OPERATIONS CONSIDERATIONS FOR MINICOMPUTER SYSTEMS

CONTENTS

1. GENERAL

1.01 This section is to provide general information concerning the Minicomputer Operations function in a Minicomputer Operations Center (MOC).

1.02 Whenever this section is reissued, the reason(s) for reissue will be listed in this paragraph.

1.03 For purposes of this section, an MOC is any site containing clustered minicomputers. Therefore, this section is applicable to minicomputer operations sharing machine room facilities with large-scale computers; and is applicable to Minicomputer Maintenance and Operations Center(s) (MMOC); and is applicable to other minicomputer sites having multiple minicomputers that are not officially classified as MMOC sites.

1.04 An MMOC is defined under AT&T's Total Network Operations Plan (TNOP) and is a TNOP operations center having the responsibility for the operation of clustered minicomputers that serve standard Operations Support Systems (OSSs) as well as locally developed minicomputer based systems.

1.05 An MOC facility takes advantage of the cost savings and operational benefits inherent to clustering minicomputers. These economies result from efficiencies in power and environmental conditions as well as those efficiencies resulting from the concentration of computer operations expertise within a single work center. Even though this section only addresses the minicomputer clustered environment, this section should still be reviewed for applicability by personnel responsible for a non-clustered minicomputer residing at a location having no other computers.

1.06 The guidelines discussed in this section only deal with the operations function within a MOC. This function is most often referred to as Operations; in a MMOC, it is called the Minicomputer Operations Group (MOG) function. The MOG is the organization that performs the routine operations for the minicomputer cluster. The MOG organization interfaces with the user, other computer centers, and maintenance organizations. A MMOC is comprised of another group called the Minicomputer Maintenance Group (MMG) who have maintenance responsibilities. MMG functions are not discussed in this Section.

1.07 In general, operations is responsible for the day-to-day operation of minicomputers. This includes the starting and restarting of each system, making entries in operation run logs, making computer switch settings specified in the operating instructions along with appropriate media handling and administration. Operations personnel respond to system error messages and alarms and take specified actions in response to user trouble reports (problems). They are responsible for analyzing and sectionalizing trouble conditions and referring these to the appropriate organizations (e.g. - vendor). Operations personnel are responsible for analyzing computer performance and preparing management reports. Environmental and security management are part of the functions performed by operations personnel.

2. ADMINISTRATIVE OPERATIONS GUIDELINES

2.01 This subsection describes general procedures designed to ensure professional management of the resources; action necessary for the protection of essential data; and to ensure the operational integrity of minicomputer systems located in the MOC. The minicomputer operations organization is responsible for ensuring that system performance is not impaired because of problems associated with the media and software that they administer.

A. MANAGEMENT OF MAGNETIC RECORDING MEDIA

2.02 Data may be recorded on various magnetic media such as magnetic tape, disk cartridges, disk packs or flexible disks. It is recommended that established guidelines be rigorously followed with regard to processing and handling these media so as to minimize the potential loss of essential information due to poor quality, neglect, contamination or physical misuse. The manufacturers of the various magnetic media publish recommendations for the use of their product to receive optimum results.

2.03 Magnetic tapes processed for Automated Message Assembly (AMA) recording systems (e.g. - AMARC) must be of the highest quality and certified to avoid tape read errors caused by poor quality tapes. Verification procedures for the assurance of quality AMA tapes should be established. Since many OSS's also record important data on magnetic tape, it is recommended that all magnetic tapes of a

MOC be of high quality and certified. (The recommendation for certification does not apply for tapes that will be used on drives that have read after write capability.)

2.04 Disk cartridges and disk packs used within the MOC should have their errors flagged and be certified to read and write 100% error free throughout their guarantee period. Flexible disks should also be certified to read error free. Applications having spare tracks that can be reassigned when problems are detected may be an exception to the requirement for certified disk packs.

2.05 Careless handling and storage of magnetic tape can cause permanent tape damage that could result in errors or loss of critical data. These errors may be minimized by taking the following reasonable precautions:

(a) Do not splice magnetic tape.

(b) Store tape reels in their containers.

(c) Store empty tape containers tightly closed so as to keep out dust and other contaminants.

(d) Handle tape reels by the reel hubs and not by the outer flange rims.

