5511.1_. All equipment will have the appropriate security classification markings clearly displayed. Procedures for handling classified information are available from your TASO or from the Security Section, DMC Detachment.

3004. PERSONAL COMPUTER/LOCAL AREA NETWORK SECURITY

1. Physical Security

a. Overview. Personal computers (PCs) and local area network (LAN) equipment must be protected against theft, destruction, and misuse which includes unauthorized use, removal from the workplace, and relocation without proper approval. Supervisory personnel are responsible for control and usage of PCs and LAN equipment. Physical security responsibilities include ensuring the equipment is used in an environment which will not result in physical damage or deterioration resulting from adverse environmental conditions.

b. Environment for PC/LAN Equipment. Where feasible, equipment will not be located in high traffic areas or near outside doorways. It should be located in a space that can be locked or has limited access. Eating, drinking, or smoking should not be allowed in the immediate vicinity of any computer equipment. All information systems equipment will be plugged into surge protectors that have been authorized by a Fire Inspector. Equipment used for processing classified information will be used in a controlled space in accordance with BO P5511.1_.

c. Contingency Planning for Personal Computers and Local Area Networks

(1) Natural Disasters. There are two major threats caused by natural disasters that affect information systems equipment and data stored on magnetic media, namely, power outages/surges and water damage. The following measures should be taken to minimize the damage caused by storms, brownouts, and equipment failures:

(a) Use surge protectors.

(b) Schedule frequent backups of diskettes and hard disk drives.

(c) Save documents being worked on frequently.

(d) Locate equipment away from windows.

(e) Elevate equipment to prevent damage due to standing water.

(f) Use plastic bags to cover equipment, preventing water damage.

(2) Troubleshooting Coordination. In the event that any organization aboard MCB Camp Lejeune experiences network problems of any kind, all troubleshooting will be coordinated with ISMD. No activity is authorized to contact Banyan World Wide Support (WWS) at Quantico directly. ISMD will be responsible for escalating any problem to WWS and tracking to successful resolution.

d. Hardware Inventories. Individual units are responsible for maintaining an inventory of all hardware, especially of keyboards, CPU's, and monitors. Refer to Chapter 6 of this Manual.

2. Software Security. Security also involves the responsibilities incurred by users when they acquire software. Acquisition of software involves the execution of licensing agreements which provide for harsh penalties if the conditions of use are violated. This is extremely critical since software can easily be copied and is quite portable.

a. Functional users of microcomputer systems should make backup copies of all original commercial software diskettes if they are not copy protected, and should not use the original diskettes for daily processing. Backup copies of commercial software are to be used only on the machine for which they were originally made. Software should be stored on the hard disk whenever possible, and the original diskettes kept as additional backup. Users should use original diskettes only to make additional backups or working copies as required. Original diskettes should be kept in a physically safe and environmentally controlled location with a locked cabinet or safe being preferable. If original diskettes become damaged, considerable processing time (4 to 12 weeks) may be lost awaiting replacement. Diskettes should never be stored or allowed to rest near any magnetic device, including telephones.

b. Read all licensing agreements carefully. Consent to the terms of the agreement is presumed when software is used. Software is not actually owned; only the right to use it on a specific machine has been purchased. It is permissible to make backup copies as governed by instructions in individual software manuals; however, it is illegal to copy software for personal use or to copy software for a machine other than that for which it was purchased. There are no exceptions. If an individual in the organization wants a copy to "take his work home," he must purchase his own licensed copy of the software. Sharing software with other Base units or using unlicensed software is also illegal and prohibited. Do not confuse

copy protection with copyrights. If a software package is not copy-protected, it still may not be copied aside from the initial backup copies discussed in 2a above, since that action violates copyright law. It goes without saying that utilization of programs to strip copy protection from original software is also illegal and fraudulent.

c. Manuals and software diskettes are easily stolen or misplaced and these items should be carefully controlled. "Loaning out" manuals and disks has proven to be the most common cause of loss. It is often impossible to get another copy of a lost manual unless you purchase a second copy of the software. Users must protect the manuals and software diskettes as carefully as they protect the machine. Conversely, the manuals should be readily available for equipment users in the course of their daily work. The effectiveness of a system is often determined by the availability of manuals and documentation for hardware and software. While these should be secured when not in use, they should be readily available during the work day for easy reference by the microcomputer user.

d. To be considered legal, the user must have the original diskettes and manual(s); or the original diskettes when no manual is provided by the company; or a Certificate of License in lieu of original software diskettes as in the case of network node software, or the Base or the Marine Corps must have a site license for the software. Some software loaded to PCs is written by the Marine Corps or other government agency for use on government PCs; this software is considered legal, even though original diskettes and/or manuals are not provided. Security procedures must be followed when users acquire software. Acquisition of software will be accomplished in accordance with Chapter 6 of this Manual. Acquisition of software involves the execution of licensing agreements which provide for harsh penalties if the conditions of use are violated. This is extremely critical since software can easily be copied and is quite portable. ISCs will maintain accurate inventories of all software purchased for government use (refer to Chapter 6, "Acquisition, Installation, Accountability, and Disposal of Information Resources"). All illegal software will be deleted once detected. Periodic inspections will be conducted to ensure no illegal software is used on government-owned computers.

e. Commercial Software Copyrights. The Marine Corps honors all copyrights. Read all licensing agreements carefully. Consent to the terms of the agreement is presumed when software is used. Software is purchased to be used on specific machines. It is illegal to copy software for personal use. There are no exceptions. Individuals who want to "take their work home," must have their own licensed copy of the software. Sharing software with other Base units or using unlicensed software is strictly prohibited. Users are allowed to make a backup copy of all licensed software. The original diskettes should be kept in a locked, controlled area. ISCs will ensure all authorized backup copies are properly secured and controlled. Manuals are used to confirm the legal purchase of software. These manuals will not be loaned to other users or units.

