COMPUTER CENTER PHYSICAL SECURITY AND DISASTER RECOVERY

PHYSICAL SECURITY

CONTENTS PAGE

1. GENERAL

1.01 The guidelines in this section were developed by a multicompany GUARDSMAN project team under the direction of AT&T Information Systems Technical Support and Standards. This section is issued by the AT&T Director—Information Systems Planning and Support to assist the Bell System Companies in implementing a Physical Security and Disaster Recovery Program.

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

1.03 This section provides the guidelines necessary to effectively select and implement the protective measures required to secure the elements of the processing environment. (Refer to Section 007-590-301.) The responsibility for adequately securing the processing environment will reside with the organization responsible for the individual computer facilities.

1.04 Where local, state, or OHSA (Occupational Safety and Health Act) regulations require higher degrees of protection, the legislated criteria should be followed.

1.05 The term physical security, as employed in this practice, refers to the protection of all elements of the processing environment from any disaster (man-made or natural) by employing the mechanical and human resources necessary to safeguard the company assets.

1.06 The methods of protecting the processing environment are divided into three areas: protection by design, by devices, and by procedures. Each area will contain the description of various

components of physical security relative to that area of protection.

1.07 Existing computer facilities should consider upgrading their security program to comply with these guidelines as soon as possible. New computer facilities are required to adhere to the security measures contained in this section.

1.08 The economic justification to upgrade or implement a security program should be consistent with the hardships that the company would suffer if the processing environment were either lost or severely disrupted. (Refer to Section 007-590-302.)

2. PROTECTION BY DESIGN

2.01 This part identifies the components essential to protecting the processing environment by design. It is strongly recommended that the design considerations identified in this section be embodied in the architecture of all processing environments. It is essential that the local building engineers be notified of these requirements in the planning stages of a computer facility.

A. Site Considerations

2.02 If possible, the computer facility should not be located in a geographic area that is vulnerable to fire, floods, tornados, and earthquakes or has a history of exposure to any type of natural disaster.

2.03 The computer facility should not be located near hazardous processes or materials such as explosives, smoke, corrosive fumes, storage tanks for fuel or natural gases, or any other potential hazard.

B. Building Considerations

2.04 The ideal situation would be to locate the computer facility in a company-owned building designed specifically for a computer facility and dedicated to housing computer-related activities, personnel, and equipment.

2.05 The next most advisable situation would be to locate the computer facility in or next to a central office building. This would take advantage of the existing security features in a central office as well as having the computer facility in a company-owned building.

2.06 Company headquarters locations are not suitable for housing computer facilities as they are easily recognizable and considerably more vulnerable to disruptive action than a remote site.

2.07 Company-leased or company-leased shared buildings are the least acceptable of all considerations. This is due to the difficulty of implementing an adequate physical security program.

C. Compartmental Design

2.08 Compartmental design uses the room-within-a room concept of designing a computer facility. Figure 1 illustrates a computer facility using the compartmental design concept. It is meant to serve as an aid in understanding the compartmental design theory and not as hard-fast design criteria. It will also serve to demonstrate that areas of physical security such as access control, environmental control, and fire detection and suppression devices can be more efficiently utilized through the use of the compartmental design technique (Section 760-630-400).

2.09 The following compartment descriptions will contain items unique to the physical security of a computer facility that should be included in its design. Each item will be described in detail in the subsequent paragraphs. Areas defined as being located within the machine room will require raised flooring.

(a) ***Computer Facility:*** The computer facility is the core of the room-within-a-room design. It is separated from the outside areas by fire-rated walls and fire doors that are 1-hour fire rated. Access to the room must be controlled by devices that require certain criteria prior to allowing entry. The environment must be controlled by air conditioning, humidity control units, and water cooling, when required, as prescribed in the vendor specifications. In addition:

- Power must be of sufficient quantity to prevent outages.
- Flooring must be raised.
- Detection devices for water, heat, and smoke should be appropriately placed.

- Fire suppression devices should be strategically located within the room.

- Water protection and detection devices should be designed into the floors and ceilings.

- Lighting must be sufficient.

(b) ***Magnetic Media Library:*** The magnetic media library is located within the computer facility, but separated by fire-rated walls and fire doors that are 2-hour fire rated. It must contain all physical security items specified in (a) above. It is recommended that Halon 1301 be used as a fire-suppression device in the magnetic media library. This library could contain tapes, disk packs, and mass storage cartridges, as well as other types of magnetic media.