(e) Avoid applying pressure on flange rims since this may warp the reels and damage the tape edges.

(f) Check tape reels before using them to be sure they are not warped and will not wobble when properly mounted on the tape drives.

(g) Do not mar the tape recording surface by allowing it to come in contact with clothing, or by poor handling during the tape mounting or threading operation.

(h) Do not affix any external labels on the recording surface.

(i) Do not reuse any tape or tape reel that has fallen until it has been inspected, tested and proven sound by the use of appropriate tape diagnostics.

(j) Do not store tapes by stacking them one atop another.

(k) Store tapes vertically in tape racks away from equipment that can generate magnetic fields (e.g. - disk drives, power transformers).

(l) Store tapes in proper humidity range (40 to 60 percent).

B. CARE AND HANDLING OF DISKS

2.06 Similar precautions should be taken when handling disk cartridge and disk packs to protect the recording surfaces from contamination. If a disk pack has fallen or has otherwise been subjected to shocks and vibrations, its recording characteristics may be damaged. Similarly, its physical dimensions may be so altered as to exceed the recording head clearance limits (a common cause of head crashes). Should a disk pack become unusable due to physical damage, the disk pack should be removed from the minicomputer facility as a precaution against inadvertently remounting the pack unto a disk drive.

2.07 Disks are sensitive to dirt, dust, moisture and static electricity. When not in use, disks should be stored in protective cases and placed in approved cabinets in the data library area. Disk

packs should not be stacked; one on top of another.

C. EQUIPMENT CARE

2.08 Operations personnel are responsible for ordinary equipment care. A schedule for the periodic cleaning of tape drives, read/write heads, guides and other equipment must be posted and carefully followed. Cleaning frequencies, procedures, tools and supplies are listed in the appropriate vendor technical manuals and handbooks, and in applicable application (e.g. - OSS) documentation. Routine maintenance of this type must be confined to work that can be performed by the system operator. Other routine maintenance that would require specially trained personnel should not be attempted without specific authorization.

2.09 Tape read errors can be caused by the accumulation of dirt particles in the heads, drives, and other parts of the tape drive mechanism. Oxide deposits, dust, smoke, lint and fingerprint smudges can contaminate disk surfaces and may in some cases cause head crashes. The same contaminants will also cause tape errors.

2.10 Corporations that specialize in the maintenance of magnetic media should be engaged to inspect, clean, and evaluate computer tapes and disks at regular intervals when in-house maintenance expertise is not available. When necessary, tapes should be recertified.

D. TRANSPORTATION OF MEDIA

2.11 A large MOC may use mobile media trucks to transport tape reels, disk packs, and other storage media between the computer room and the media library in the same building. To protect magnetic tapes during shipment to another location, pack the magnetic tapes in standard tape reel shipping cases or special shipping cases. Disk packs and cartridges should be transported in impact resistant storage cases equipped with foam liners to protect them from physical damage. Metallic shielded shipping cases should be used if a possibility exists that data may be exposed to high intensity magnetic fields during shipment. All magnetic media to be shipped should be clearly labeled "DO NOT X-RAY - PLEASE OPEN FOR INSPECTION" to avoid having the data erased or not readable.

3. SOFTWARE MAINTENANCE

A. GENERAL

3.01 Many of the items discussed in this subsection have been taken from BSP Section 007-550-301. Guidelines describing interfaces between AT&T (or other Bell Company) and Southwestern Bell Telephone Company has been excluded. In order to interface with other AT&T organizations, Southwestern Bell should adhere to the BSP guidelines established for interfacing with other AT&T organizations and companies.

3.02 Operations personnel are responsible for the operation and integrity of a number of minicomputer systems serving users in many different departments and organizations. This subsection is applicable to both centrally developed and Southwestern Bell developed systems.

3.03 The computer instructions and logic that have been programmed for minicomputer systems consist of software modules that are linked (combined) together comprising what is called a GENERIC program. This generic program includes the following:

(a) OPERATING SYSTEM: The executive and

system programs that organize a central processor and its peripherals into a working unit for the execution of user application programs. Bell Telephone Laboratories (BTL) as well as other vendors provide such software. In many cases, vendors provide this software simultaneously with the installation of the minicomputer hardware.