f. Auditing Software. The Information Systems Management Division will install auditing software on all MCB servers. This software will allow the ISMD specialists and the organization's ISC to monitor all PCs for illegal/unauthorized software. This auditing software is mandatory and commanders and department heads will conduct periodic audits in accordance with procedures provided by ISMD.

g. Shareware/Freeware Use. Freeware or shareware is not authorized unless it comes from a U.S. Government sanctioned bulletin board and has been tested for the presence of a virus before use. Any software downloaded from a bulletin board must be downloaded to a diskette and NOT to the hard drive. Shareware paid for by an individual is considered privately owned and is not authorized for use on government-owned computers. Freeware (software which does not require any kind of registration or fee for individual use) may still require a license before it can be used by government or commercial organizations.

h. Demonstration Software. Software manufacturers sometimes provide individuals or organizations software for use on a trial basis. Some demonstration software becomes useless after a certain date. Other software may remain functional, but vendors request the software to be returned if not purchased. The use and particularly the return of all demonstration software must be documented.

i. Server-based Software. Some software packages are bought to be loaded to server(s) on a local area network. This software usually has a limit to how many users can access the software simultaneously. The ISCs will be responsible to ensure the LAN is configured so as not to allow more than the number of users specified in the software license to access the software simultaneously.

j. Bundled Software. PCs purchased from vendors may come with specific software packages included. Any software that conflicts with established EUC standards (i.e., word processors, graphics packages, spread sheet packages, database packages, operating systems) should be deleted from all systems. If software diskettes were provided, report them as excess in accordance with paragraph 6005 which governs disposal of excess hardware/software. Any productivity software that does not conflict with an established standard, and is for local office use only, may be retained. Non-standard file formats will not be transmitted between organizations. The proper disk backups and manuals must be maintained as outlined above. All restrictions applicable to commercial software apply.

3. Virus Control Measures

a. General Information

(1) Microcomputer-based software is the source of a potentially serious problem commonly known as the "microcomputer virus." The "virus" is an unauthorized program that can clone itself rapidly and spread from one microcomputer disk to another and from one program to another. Viruses are normally designed by computer hackers attempting to invade a system, or disgruntled individuals who willfully desire to damage a system. The virus can damage files and directories, and can cause serious problems in local area networks by duplicating itself into other programs or into the network operating software. These programs can modify the functioning of the system so as to cause it to malfunction, crash, or destroy data. Viruses are most often encountered by users of shared software. The virus can spread by a number of means:

(a) A programmer creates an unauthorized program that can secretly bind itself to another program or to the operating system, and repetitively copy itself.

(b) The program may be copied to a floppy diskette or transmitted by information disseminated on an electronic bulletin board.

(c) The program may be automatically copied into pirated or illegally reproduced software, or utilities that strip copy protection off software diskettes. This most often occurs with pirated game software.

(d) Once resident in the computer, the program copies itself onto floppy diskettes or onto the computer's fixed disk.

(e) When data is transferred from one microcomputer to another, the problem program is also transferred.

(f) The program can be activated at a later time, according to instructions embedded in it, or at a specified date and time.

(2) The presence of microcomputer virus programs has been detected on microcomputers in several MCB organizations. To protect against the spread of these viruses, MCB microcomputer users are not authorized to download executable programs from electronic bulletin boards, and must not accept or use copied, pirated, or game software under any circumstances. All diskettes MUST be scanned using virus detection software prior to use, including commercial software purchased by the government.

(3) Viruses, in general, attack specific files and areas of microcomputers. The number one victim of a virus attack is the computer's memory or the boot sector of diskettes. Since the evolution of Local Area Networks, the threat of virus attacks has been reduced for some units. Those units that rely heavily on diskette use are at high risk of virus infections. All viruses that are memory resident, meaning they do not infect files, can only infect a computer when the computer is "booted" from an infected diskette, even if the "boot" was not successful. Accessing the diskette to transfer, read, or delete files can not load the virus into the computer's memory. Examples of these memory resident viruses are "Michelangelo" and "Stoned." Since booting from a diskette is rare, infection of microcomputers is limited. Infection of networks is rare since viruses do not attach to data files, which are the primary files transmitted through E-mail. With effective anti-viral software, use of only legal, validated software, frequent backups, and proper scanning procedures the threat of viruses can be eliminated.

b. Anti-Viral Software. Department heads/ISCs ensure all microcomputers in their department have current version of virus protection software. The anti-viral software must reside in the security directory on the C drive of all microcomputers, regardless if the computer is standalone, a laptop or connected to a LAN. Deleting anti-viral software will be considered a security violation and may constitute administrative action against the violator. The anti-viral software must also reside on one of the drives for all servers. If at all possible, a memory resident virus protection program will be used on all computers to avoid the spread of viruses. Such programs will lock up the computer if a virus is detected on a diskette that has been accessed.

c. Scanning Computers and Diskettes. All microcomputers, including Local Area Network servers, must be scanned immediately upon installation of anti-viral software and at least once a week thereafter. Users must scan all diskettes before use. If the diskette(s) has been scanned once and does not leave the immediate control of the user, the diskette(s) does not need to be re-scanned before use; however, if a user brings a diskette from home, it is considered to be out of the user's immediate control and must be scanned before use on a government computer. All diskettes and computers that are bought brand new, must also be scanned. It is a documented fact that some disgruntled employees have put malicious codes in brand new products. Never assume a product is virus free just because it has come straight from the factory; scan all diskettes and computers.

d. Game Software on Government Computers

(1) One of the most common carriers of viruses is game software. This is one reason why game software is strictly controlled on all government computers. The only authorized game software is Marine Corps versions of selected battle skills games that are used as part of a formal unit training program. (See ALMAR 025/97 for more information). Some legally purchased software comes with games to help users become comfortable using a mouse. Since many users continue to use these games after they have become proficient with their mouse, only computers in a formal training environment will be allowed to keep these games active. All other computers must disable these programs.