(c) ***Communications/Electronic Equipment Room:*** The communications/electronic equipment room, which houses the telecommunication equipment and power breakers, is located within the computer facility and contains the same elements of physical security. It should be separated from the computer facility by fire-rated walls and fire doors that are 1-hour fire rated. The access control device can be of a pick-resistant, long-throw key lock variety. Key control procedures should be utilized.

(d) ***Storage Area:*** The storage area must be located outside the computer facility. This is not the primary storage area and should contain only those supplies necessary for the operation of one shift. It is separated from the computer facility by fire-rated walls and fire doors that are 1-hour fire rated. The fire wall can be the outside wall of the computer facility. The doors leading from the computer facility to the storage area should be equipped with alarms. The storage area must contain adequate fire detection and suppression devices.

(e) ***Input/Output Area:*** The input/output (I/O) area resides outside the computer facility. Access to the computer facility should be limited to window-type openings that would allow input/output to be passed between the computer facility and the I/O area. The window-type openings must include devices that can be closed and secured during off-tour hours. Access should be limited to authorized personnel only.

(f) ***Operations Area:*** The operations area is located outside the computer facility and serves as a buffer zone between the building proper and the computer facility. This room should be equipped with an access control device to limit access during off-tour hours. Personnel in direct support of computer facility operation will reside in this area.

(g) ***CE (Customer Engineer) Room:*** The CE room shall be located outside the computer facility. It should be secured with a key lock system to safeguard vendor equipment. There should be no means of access from the CE room into the computer facility.

2.10 ***Identification:*** The external identification of the building should be limited to the Bell logo and the company name. (See GL 75-01-184.) It should not identify the building as a computer facility. There should be no internal indications that the building contains a computer facility or any references to the location of the computer facility. (See GL 73-07-044.)

2.11 ***Location:*** The computer facility should be located in the core of the building. This would allow the building proper to act as a buffer between the building entrance and the computer facility.

(a) It should be housed above the ground level as to alleviate exposure to floods or other hazards, but should be no higher than the sixth floor due to the limitations of fire fighting equipment. However, if the building is a single story structure, the computer facility shall be designed to contain all protection designs and devices necessary to secure it from possible hazards.

(b) The computer facility should not be located above, below, or adjacent to parking garages, loading docks, cafeterias, test laboratories, or any other potentially hazardous area. Water pipes (other than the chilled water to cool the computers), sewage pipes, or any other potentially damaging substance should not pass through the floors, walls, or ceiling of the computer facility.

2.12 ***Construction:*** The purpose of this paragraph is to provide general planning information applicable to all computer facilities. Where such information is available in other

documentation, the documents will be referenced. This paragraph should be used as a guideline when discussing the construction of a computer facility with groups such as building engineering, fire protection, etc. Additional information for Building Planning for Operations Support Systems and Building Planning for Electronic Data Processing Systems is contained in Sections 760-150-155 and 760-250-150, respectively.

(a) ***Windows:*** It is recommended that the computer facility be windowless. However, if this is not possible, the windows should be of sufficient strength to withstand high impact levels. They should also contain the insulation necessary to protect the thermal environment of the computer facility. The decisions as to the type of window necessary should be made by the building engineers.

(b) ***Ceilings:*** The ceilings for computer facilities should be of a type that does not dust or flake. Ceilings should be constructed of noncombustible material or Underwriters Laboratory (UL) listed with a flame spread of 25 or less and a smoke develop rating of 50 or less. Ceiling height requirements are the same as New Equipment Building Systems (NEBS) equipment areas to provide space for equipment and cabling. Refer to Sections 760-300-150, 760-600-230, and 760-630-200 for additional information.

(c) ***Walls:*** The walls enclosing the computer facility shall extend from the concrete slab of one floor to the concrete slab of the next floor and shall be constructed of 1-hour, fire-rated noncombustible material. The tape library should be enclosed by 2-hour fire-rated noncombustible walls extending from slab to slab. Additional information can be obtained in Sections 760-630-100 and 760-630-200.

(d) ***Doors:*** The doors in the computer facility shall be UL listed class C doors. To provide the protection for which they were designed, fire doors are equipped with a self-closing device and shall be maintained in the normally closed position at all times. Refer to Sections 760-630-100 and 760-630-400 for additional information.

(e) ***Raised Floors:*** It is recommended that the raised flooring within the computer facility be 18 inches from the floor slab to the top side of the floor panels. (Refer to Section 760-200-110.) This height will provide the space necessary for the underfloor equipment and underfloor access.