(b) APPLICATION SOFTWARE: Programs that perform the specific tasks required by a particular application system.

(c) DATA BASE MANAGEMENT PROGRAMS: Programs that enable the user to create, maintain, and reference file data unique to a particular application system. Sometimes, such programs are called Utility Programs.

B. PROTECTION OF SYSTEM SOFTWARE

3.04 Operations management must establish policies and implement procedures to protect the integrity of the system software and data base information (also see Section 007-301-901SW, Data Security, for further reference). Software problems can cause repeated system crashes or erratic operation with a resultant loss of user confidence in an application system; damage to or loss of essential data can have a serious effect on customer service and company operations.

3.05 Policies and procedures to protect the integrity of the system software and data base information should include:

(a) Prohibition of unauthorized user programming.

(b) Data Base protection.

(c) Preparation and storage of backup media.

(d) Controls on the modification, change and update of system and applications software.

(e) Protection of system software and data base maintenance activities and major software revisions.

C. UNAUTHORIZED USER PROGRAMMING

3.06 System users and MOC operations personnel must not be permitted to make any unauthorized changes in the Generic Program such as the addition of user developed system enhancements. These personnel should not be allowed to install any application programs designed for personal use or for performing tasks unrelated to MOC needs.

3.07 The effects of unauthorized programming changes or additions are unpredictable. If a standard OSS is affected, then this can result with the loss of Product Engineering Control Center support or BTL support for these systems. For Southwestern Bell developed systems, such changes could cause loss of operation for extended periods of time affecting company business. Also, severe support problems could develop because of discrepancies between the actual system programs and the documentation available to the support (maintenance) organization.

D. DATA BASE PROTECTION

3.08 Southwestern Bell can access the system files of a standard OSS in order to create and maintain its own unique data base. The procedures established for a particular OSS (or Southwestern Bell developed) system shall dictate the manner in which the data is accessed and updated.

3.09 MOC management and the various user groups must have a clear understanding and be in complete agreement as to where the responsibility for data management lies. If the system user is responsible for data base maintenance, the data base manager must notify the operations supervisor whenever a major data base update has been completed so that the system backup media can be jointly scheduled for update to include the new information. Data base backup must be done on a regular scheduled basis to protect the data base; use an adequate number of log tapes and disk copies.

3.10 The designs of some systems may include one or more dial up ports for data management and other system uses. Since anyone at such terminal can modify the data files, access to the system via these terminals must be carefully controlled. Refer to Section 007-301-901SW for data security guidelines.

E. SOFTWARE BACKUP

3.11 Support system software and data base files can be damaged or destroyed through human error, equipment malfunctions or during hardware maintenance activities. Essential company records can be irretrievably lost or can only be recreated by the expenditure of much time, effort and expense. MOC management must establish procedures and controls to ensure that updated copies of system software and data base files are available to restore system service. The backup media may be on punched card, paper tape, disk cartridge, disk pack, or magnetic tape.

3.12 General procedures for the preparation of system backup data include the following:

(a) Identify the specific data requiring backup for each system located in the MOC and determine the intervals at which it should be updated.

(b) Prepare a schedule for removing a minicomputer system from service to create backup data. This is a joint responsibility of the operations supervisor and an authorized representative of the user organization.

(c) Consider the appropriateness of having system backup data available after major hardware changes.

(d) Schedule the backup process at times of least system usage or time of least impact on the user community.

(e) Provide system users with a copy of the schedule so that they can schedule system activity at a time that will not conflict with data base backup routines.

(f) Prepare specific instructions and procedures to be followed in preparing backup data for each type of minicomputer system located in the MOC.

(g) Post the schedule to prompt operating personnel.

(h) Always make a backup copy just prior to and immediately following a software modification. In the event of a failure, the change can easily be removed restoring the system to the software that existed prior to the update.

3.13 Operating procedures should specify the number of copies to be prepared, where they should be kept and

the length of time they should be retained. An up-to-date copy must always be kept on-site for immediate system recovery.

3.14 Typically, backup for critical data may exist in the minicomputer room, the data library, and the off-premise storage location. It is the responsibility of the operations staff to ensure validity of the backup data.