(2) Utilization of computers belonging to MCB, Camp Lejeune and/or the United States Marine Corps for playing unauthorized computer games, and the loading of such games on government-owned equipment, is expressly forbidden and is subject to penalties. Unauthorized game software discovered on Marine Corps equipment should be reported to the Information Systems Coordinator (ISC) and are subject to confiscation.

4. Local Area Network Password Control

a. Passwords are used to ensure only authorized users access the network. Users must protect their password from disclosure and immediately change the password should it be compromised. Careless use of network passwords may result in loss of access privileges, and users that negligently or purposely allow unauthorized access from their network workstation/computer may be subject to disciplinary action.

b. Local Area Network passwords are established with a 90-day expiration timeframe, for consistency with mainframe password requirements. This common standard for password expiration will provide for a smooth future transition from mainframe to client-server operations.

c. The Information Systems Coordinator/LAN Administrator is responsible for setting the proper expiration date for LAN passwords.

CHAPTER 4

CUSTOMER SUPPORT

	PARAGRAPH	PAGE
GENERAL	4001	4-3
HELPDESK FUNCTIONS	4002	4-3
TROUBLESHOOTING	4003	4-3

CHAPTER 4

CUSTOMER SUPPORT

4001. GENERAL. The key element in providing support for customers in the area of information systems is the ISMD HelpDesk. The HelpDesk is staffed with a variety of technical personnel versed in the various information systems specialty areas. The HelpDesk is manned Monday through Friday from 0630 until 1730. At other times calls will be handled by duty personnel who can contact responsible technical personnel to assist in problem resolution. The HelpDesk phone number is 451-1019.

4002. HELPDESK FUNCTIONS. The function of the HelpDesk is to provide an immediate response to user problems and requests for assistance. The goal of the HelpDesk is to assure the highest level of customer satisfaction and minimize customer downtime. Every effort will be made to solve the user's problem on the first call. Problems requiring a more detailed analysis will result in the generation of a trouble ticket. The trouble ticket is used to refer the problem to a technical specialist for action and to track progress of the problem cycle through to completion. The customer will be provided the ticket number to refer to when inquiring on status of an existing problem.

4003. TROUBLESHOOTING. First echelon troubleshooting is to be done by the user. The user should record any error messages and a description of the events leading up to the equipment or software failure. Any information that will assist in duplicating the error will aide in the problem resolution process. Problems that cannot be immediately diagnosed or resolved should be relayed to the organization's Information Systems Coordinator (ISC), who will in turn relay it to the HelpDesk if he/she is not able to resolve the problem locally. When an ISC calls into the HelpDesk, the first step is to determine the nature of the problem, i.e., PC-related, LAN/WAN, or mainframe application or security related. If the ISC is able to make this determination prior to calling the HelpDesk, solution of the problem can be greatly expedited. Once the nature of the problem has been identified, the HelpDesk technician can determine the best course of action to resolve the problem.

1. PC Trouble Calls. The organization's ISC, or designated alternate, will make the call to the HelpDesk after preliminary troubleshooting procedures have been accomplished. If a PC hardware problem has been identified a PC repair ticket will be generated. Marine Corps Base has a microcomputer maintenance contract with a commercial vendor to handle all PC and related equipment repairs. A technician will come on site to diagnose and correct the problem. ISCs should notify the HelpDesk if a PC is currently under a manufacturer's warranty. Warranty repairs are performed by the manufacturer's designated representative and are not covered under the Base contract until expiration of the warranty period. The following information must be provided to the HelpDesk when placing a call for a PC under the MCB microcomputer maintenance contract:

a. Unit and section where the equipment to be repaired is physically located.

b. Primary and secondary points of contact where the equipment is physically located.

c. Building and phone number where the equipment is physically located.

d. Manufacturer, model, and serial numbers of the equipment needing repair.

e. Definition of the problem.

2. LAN Trouble Calls. After preliminary troubleshooting by the ISC/LAN Administrator, a trouble call is placed to the HelpDesk. If the problem cannot be resolved immediately, a trouble ticket will be generated and referred to the appropriate ISMD technical specialist for action. In order to provide assistance on LAN, it is necessary that trouble calls have the ISMD Admin group resident on the group Admin Lists, including Server-Name@SERVERS.

a. Server/Hardware Problems. If the problem is determined to be a hardware failure it will be handled in the same manner as a PC repair problem.

b. Circuit Problems. If the problem is determined to be a circuit problem a repair call will be made to the Base Telephone Office for action.

c. Software Problems. If the problem is determined to be network operating system software or application program related, it will be referred to the appropriate computer specialist for action.

3. MFI 3270 Terminal/Controller Problems. Initial efforts to activate the line and terminal equipment will be performed by the HelpDesk. If necessary, a trouble ticket will be opened and transferred to the Network Control Section for action.

a. Circuit Problems. If the source of the problem is a telephone circuit, the Network Control Section will report the problem to the Base Telephone Office for action.

b. Terminal/Controller/Modem Problem. A Network Technician will be dispatched to the user's site for detailed diagnosis. If the terminal or controller has a physical hardware problem that cannot be fixed by the technician, a repair ticket will be generated with the commercial vendor responsible for network equipment maintenance.