(f) ***Lighting:*** The lighting for the computer facility should be designed to have illumination levels of 70 foot candles measured at desk height. The lighting should be on a separate ac lead from the ac lead serving the computer. It shall also be connected to the standby engine. The design standards for lighting systems are covered in Section 760-230-130.

(g) ***Power:*** High voltage commercial service should be distributed directly to a dedicated step-down transformer located in the vicinity of the computer facility. If this is not possible, a dedicated feeder or feeders must be provided from the local distribution board. Power vaults and access rooms or area (including person holes) should be located by design to allow for security. For additional information, refer to GL 77-04-087, GL 77-08-178, and GL 78-05-173.

(h) ***Air Conditioning:*** The air conditioning unit shall be of sufficient capacity to maintain a temperature level consistent with the temperature requirements specified by the computer manufacturer. It is strongly recommended that the air conditioning unit be dedicated to the computer facility and be connected to the emergency engine alternator. Refer to GL 76-11-067, GL 70-07-236, and Section 760-640-100 for additional information.

(i) ***Humidity Control:*** The humidity control unit should be of sufficient capacity to ensure that the proper relative humidity is maintained in the computer facility at all times. The humidity level should meet the requirements specified by the computer manufacturer. Refer to GL 76-11-067 and GL 70-07-236 for additional information.

(j) ***Structural Floor:*** It is recommended that the structural floor be constructed of reinforced concrete in accordance with Section 760-200-100. In active seismic areas, the design should include the standards for earthquake design loads contained in Section 760-200-023. Areas containing cable holes or cable slots should be constructed as described in Section 760-200-032 and fire stopped per Section 760-630-410. It is also strongly recommended that the structural floor not be covered with any type of floor covering materials so that the support assembly

for the raised flooring will rest directly on the concrete slab.

(k) ***Uninterrupted Power Supply (UPS) Room:*** Strong consideration should be given to constructing a room to house the UPS equipment during the design stage of a computer facility. This would eliminate the need to construct such a room at a later time when the cost may become prohibitive.

(l) ***Tape Vault:*** Consideration should be given to the construction of an on-site tape vault which would meet the criteria for an off-site storage facility. The criteria, as defined in Section 007-590-304, are as follows:

- It must be survivable when the primary facility has been totally destroyed.
- It must be accessible when the primary facility has collapsed.
- It must have security which is independent from that of the primary facility.

In order to accomplish this, the vault should meet the following requirements:

- Be constructed of materials equal to or stronger than the building
- Be located underground beyond the perimeter of the outside wall
- Be connected to the building by a tunnel that is secured and can be sealed to prevent damage from fire, water, smoke, or any other hazard
- Should contain the identical elements of environmental and physical security as the tape library.

(m) ***Radio Frequency Interference (RFI) Shielding:*** The RFI intensity should be limited to the computer manufacturer's specified level of less than 1 volt per meter. The RFI shielding may have to be constructed into the walls of the computer facility to meet this requirement. For additional information, refer to Section 760-220-100 and GL 78-02-019.

(n) ***Communication/Power Cable Room:*** The location within the building where the communication and power cables (that support the computer facility) enter should be secured. The cable should be accessible only to authorized personnel. Consideration should be given to housing these cables in a room equipped with an access control device. A key lock system would satisfy the requirements.

3. PROTECTION BY DEVICES

3.01 This part provides the guidelines for selecting and implementing the devices necessary to protect the computer facility from potential disasters. The recommendations in this part should be followed as closely as possible and implemented in a manner appropriate to the loss the company would suffer if the computer facility were lost or severely disrupted.

A. Detectors

3.02 ***Fire Detection Systems:*** An approved early warning fire detection system must be installed throughout the computer facility and adjacent storage and administrative areas. The system must function during a loss of normal power. The system must detect fire within the compartment as well as below raised floors and above dropped ceilings. The fire detection system must provide audible and visual alarms within the computer facility and to other areas of the building such as the security area or an attended maintenance area. For a complete description of the various fire detection systems, refer to Section 760-650-100.

3.03 ***Water Detectors:*** Water detection devices should be placed under the raised floors throughout the computer facility, tape library, and any other area where water might damage the underfloor cables. This is a necessity in computer facilities that contain computer components cooled by chilled water since the piping for the chilled water is located under the raised flooring.

3.04 ***Temperature and Humidity Recording Devices:*** The temperature and humidity in the computer facility must be monitored and recorded on a 24-hour basis. Alarms, visual and audible, must be provided so as to signal that maximum or minimum temperature or humidity limitations are being approached.