4. DATA IDENTIFICATION AND STORAGE

A. MEDIA IDENTIFICATION

4.01 An external label shall be attached to magnetic tape reels, disk cartridges, disk packs or other media for identification. Use blank pressure sensitive labels or obtain custom printed labels for specific applications. A typical label (for a tape reel) will contain the following information:

1. MOC (MMOC) identifier
2. Application system or OSS identification
3. Identification of data on tape
4. Date data was transferred to the tape
5. Date data on tape becomes obsolete (retention period)

4.02 Magnetic tapes containing standard OSS software data are labeled according to specifications used for mass distribution to OTC's. Per BSP Section 007-550-301, copies of these tapes shall have an external label affixed showing at least identical information as the original tape received from the central development group for items 2 and 3 of paragraph 4.01.

B. DATA LIBRARY

4.03 System backup media contain critical records that must be protected from loss, damage and contamination. These data should be kept in a separate media storage area or data library.

4.04 A data library may be thought of as public library in which each tape reel, disk cartridge, disk pack or flexible disk is equivalent to a book. Each item in the library must be inventoried, cataloged and stored in a safe location from which it can be quickly and easily retrieved. Administrative controls must be established and carefully followed to ensure that essential data are not misplaced, lost or damaged.

4.05 A small minicomputer center or a center having some systems that require certain data to be immediately available may store a minimum amount of system backup data in the computer room. In a large (more than 10 minicomputers) center, however, system backup information recorded on magnetic media should be stored in a data library located in the same building and near or adjacent to the minicomputer room.

4.06 General guidelines for a data library are:

(a) The data library should be near or adjacent to the minicomputer room.

(b) Room temperature should be between $60^{o}F$ and $80^{o}F$ with relative humidity of 40% to 60%. Ideally, the environment should be identical with that of the computer room. Audible and visual environmental alarms should be provided.

(c) The data library should be equipped with fire detection and alarm

systems. Suitable fire extinguishers should be provided (see Section 007-590-903SW, Physical Planning and Physical Security). Do not store any combustibles in the area.

(d) Emergency lighting should be provided.

(e) Security requirements must be vigorously followed.

(f) Do not use the library as a general work area. Only file management related activities should be allowed.

(g) Do not operate equipment capable of generating strong electrical fields in this area.

(h) Smoking and the use of flammable substances must be prohibited in the data library.

C. MEDIA STORAGE

4.07 Magnetic media should be stored in steel storage cabinets according to the following guidelines.

(a) MAGNETIC TAPE: Store magnetic tape reels vertically to prevent possible tape damage. Tapes in tape seals should be suspended from sealed reel hanger bars; tapes in canisters should be placed in standup canister racks.

(b) DISK CARTRIDGES: Store front or top loading disk cartridges in mounting racks sized for the specific cartridge type.

(c) DISK PACKS: Store disk packs in a suitable cabinet equipped with strong horizontal shelves. DO NOT STACK.

(d) FLEXIBLE DISKS: Store flexible disks in their original cases on the library shelves.

4.08 A large MOC may have specific storage cabinets for each media type. In smaller centers, standard cabinets can be custom configured for mixed media storage.

4.09 Assign specific storage areas for the backup media associated with each support system type. Assign a section within the area for each specific system. Affix labels to identify the area and section. Within the section, designate rows or shelves for particular functions. Number the slots or racks from left to right, top to bottom. This arrangement allows operations personnel to select any tape quickly and easily.

4.10 Do not store blank tapes or tapes containing generic program data, utility programs, diagnostic tests and similar information in the same cabinets as system backup tapes.

4.11 Provide locked cabinets for media containing critical or confidential information and other items of a similar nature.

D. LIBRARY INVENTORY CONTROL

4.12 Establish an inventory control system to identify the present location and use of each magnetic tape, cartridge and disk pack or any other library item of a similar nature. A system of this type will track media usage and performance to meet ongoing requirements for quality and expense control.

4.13 Three essentials for inventory control are:

(a) A unique serial number for each itemin the library.

(b) An index to its present location.

(c) A history file.

E. SERIAL NUMBER

4.14 Assign a unique serial number to each magnetic tape, disk, or other library item immediately after receiving it from the vendor or distributor. Affix a permanent, exterior identification label. It should contain the following information:

(a) Serial number

(b) Date that the magnetic media went into service

(c) Location in library.