4. Mainframe and Security Problems. Problems with mainframe applications at other Marine Corps activities will be coordinated with the host site's HelpDesk. Local problem determination will be handled by the HelpDesk or, if necessary, a trouble ticket will be generated and the problem referred to the appropriate programming specialist.

CHAPTER 5

TRAINING

	PARAGRAPH	PAGE
GENERAL	5001	5-3
LAN/WAN ADMINISTRATOR TRAINING	5002	5-3
PC SOFTWARE TRAINING	5003	5-3
SECURITY TRAINING	5004	5-3
NATURAL PROGRAMMING	5005	5-3
INFO-PAC TRAINING	5006	5-3

CHAPTER 5

TRAINING

5001. GENERAL. The ISMD is responsible for coordinating information systems related training for MCB organizations. Training is provided in a myriad of information systems disciplines including; PC-based software, LAN/WAN administration, PC and mainframe security, mainframe NATURAL programming, INFO-PAC support, and other special classes as required to support Marine Corps programs. Requests for course availability, schedules, and course locations, should be made to the ISMD Training Coordinator.

5002. LAN/WAN ADMINISTRATOR TRAINING. Base organizations are responsible for assigning a person as an Information Systems Coordinator (ISC) and ensuring their completion of the required ISC certification training which is provided by the ISMD. The ISC is the direct interface to the ISMD on all matters pertaining to PC and LAN/WAN issues, and generally acts as the LAN administrator for his/her organization. The ISMD has developed a ISC Certification Training Program, including training in LAN/WAN administration, to assist the ISCs in the accomplishment of their duties. ISCs will begin the Certification Training Program within 30 days of their assignment as an ISC.

5003. PC SOFTWARE TRAINING. The ISMD provides user training on all Marine Corps standard software. Classes are taught by a contracted instructor on a weekly basis from 0800 - 1600, Monday through Friday. ISCs or section supervisors should call the ISMD Training Coordinator to schedule class seats.

5004. SECURITY TRAINING. Terminal Area Security Officer (TASO) training is provided on an as required basis.

5005. NATURAL PROGRAMMING. A NATURAL programming course is provided on a quarterly basis for organizations having data reporting requirements on the mainframe. Contact the ISMD Training Coordinator for class schedules, and to reserve seating.

5006. INFO-PAC TRAINING. Training in INFO-PAC, which permits local control of printing from mainframe-based systems, is available as required. Point of contact for scheduling is the ISMD Training Coordinator.

CHAPTER 6

ACQUISITION, INSTALLATION, ACCOUNTABILITY, AND DISPOSAL OF INFORMATION RESOURCES

	PARAGRAPH	PAGE
ACQUISITION	6001	6-3
INSTALLATION	6002	6-5
ACCOUNTABILITY	6003	6-7
MAINTENANCE OF MICROCOMPUTER EQUIPMENT	6004	6-8
DISPOSAL	6005	6-9

CHAPTER 6

ACQUISITION, INSTALLATION, ACCOUNTABILITY, AND DISPOSAL OF INFORMATION RESOURCES

6001. ACQUISITION

1. Acquisition of information resources will be in accordance with established policies in reference (a).

a. Competitive information resource acquisitions less than $300K (noncompetitive less than $100K) will be managed locally without formal submission of an ASDP to the Marine Corps Systems Command (MARCORSYSCOM). A file of locally approved ASDPs will be maintained by the Information Systems Management Division (ISMD) for verification purposes and a copy will be forwarded to the Contracting Division. (See ISC Handbook for more information about ASDP preparation.)

b. Competitive information resource acquisitions greater than $300K (noncompetitive greater than $100K) require a Delegation of Procurement Authority (DPA) from MARCORSYSCOM. The Information Systems Management Division will forward the ASDP to MARCORSYSCOM for review and issuance of a DPA for acquisition.

c. The Assistant Chief of Staff, Comptroller will provide central funding to the Management Support Department (MSD) for information resource procurement. Commanding officers/department heads may request their funds be used for procurement when central funds are not available. The Base Resources Management Review Board will review requests for procurement of ADP resources with centrally managed funds and make recommendations to the Commanding General.

2. Responsibilities

a. Commanding Officers/Department Heads. Commanding officers/department heads will forward requests to procure ADP resources to the Management Support Department/Information Systems Management Division for command-wide coordination of ADP acquisitions; and will assist ISMD personnel in analysis of the requirement and preparation of the ASDP.

b. Assistant Chief of Staff, Management Support

(1) The AC/S, Management Support will coordinate the Information Resources Management program for Camp Lejeune and conduct analysis, review, and planning relative to all current and future information resources for Camp Lejeune. This includes preparation of budget information for acquisition of the hardware and software required to support MCB information systems. The AC/S Management Support will review all requests for acquisition of ADP resources for compliance with applicable system standards and specifications and ensure the required documentation (ASDP) for each procurement is prepared. The following Divisions in MSD will:

(2) Head, Information Systems Management Division

(a) Provide analytical support to commanding officers/department heads in the determination of their requirements for information resources.

(b) Provide procurement data, including source of supply and estimated costs to commanding officers/departments heads, Base Property Control and Contracting Division, as required. Act as technical consultant for all information resource procurement.

(c) Prepare final ASDPs with recommended configurations for certification by the Assistant Chief of Staff, Management Support. Ensure recommended acquisitions comply with Marine Corps approved standards.

(d) Establish procedures to ensure all information resource funded requisitions are countersigned by approved ISMD personnel prior to being forwarded for acquisition. The individual countersigning this requisition is certifying that it is in accordance with an approved ASDP, where applicable, and meets all other procurement requirements.

(e) Maintain the official file of ASDPs for audit purposes.

(f) Maintain a readily available complete set of IRM Technical Publications and Marine Corps Orders pertaining to information resources.

(g) Provide information requested by the Information Resources Management and Plans Division (IRMP) pertaining to information resource acquisitions, planning and budgeting.

(3) Head, Information Resources Management and Plans Division

(a) Act as the central point for base-wide information resources planning.

(b) Coordinate with ISMD for submission of the annual Mid-Range Information Systems Plan and other reports that may be required.

(c) Review all ASDPs.

(4) Head, Budget Division

(a) Provide funding guidance to IRMP and ISMD for information resource acquisitions.

(b) Coordinate submission of budget information to the Assistant Chief of Staff, Comptroller.

(c) Act as the Fund Administrator and maintain the information resources budget.

c. Assistant Chief of Staff, Logistics. The AC/S, Logistics will:

(1) Process requisitions using standard procurement procedures ensuring that they are countersigned by authorized ISMD personnel.

(2) Coordinate with ISMD computer specialists to ensure that information resources procured will meet required specifications.

(3) In cases of highly technical procurement, Contracting Division will ensure participation of ISMD personnel in evaluation of proposals and submissions.

(4) Contracting Division, in concert with ISMD personnel, will develop and maintain contracts in support of microcomputer maintenance. The Contracting Officer will designate ISMD personnel as the Contracting Officer's Representative (COR) for the purpose of ordering of maintenance and repair service required under contract for the surveillance, verification, and certification of required services.

(5) ISMD monitors the status of equipment requisitioned through MSD funds, and will provide feedback to functional users regarding estimated delivery dates.

d. Assistant Chief of Staff, Comptroller. Provide O&MMC funds, according to the local budget plan, to the Assistant Chief of Staff, Management Support for acquisitions and maintenance in support of the command-wide information resources program (except formal schools classrooms, which will be provided from training funds).

6002. INSTALLATION

1. General. The ISMD provides direct technical support to all MCB organizations for LAN/WAN and PC installation. Support is normally coordinated through the organization's ISC.

2. Equipment Setup. Installation and setup of a LAN and associated equipment is a joint effort of the ISMD, Base Telephone, and the receiving organization's ISC.

a. Upon completion of the system study for a new LAN, the ISC will assist in development of any necessary floor plans and requirements for LAN wiring and WAN circuits in conjunction with the ISMD. This input will be used to develop telephone service requests (TSRs) for necessary circuit installation. All circuit and wiring requirements, in the form of TSRs, will be submitted to Base Telephone for installation. Services include two- and four-wire data circuits, and wiring within buildings to support local area networks. Telephone service is requested on Form MCBCL 2305/28 (Rev 04-86). Base Order 2305.5 provides guidance for completion.

b. Identification of power requirements, climate control, structural modifications, and any other requirements impacting the installation of microcomputer equipment must be accomplished prior to the installation of the equipment. Requirements will be coordinated with AC/S Facilities and Base Maintenance personnel.

c. Installation and setup of LAN servers is the joint responsibility of the ISMD and the ISC. ISMD will configure and install the Network Operating System (NOS) on the server. Initial definition of LAN user-IDs, services, and software will be performed by the ISMD. ISMD will ensure that all circuits are operational and that the LAN is fully operational. The ISC will receive training in day-to-day LAN administration and system maintenance procedures. The ISC will be the primary POC in troubleshooting LAN problems. The ISMD will monitor server performance electronically, and accordingly will be resident on all group Admin Lists, to include Server-Name@SERVERS.

d. Installation of PCs and peripherals will be a joint effort between the ISC and ISMD. ISMD will provide initial technical assistance and ensure the ISC is instructed in the proper setup of all equipment.

e. Installation of LAN-based application software and PC-based software (including software upgrades) will be a joint effort between the ISC and the ISMD. Every effort will be made to make the ISC as self-sufficient as possible.

f. Mainframe Connection via NCR COMTEN Front End Processor (FEP). The Network Control Section of ISMD is responsible for planning and coordinating the installation and/or relocation of all terminal equipment and data circuits in support of MCB functions. After coordination between the requesting unit and ISMD, the Network Control Section will initiate and submit the proper TSR to the Base Telephone Office. Network services are obtained by submitting a formal request to ISMD via official correspondence, or to the Organizational Mailbox in accordance with Chapter 10 of this Manual. To prevent any unnecessary delay in processing your request, ensure it is properly endorsed and as complete as possible. Include the following information as applicable.

(1) Type of service requested.
(2) Building number and office space(s) involved.
(3) Type of equipment.
(4) Application access requested.
(5) Point of contact with phone number.

g. LAN/WAN Data Circuits. TSRs to support LAN/WAN installation and/or relocation are coordinated by the Customer Support Section of the ISMD. This includes requests for wiring of new LAN installations, LAN expansions, WAN circuits, and server dial-up circuits. Organizations should have their ISC contact their respective ISMD computer specialist for coordination of requirements, or submit requirements via official correspondence or E-mail to the Organizational Mailbox in accordance with Chapter 10 of this Manual. Requirements for LAN/WAN installs and/or modifications should include a floor plan indicating the building number(s), room number(s), and desired location of workstation(s), server(s), and wall jacks.

TSRs will be prepared by the ISMD specialists and forwarded to Base Telephone for action. All network wiring, both internal and external, will be coordinated and approved by Base Telephone and ISMD.

6003. ACCOUNTABILITY

1. Property Accounting Procedures. Base Property Control Division, Logistics Department is responsible for administration and accounting of all Plant Account/Minor Property at Marine Corps Base. When ADP equipment has been received by a Base organization, the organization's Responsible Officer will enter it on the organization's CMR. Each piece to the suite must be recorded with its own NSN (ex. monitor, PC, printer, keyboard) in accordance with current directives. This can be done with an Inventory and Miscellaneous Gain Transaction (D8B) document. All ADP equipment also will be loaded by the Responsible Officer into the DoD Automation Resources Management System (ARMS) for inventory accountability as well as redistribution management.