F. DATA LIBRARY INDEX

4.15 Record the serial number and other pertinent information on a form such as shown in Exhibit 1. Use separate sheets for each media type. The index contains basic information on the tapes and disks in the data library listed by serial number. It identifies the manufacturer and brand name, the date of initial service and the system in which it is being used. The remarks column may be used to list pertinent items such as the purchase order number, the distributor and other such information.

G. DATA LIBRARY STATUS FILE

4.16 The data library status file (see Exhibit 2) contains a separate card or sheet for each tape, disk or disk pack. These are filed consecutively by media type and serial number. It identifies the particular minicomputer system and application in which the tape is currently being used; the date on which the data becomes obsolete; and also includes a space for remarks. The status file is also used as a record of previous use. In a large center, a mechanized tape library system would eliminate manual record keeping and avoid errors.

H. OFF-SITE STORAGE OF RECORDS

4.17 Essential records such as OSS data bases and other data that would be difficult or impossible to recover following the loss or damage to the original must be duplicated and stored in a secure area at another location. See Section 007-590-901SW for further criteria.

4.18 The storage area must be airconditioned and meet the same environmental requirements as specified in paragraph 4.06.

4.19 The off-site storage area should be equipped with a lockable data safe. The safe should meet the minimum requirement of the Underwriter's Laboratories Fire Class 150 Two-Hour Label.

4.20 Establish a schedule for periodic duplication of essential records and for their transfer to an alternate storage site. Log all movement of these records from the operations center to the off-site storage location and vice versa. Establish a check procedure at each location to acknowledge receipt of these files. In addition to data files, other essential information with off-site storage requirements would include:

(a) System software

(b) Application programs

(c) Operational documentation

(d) Important tape and disk library records.

5. OPERATIONS SUPERVISOR RESPONSIBILITIES

5.01 The operations supervisor should work closely with the user departments and the Minicomputer Hardware Maintenance Group (e.g. - MMG) to resolve problems that affect minicomputer system operation.

5.02 Procedures should be established to notify minicomputer users when:

(a) A system must be or has been removed from service because of a hardware failure and there is no backup available.

(b) A power or environmental condition has halted or seriously affected system operation.

(c) A defective communications link, facility, or terminal is identified.

(d) A hardware or software related problem is cleared.

5.03 The operations supervisor should negotiate with the system users and maintenance organization on a proposed preventative maintenance (PM) schedule. The operations supervisor should coordinate and adjust the PM schedule with the maintenance group and/or contractor.

5.04 The operations supervisor should prepare and distribute standard operating and procedural instructions for reporting and clearing troubles for each type of OSS or Southwestern Bell developed system within the MOC. This pre-emergency planning should be done in order to minimize the potential confusion caused by multiple trouble reports, incorrect referrals, insufficient trouble details, improper dispatching and uncoordinated trouble clearing that can result without a good preplanned standard operating procedure.

5.05 The standard operating procedures for reporting and clearing troubles should clearly define the responsibilities of the system user or user organization for identifying and clearing local troubles or other poor operating procedures.

5.06 The operations supervisor should be on the alert for unusual operating conditions and have a procedure available for their identification, patterning, and reporting to the appropriate maintenance organization. Included in this category are troubles whose cause cannot be determined, suspected hardware/software related problems, and any other troubles or conditions that interface with the normal operation of any system within the MOC. This kind of problem should be reported to a specifically designated trouble reporting location (generally in the operations group). Arrangements should be made for handling these trouble reports on an out-of-hours basis or during those periods when the problem is uncovered. Under these circumstances, the operations group becomes a limited control center and the operations supervisor assumes the responsibility for the coordination of minicomputer system repair activities.

6. TROUBLE REPORTING ADMINISTRATION

6.01 The following functions should be included for the administration of trouble reports by the operations group (e.g. - MOG):

(a) Receipt and logging of trouble reports

from all sources (particularly end-users) on systems being operated on by the operations group.

(b) Issuance of trouble tickets (for systems that specify the use of trouble tickets as the mechanism for reporting troubles).

(c) Analyzing of trouble reports and verification of trouble conditions.