2. Physical Security of Information Resources. The Plant Account/Minor Property Responsible Officer, assigned in writing will provide physical security and accountability for all microcomputer equipment, software and hardware in his/her charge; signature authority for pickup of microcomputer equipment in the absence of the responsible officer; proper written approval for disposition; and a guarantee that microcomputer equipment/software is not traded/exchanged or otherwise disposed of without prior approval.

3. Inventory. Physical inventories will be conducted in accordance and in conjunction with the scheduled inventories for Plant Account and Minor Property as identified in MCO P10150.1, Garrison Property Policy Manual and BO 4400.17_. Logistics Manual. ISMD will receive a report of all microcomputer equipment/ software from the ISC for each responsible unit.

4. Validation of Purchase Authority. ISMD will submit a recommended equipment configuration as an enclosure to the ASDP. Once the ASDP has been approved and signed, the organization will be contacted by ISMD to pick up the ASDP. When the organizational representatives pick up the ASDPs they must bring the requisitions with them to be signed by designated ISMD personnel unless the purchase is to be made with an IMPAC card, in which case IMPAC card purchase procedures will be used. Contracting Division will not accept requisitions without this signature. Once the organization has received the completed ASDP and the signed requisitions, it will forward the signed funded requisitions, with a copy of the study, to Contracting Division for procurement action. If the funding for the equipment purchase is provided by the organization, the equipment will be delivered directly to them. If the equipment is purchased with MSD funds, the equipment will be delivered to MSD and then turned over to the organization.

5. Temporary Loans. Temporary loans of microcomputer equipment may be made on a very limited basis subject to availability of equipment.

6. Investigations. The Responsible Officer will initiate a request for investigation when property on accountable records has been lost, damaged, or otherwise rendered unserviceable for its intended use; and "Missing, Lost, Stolen,

Recovered Government Property" reporting for material gains/losses in accordance with BO 4400.5E, Chapters 6 and 8, respectively. A copy of the reports for missing, lost, excess and stolen microcomputer property will be forwarded to ISMD.

6004. MAINTENANCE OF MICROCOMPUTER EQUIPMENT

1. Procurement and installation of repair parts by individual Base organizations is not authorized. Repair of microcomputer equipment is covered under a Base-wide requirements contract, and will be arranged by ISMD.

2. The microcomputer maintenance contract Contracting Officer's Representative (COR), who is located in the ISMD, will monitor contractor performance in accordance with the contract. The COR shall advise the end-user to be attentive to the contractor's presence, to read the information written on work ticket by the contractor prior to signing for the repair, and to fill out complaint sheets and forward to the COR if the end user is not satisfied with the service. The COR will maintain contractor performance documentation in a permanent file.

3. Equipment Replacement. Although no one analysis formula can be established for determining when any particular item of equipment should be replaced, an evaluation of equipment condition, service life, age, obsolescence, and safety hazard in determining what equipment will be replaced. The following procedures will be utilized when determining replacement requirements:

a. CMR. The responsible property officer will receive a Consolidated Memorandum Record detailing the complete listing of property (including hardware and authorized software). The CMR will identify the item, unit cost and installation date.

b. Condition Codes. Upon receipt of the CMR listing, the responsible property officer will review and update the condition codes. Prior to turn-in, all microcomputer equipment will have a Limited Technical Inspection (LTI) completed and approved by ISMD. A copy of the LTI will be retained by ISMD. One copy of the updated CMR listing will be returned to the Base Property Control Division.

c. Obsolescence. It is realized that in many cases, it is more economical to replace equipment/software than to retain serviceable equipment which has not outlived normal service life. This is a result of improved equipment having been manufactured which usually reduces consumption of material or operation, consideration will be given to these items. In addition to the condition code, the word "obsolete" will be written after the item name. A statement will be made as to the reason for the equipment/software obsolescence.

d. Safety Factors. Equipment which is considered to be hazardous will be so indicated on the Plant Account listing. The Base Safety Manager should always be contacted in regard to equipment presenting safety hazards.

e. Service Life. Service life of equipment is the average useful life as established through statistics or estimated by qualified technical personnel. Upon receipt of the CMR listing, ISMD will determine the service life of equipment through use of various Marine Corps Orders and commercial catalogs.

f. All requests and procurement for replacement microcomputer accessory equipment must be accompanied by an ASDP, be approved by ISMD and procured through Management Support Department.

g. Replacement keyboards will not be added to the CMR, but will be provided by ISMD through a one for one exchange program.

h. The following statement must accompany all requests for consumable supplies:

"THIS REQUEST IS FOR OFFICIAL GOVERNMENT BUSINESS AND IS ESSENTIAL TO THE COMPLETION OF THE REQUESTING AGENCY'S MISSION. THE SOLUTION BEING IMPLEMENTED IS THE MOST EFFECTIVE AND COMPLIES WITH THE GOALS OF SECNAVINST 5231.1C. WHEN SIGNED BELOW, BY AUTHORIZED OFFICIALS, THIS STATEMENT CONSTITUTES LIFE CYCLE MANAGEMENT (LCM) APPROVAL."

REQUIREMENT VALIDATION	LCM APPROVAL
ORG, NAME AND TITLE	ORG, NAME AND TITLE

6005. DISPOSAL

1. Disposal Procedures Using the ARMS System. Excess serviceable, unserviceable, and obsolete microcomputer equipment will be disposed of as follows:

a. Each item will be listed separately on Standard Form 120 (report of Excess Personal Property) showing Serial Number, Make, Model, Unit Cost, and Condition Code and forwarded to the Base Information Systems Management Division (ISMD).