(d) Restoration of service for those systems provided with backup processors and/or peripherals.

(e) Isolation of trouble conditions using system diagnostics or other fault isolation procedures specified in system documentation or in company operating instructions.

(f) Referral of troubles to appropriate work force for correction.

(g) Establishment of an identification system to track troubles.

(h) Entry of time and date of trouble referral into tracking system.

(i) Tracking the status of all trouble conditions to assess the need for escalation.

(j) Following approved plan for trouble escalation when preplanned time ranges for trouble resolutions are not met.

(k) Conveying status of trouble condition to user (e.g. - once per hour while problem is outstanding).

(l) Testing of systems after trouble is cleared.

(m) Restoration of normal service after notifying the responsible manager of the user organization.

(n) Closing out trouble incidents (i.e. - problem is resolved).

(o) Completing and forwarding, when required, Minicomputer Maintenance Activity reports.

(p) Filing the completed trouble report (or trouble ticket) for future trouble analysis studies. This file should include all associated documents pertaining to the trouble condition that might be useful for future reference (i.e. - error printouts, etc).

6.02 Exhibit 3 illustrates a form created by AT&T to be used as an OSS trouble ticket. Exhibit 4 represents a trouble log which can be used in conjunction with the trouble ticket. When centrally supplied OSS systems are involved, it is recommended that the AT&T forms be used so as to stay consistent with personnel who designed and support the particular OSS system. These personnel expect to reference the AT&T established form.

6.03 Quite often, problems on minicomputer systems are of an intermittent nature. These troubles affect system operation but rarely generate a formal trouble report. Therefore, it is important that operations personnel be made aware of the need to identify these types of troubles so that they too can become part of the data used for trouble analysis. A successful maintenance program should include procedures for collecting and analyzing all available trouble indicators as well as potential sources of OSS troubles.

6.04 To have a successful maintenance program, established procedures should include the following:

(a) An analysis of closed out problems,

problem logs, and diagnostic output messages for pattern analysis and evidence of recurring trouble patterns.

(b) A pattern analysis of error files when error logging features are inherent to the software of the impaired system.

(c) An examination of vendor/telephone company (Southwestern Bell) hardware PM schedules for evidence of activity caused trouble.

(d) Scheduling and running standard diagnostic test packages appropriate for the troubled system. (This function may be the responsibility of the MMG. In these cases, operations assumes a coordinating and scheduling role.)

7. PROBLEM AND CHANGE MANAGEMENT

7.01 In general, computer systems experience problems (troubles). Likewise, technological advancement and/or new environmental conditions create a need for computer system changes. For these reasons, procedures must be established to control the minicomputer processing environment.

7.02 Problem management is the process of minimizing the impact of problems (troubles) affecting the minicomputer environment. This objective is achieved by establishing procedures addressing the following:

(a) PROBLEM CLASSIFICATION - After a problem has been identified, it is necessary to assign the problem a severity classification. This classification then dictates subsequent action leading to restoration of the processing environment. Any classification scheme that meets local requirements is considered valid. Two examples follow:

Example 1:

Severity 1 - A trouble condition exists which cannot be circumvented and either: 1) Inhibits a significant portion of the system from performing its designated function OR 2) Critically affects operations. This classification is the most critical and requires immediate attention.

Severity 2 - A problem condition similar to severity one exists; however, repair action is not required until a known future date.

Severity 3 - A problem condition exists which is not critical to operations and which can be circumvented.

Severity 4 - A problem condition exists which is of minor consequence. Corrective action is performed as time permits.

Example 2:

Severity 1 - A problem condition exists which makes it impossible to continue processing. This is extremely critical and requires immediate attention.

Severity 2 - A problem condition exists which critically affects operation of the minicomputer system. A circumvention for the problem does not exist. This condition also requires immediate action even though a part of the system is still operational.

Severity 3 - A problem condition exists which affects system operation. A circumvention does exist. Permanent repair action needs to be scheduled.

Severity 4 - A minor problem exists. Repair action will be addressed as time permits. Contingency should exist to escalate such problems to assure they do not remain outstanding indefinitely.

(b) CONTACT LISTS - Many problems cannot be resolved by local operations staffs. Outside consultation is required; be it another company organization or a vendor. To get this aid in a timely manner, contact lists must be created and made easily accessible to the MOC operations staff. All personnel and vendors that are to be directly contacted by the MOC, when problems occur, must be included in the lists.

(c) PROBLEM ESCALATION - Problem escalation methodology considers two types of escalation; resource availability, and management notification. Specifically:

1. Escalation of Problem Severity: The goal to be achieved when escalating problem severity is to provide more resources for resolution of the problem. This process should not result with more management direct involvement; rather it is management's function to assure that needed technical resources are made available.
2. Management Notification: This process is only to provide information. Notification intervals have been previously established.

(d) PROBLEM REPORTING - The existence of a problem is normally initially noticed by the end-user or operations personnel. Procedures need to be established, on an application system basis, that define a notification process. Written as well as telephone notification can be valid assuming that the specific method has been documented and that the end-user has been properly notified of the option chosen. A central receipt point for these problems shall be designated. It is the responsibility of the coordinator to assure that all problems are then distributed for assignment. Priority of these tasks is guided by the application system established problem classifications. If the problem is with an AT&T (BTL, Western Electric, etc) centrally provided system, then the problem coordinator should consult BSP Section 007-240-210 subsection 3 for further action. Paragraph 3.01 dictates the following: A trouble report (see appendices 1 & 6 to BSP Section 007-240-210) is submitted by the user when the system is not performing in accordance with the present design, or a design deficiency exists which does not allow the system to meet its objectives. Trouble reports are

originated by the OTC for repair maintenance, or for Personnel Subsystem (PSS) troubles. (Appendix 8 of BSP Section 007-240-210 describes trouble report completion instructions.) Paragraphs 3.02 through 3.08 of BSP Section 007-240-210, primarily describe subsequent responsibilities of AT&T for addressing the problem. Paragraph 3.08 describes the procedure to follow when AT&T does not agree that the incident was a problem. As noted, the final arbiter is the AT&T project manager for the specific project.

(e) PROBLEM RESOLUTION: Upon establishing a resolution to the problem, a test will be performed to validate that the suspected resolution does in fact correct the outstanding problem. Permanent installation of the resolution (e.g. - software correction, procedural change, etc) means that the problem is no longer outstanding; i.e. closed. Documentation shall accompany resolution installation. If the resolution is transmitted orally, associated formal documentation should follow within 15 days.

7.03 Change Management provides for planning, coordinating and implementing changes to the minicomputer processing facilities. Methods need establishment for the requesting of changes and the installation of changes. Installation of a change is independent of the original reason for its inception.

(a) Reasons for Change:

1. The change may have been originated as the result of problem resolution efforts.
2. The change may be due to someone recognizing a need to expand the capabilities beyond initial design objectives.
3. The change may be due to technological improvements or economic considerations.

(b) Change Requesting - All change requests shall have the following accompanying documentation:

1. Description of the change
2. Reason for the change request
3. The operational impact of the change
4. The economical impact (and/or justification) of the change.

The manner in which change requests are routed through company sections is dictated by the Southwestern Bell project manager of the target application. All changes shall be submitted in writing.

(c) Change Processing - The change coordinator (for the application, or for the operating system) must log all incoming change requests. It is then that person's responsibility to appropriately route the request for action. If the target application is Southwestern Bell developed, the change coordinator will:

1. Track the request through established routing channels.
2. Will provide status information to the requester.
3. Will remain primary coordinator for the change request until final disposition. At this time, the change request will be considered terminated (closed).
4. Will insure that any change scheduled for implementation has been thoroughly tested.

5. Will insure that corresponding documentation accompanies the change.
6. If request for change is denied, then the change coordinator will so notify requestor. If the change targeted application is an AT&T developed system, then the change coordinator must conform to the guidelines of subsection 5 and paragraphs 6.08 through 6.14 of BSP Section 007-240-210. The change coordinator, in this instance, is the same as the BSP specified, OTC-MCC.

7.04 Organizational Requirements (MCC) - The Southwestern Bell section responsible for managing a centrally developed product (product management) shall appoint a product manager. The product manager has the responsibility of designating individuals to serve as problem and change coordinators (can be same individual). This function is designated by AT&T as the OTC-MCC (MCC = Maintenance Control Center) in the Bell System Practices. See BSP Section 007-240-210 for further clarification of the MCC function.