(1) Upon receipt of the request for turn-in, ISMD personnel will review and return the Standard Form 120 to the Responsible Officer (RO) having custody of the property.

(2) The responsible unit requesting turn-in will then enter each item into the Automation Resources Management Systems (ARMS) and await their Automation Release Date (ARD) letter from the Defense Automation Resources Information Center (DARIC).

b. The RO will list each item separately on DD Form 1348 (Request for Turn-In), showing plant account number (if applicable) and serial number.

c. All requests for turn-in, accompanied by a copy of the ARD letter from DARIC, will be forwarded by the RO to the Base Property Control Officer.

d. Upon receipt of the request for turn-in and the appropriate DARIC statement, the Base Property Control Officer will provide the RO having custody of the property with disposition instructions.

2. Acquisition and Utilization of Obsolescent Equipment. From time to time, obsolescent microcomputer equipment becomes available as Marine Corps activities migrate to newer technologies. This equipment can be advantageously used for interim relief of equipment requirements in the face of shrinking budgets.

However, an influx of older machines in any significant number poses a problem in the area of greatly increased microcomputer maintenance. Generally, equipment acquired in this manner is not covered by existing maintenance contracts, and must be visibly marked, internally and externally, as being ineligible for repair. Organizations must account for such equipment and not subject the Base to unwarranted repair calls on the equipment. Organizations contemplating the acquisition of excessed obsolescent equipment should consider the following:

a. A legitimate requirement for the equipment should be demonstrated and documented utilizing an ASDP, in the same manner as a requirement for new equipment, and as outlined above in Paragraph 6001.

b. Internal equipment assets should be redistributed, where possible, before going outside to other activities to obtain resources.

c. Any software acquired for or with obsolescent equipment must be legal and licensed, in accordance with Chapter 3 of this Manual.

d. Organizations receiving equipment must add it to their property account in accordance with guidelines given above in Paragraph 6003.

CHAPTER 7

ELECTRONIC MAIL POLICY

	PARAGRAPH	PAGE
GENERAL GUIDANCE	7001	7-3

CHAPTER 7

ELECTRONIC MAIL POLICY

7001. GENERAL GUIDANCE

1. The use of E-Mail as an alternate method to written communications for the purpose of exchanging individual, section, and organizational information as well as to facilitate day-to-day administrative activity is encouraged. However, improper use of E-Mail has far-reaching implications that directly impacts upon information control and information security. Therefore, E-mail in general must be used appropriately and official E-Mail must be managed under the Marine Corps records system in the same manner as typed Naval correspondence in order to prevent the loss of information.

2. E-Mail must not be used to circumvent proper staff coordination.

3. Per reference (b), E-Mail is restricted to official use only, as in the use of Government telephone and postal system. Should the answer to all of the following questions be "yes" when deciding whether E-Mail would be proper, then it would be appropriate to use E-Mail:

a. Is the message or information necessary in the performance of duties or of benefit to the health, welfare, or safety of others?

b. Is the contents of the message or information presented in a manner that will not embarrass an individual, this Command, or the United States Marine Corps?

c. Is the author willing to share the contents of the message or information with anyone else other than to whom addressed?

4. Reference (b) restricts the use of blanket wildcard E-mail addresses (e.g., *@*).

CHAPTER 8

INTERNET ACCESS POLICY

	PARAGRAPH	PAGE
BACKGROUND	8001	8-3
POLICY	8002	8-3
INTERNET E-MAIL	8003	8-4
ACCESS TO THE WORLD-WIDE WEB	8004	8-5
INTERNET USERS ACCESS AGREEMENT	8005	8-5

CHAPTER 8

INTERNET ACCESS POLICY

8001. BACKGROUND. The INTERNET, specifically the World-Wide Web (WWW), is a valuable tool for obtaining and disseminating information world-wide. When used properly it can facilitate Marine Corps information management needs and enhance productivity. However, the Marine Corps network which connects to the INTERNET and the WWW has limits to the number and types of information files (text, pictures, etc.) it can transport. Too many people simultaneously sending and/or receiving large files can degrade network performance and deny access to other official INTERNET users. Also, the INTERNET provides access to information which is not appropriately accessed via the Marine Corps network. These conditions demand discipline with both the size of files and the types of information accessed when using Marine Corps systems in conjunction with the INTERNET.

8002. POLICY

1. Official Use. Marine Corps resources (i.e., computer hardware, software and telecommunications infrastructure) that facilitate use of INTERNET services can be used when work related and determined to be in the best interests of the Federal Government and the Marine Corps. Access should be appropriate in frequency, duration, and be related to assigned tasks. Examples include using the INTERNET to:

a. Obtain information to support DoD/DoN/Marine Corps missions.

b. Obtain information that enhances the professional skills of Marine Corps personnel.

c. Improve professional or personal skills as part of a formal academic education or military/civilian professional development program, if approved by the department head/commander.

2. Authorized Use. Marine Corps computers may be used to access the INTERNET for incidental personal purposes such as INTERNET searches and brief communications as long as such use:

a. Does not adversely affect the performance of official duties by the Marine/employee.

b. Serves a legitimate public interest such as enhancing professional skills.

c. Is of minimal frequency and duration and occurs during an individual's personal time.

d. Does not overburden Marine Corps computing resources or communication systems.

e. Does not result in added costs to the Government.

f. Is not used for purposes that adversely reflect upon the Marine Corps.

g. These permissible activities will be governed and may be limited by department heads and commanders.