7.05 The Southwestern Bell project manager shall have authority to act as the final arbiter for any Southwestern Bell developed system when disputes develop between the problem or change submitter and personnel assigned the task to resolve the problem or to develop the change. If the system is AT&T centrally supplied, then the AT&T project manager is the final arbiter of any dispute. A dispute is said to be in progress when one of the two following conditions are in progress:

(a) An incident is submitted as a problem for resolution. The organization (or personnel) assigned to resolve the problem determine that it is not a problem. The submitter disagrees.

(b) A change request is submitted and is refused. The requestor still believes that the request is valid.

8. SELF-CHECK QUESTIONS

8.01 The purpose of the following questions is to provide a tool for evaluating the present environment as it pertains to this Section. All questions answered with a 'YES' indicate that the MOC is conforming to the requirement or recommendation. A reply of 'NO' implies that a weakness exists. The MOC should investigate this weakness and determine what actions should be taken to alleviate the potential problem. It is possible that no action be taken due to economic considerations. The economic consideration justifying that no action be taken should be formally documented.

(a) Are magnetic tapes and disks filed in an orderly manner?

(b) Is there a tape and/or disk cleaning plan?

1. Are tapes cleaned on a regular basis?
2. Are disk packs checked and cleaned?

(c) Are tapes stored vertically?

(d) Are disk and tapes stored in protective cases?

(e) Are all disk packs stored such that they are not stacked atop one another?

(f) Is media shelving labeled appropriately?

(g) Are tape utilization records maintained?

(h) Is there a schedule for continually replacing the backup media at off-site premises with more current backup data?

(i) Does the off-site storage location have environmental controls conducive to magnetic media storage?

(j) Are tapes transported to off-site premise storage in approved tape transport containers?

(k) Have record systems indicating vendor, model numbers and features, and level of engineering change been established?

(l) Is there an inventory of all software in the MOC?

(m) Are scheduled maintenance activities monitored to assure proper reliability and hardware performance?

(n) Is there a mechanism to verify that maintenance CLAIMED is maintenance PERFORMED?

(o) Are Preventative Maintenance (PM) procedures adequate? Are hardware reliability objectives being met?

(p) Are all periods of downtime verified?

(q) Are steps taken to resolve all minicomputer related problems?

(r) Are the trouble and recording controls adequate?

(s) Do problem escalation procedures exist?

(t) Are contact lists up-to-date?

(u) Are there backup procedures for:

1. Operating system software?
2. Application software?
3. Data bases?

(v) Are all applications in the MOC prioritized?

(w) Do data restoral procedures exist for all systems?

(x) Are there controls for dial-up ports?

(y) Are passwords changed regularly?

(z) Are program changes controlled and recorded?

(aa) Has a "dry-run" been held in the past three months to test the ease and accuracy of the backup system?

EXHIBIT 1

DATA LIBRARY INDEX

MEDIA _____ Page _____

SERIAL NUMBER	BRAND NAME	SERVICE DATE	SYSTEM NAME	REMARKS

EXHIBIT 2

DATA LIBRARY STATUS FILE

MEDIA TYPE _____ SERIAL NO. _____
BRAND NAME _____ SERVICE DATE _____

COMPUTER SYSTEM ID	APPL. NAME	CREATION DATE	EXPIRATION DATE	REMARKS

EXHIBIT 3

COMPUTER OPERATIONS CENTER TROUBLE TICKET

location	OSS	date	time	ticket no.
system	terminal	data circuit	reported by	received by

TROUBLE REPORT-

ANALYSIS/ACTION TAKEN-

referred to	date	time	ticket #

RESOLUTION-

COMPUTER SYSTEM	
front end	
local	
remote	
TROUBLE TYPE	
hardware	
software	
procedure	
other	
NETWORK	
private line	
bridge	
dial up	
facilities	
data set	
protocol	
other	

TROUBLE CLEARANCE			SERVICE RESTORAL		
by	date	time	by	date	time

TERMINAL	
hardware	
hardware	

Exhibit 4

OSS TROUBLE LOG

MOC/OSS _____

DATE	TIME	SYS	TICKET NO.	TROUBLE REPORT	CLEARED