3. Prohibited Use. Use of Marine Corps resources to connect to the INTERNET for purposes other than those described in paragraphs 1 and 2 above is prohibited. Examples of prohibited use include, but are not limited to the following:

a. Illegal, fraudulent, or malicious activities.

b. Partisan political activity, political or religious lobbying or advocacy of activities on behalf of organizations having no affiliation with the Marine Corps or DoD.

c. Activities whose purposes are for personal or commercial financial gain. These activities may include chain letters, solicitation of business services, or sale of personal property.

d. Unauthorized fundraising.

e. Accessing, storing, processing, displaying, or distributing offensive or obscene material such as pornography and hate literature.

f. Obtaining, installing, or using software obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement.

g. Sharing of INTERNET accounts.

4. The prohibited activities listed above may result in administrative or disciplinary action, including nonjudicial punishment or courts-martial.

5. Security. Storing, accessing, processing, or distributing classified, proprietary, sensitive, or "For Official Use Only" (FOUO) information on a computer or network must be in accordance with DoD Dir 5500.7R.

8003. INTERNET E-MAIL. The use of INTERNET E-mail is generally available to all users having a valid requirement. Use of INTERNET E-mail must support legitimate, mission-related functions, and must be consistent with prudent operational and security considerations. An SMTP Gateway that interfaces with Banyan Mail is currently available to service INTERNET mail requirements for the Camp Lejeune regional WAN users. Each department head/commander will approve access for users having a valid mission-related requirement for INTERNET E-mail. Subscriptions to mailing lists, which can generate excessive amounts of mail traffic, will not be approved. Subscription to mail lists will be authorized only after the department head/commander has validated the requirements and considers the subscription necessary official business. Valid requirements for such access will be consolidated within an organization and only one account will be permitted to register. Recreational, unvalidated, non-official subscriptions to mail lists are prohibited.

8004. ACCESS TO THE WORLD-WIDE WEB (WWW)

1. The availability of WWW browsers and access to files created with Hypertext Transfer Protocol (HTTP), Gopher, Anonymous File Transfer Protocol (FTP) and other anonymous information servers pose the greatest potential for impacting the Marine Corps network. Access to these resources must be controlled to protect the network.

2. HQMC announced Mosaic, Netscape, and Microsoft Internet Explorer as suggested products for INTERNET browsers. Although Mosaic is a free INTERNET browser, it consumes a large amount of bandwidth. Netscape is the INTERNET browser currently fielded with all tactical data network (TDN) systems. Netscape is considered to be a much more efficient product, but it is not freeware. For reasons of network efficiency and standardization, Netscape and Internet Explorer are the only authorized network browser product for the Camp Lejeune regional network.

3. File Downloading. Downloading of necessary, large files will be limited to off-peak hours. The downloading of ".exe" or ".com" files will be directed to a floppy disk which must be scanned using approved virus protection/detection software prior to uploading to any other computer or disk drive. All downloaded files become Government property.

4. Connections to the INTERNET will be established only through official Marine Corps or DoD circuits. Access to the INTERNET via commercial service providers is prohibited without authorized approval from the Commanding General, (AC/S Management Support). Any such connections will not be made to any computer connected to the Camp Lejeune Wide-Area Network.

5. Any user requiring mission-essential access to the WWW must submit a request to the Information Systems Management Division via their department head/commander for approval.

6. All INTERNET usage is being electronically monitored for nonofficial accesses to the INTERNET. Access to WWW pages that contain pornography or adult oriented material is strictly forbidden. Prohibited access to the INTERNET may result in administrative or other disciplinary action such as courts-martial or nonjudicial punishment.

8005. INTERNET USERS ACCESS AGREEMENT

1. Appendix A of this Manual provides an INTERNET Access Agreement. All MCB users desiring access to the INTERNET via the Camp Lejeune network must execute this agreement prior to being granted access. Current users must execute this agreement within 30 days of the effective date of this Manual.

2. Department heads and commanders will ensure all INTERNET users under their cognizance execute this agreement.

3. All MCB organizations should retain a copy of the executed agreements on file and provide a copy to the Base Information Systems Management Division (Attn: Security Section).

APPENDIX A

INTERNET ACCESS AGREEMENT

INTERNET User: _____

(Name) (Organization)

I hereby acknowledge I am being granted access to the INTERNET for authorized U.S. Government use only and I will not access the INTERNET via a Marine Corps computer for any prohibited purpose. Prohibited uses include, but are not limited to:

- Illegal, fraudulent, or malicious activities.
- Partisan political activity, political or religious lobbying or advocacy of activities on behalf of organizations having no affiliation with the Marine Corps or DoD.
- Activities whose purposes are for personal or commercial financial gain. These activities may include chain letters, solicitation of business services, or sale of personal property.
- Unauthorized fundraising.
- Accessing, storing, processing, displaying, or distributing offensive or obscene material such as pornography and hate literature.
- Obtaining, installing, or using software obtained in violation of the appropriate vendor's patent, copyright, trade secret or license agreement.
- Sharing of INTERNET accounts.
- Storing, accessing, processing, or distributing classified, proprietary, sensitive or "For Official Use Only" (FOUO) information.

I understand and acknowledge that engaging in the prohibited activities listed above may result in administrative, disciplinary, or legal action being taken against me including criminal prosecution.

I understand that INTERNET usage at Marine Corps Base is routinely monitored to prevent unauthorized or prohibited usage, criminal activity, and violations of security regulations. All information, including personal information, placed on or sent over this system may be monitored. During monitoring, information may be examined, recorded, copied and used for authorized purposes. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. My use of this system constitutes consent to monitoring for these purposes.

_____ _____

Signature of OIC, Title, Date Signature of User, Date