3.05 ***Power Line Monitors:*** Power line disturbances may or may not be present at any particular site. To determine the quality of the commercial power at a specific location, a power line monitoring program should be undertaken (GL 77-04-087, GL 77-08-178). The line monitor chosen should be capable of detecting the following:

- Impulses of microsecond-to-millisecond duration
- Sags and surges, including a measurement of their duration
- Brownouts and long duration excursions of normal voltage
- Blackouts, including a measurement of their duration.

B. Fire Suppression Devices

3.06 ***Hand-Held (Portable) Extinguishers:*** The hand-held (portable) extinguishers should contain nonwetting fire extinguishing agents for electrical equipment; either carbon dioxide or Halon (1A 10BC) is recommended (Section 760-640-200). Water-type or Halon extinguishers should be provided to protect against fires in ordinary combustible materials such as paper. Fire extinguishers shall be distributed as outlined in Section 760-640-200, taking into account the maximum travel distance of 75 feet. Extinguishers shall be located where they are easily seen and readily available.

3.07 ***Water Sprinklers:*** Water sprinklers are generally not recommended for use within the computer facility. They are not effective on computer equipment fires. However, water sprinklers should be considered for areas such as the storage area or the administrative area. Refer to Section 760-640-300 for additional information.

3.08 ***Halon:*** The Halon 1301 automatic flooding system may be considered for use as a master fire extinguishing system for the computer facility, based on the economic feasibility of installing such a system. This decision should be consistent with the overall hardships that the company would suffer if the processing environment were either lost or severely disrupted. It is strongly recommended that Halon 1301 be used as an extinguishing agent in the tape library. When Halon 1301 is used in the proper concentration, it will extinguish fires, minimize machine damage, and will be of little or no hazard to personnel. Refer to Section 760-640-300 for additional details.

3.09 ***Carbon Dioxide:*** Carbon dioxide (CO_2) is not recommended for use as a master fire extinguishing system in the computer facility since it is potentially hazardous to the health of any employee exposed to it.

3.10 ***Standpipe and Hose System:*** Standpipe and hose systems shall be provided in accordance with Section 760-600-230 and 760-640-310.

C. Water Protection Devices

3.11 ***Hoods:*** If the computer facility is located either below another computer facility with chilled water cooling pipes or in an area where the potential for large amounts of water to enter through the ceiling exists, the installation of hoods in the ceiling should be considered. The purpose of the hoods is to direct the runoff of water away from the computer equipment.

3.12 ***Plastic Sheets:*** It is recommended that plastic sheets be located in readily accessible areas throughout the computer. Should a water problem occur, the sheets will be used to cover the computer equipment after the blowers go off. The sheets should meet the required standards for flame retardation (Section 760-610-200).

3.13 ***Drains and Pumps:*** Computer facilities containing water-cooled computer equipment should consider some type of in-floor drainage. The installation of a drainage system, with drains located in strategic areas of the computer facility, is one consideration. Another consideration would be the installation of pumps throughout the computer facility.

3.14 ***Safety Valves/Gauges:*** Water piping to the air conditioning units and to computer components that require chilled water should be equipped with shutoff valves, check valves, and pressure gauges. Shutoff valves will allow portions of the water system or the entire water system to be shut down in case of emergency. The valves should be clearly identified and readily accessible. Check valves allow water to flow in one direction only, thereby eliminating the possibility of water backing up through the pipes into the computer facility. Pressure gauges will detect any sudden

rise or fall in the pressure of the coolant being distributed through the system, sound an alarm, and automatically shut down the unit.

D. Access Control Devices

3.15 ***Door Alarms:*** It is required that door alarms be installed on all doors that access the computer facility and are not protected by an access control device, such as a card key system. The alarms should be designed so as to be audible throughout the computer facility and to signal the security area that a problem may exist.

3.16 ***Card Key Systems:*** The card key systems are strongly recommended as the primary access control device for the computer facility. The most highly recommended type of system is one that will:

- Control access to the computer center by the addition and deletion of card key numbers stored in a data base
- Record all entries and exists
- Allow levels of access between areas to be controlled, ie, between the computer facility and tape library
- Operate in a stepped-down mode even when its primary processing unit is down
- Deter pass-back (ie, two or more persons entering on a given employees's pass within a preset time dependent upon access/egress requirements)
- Program capability on levels of access authorization such as craft, management through second level, management third level and above, etc. This would allow for immediate "class of authorizations" denial of access should a work stoppage or other problem appear imminent. (Voice or other secondary access arrangement such as manual verification and access would be required to allow access by nonstriking personnel.)

This system should be attached to the emergency engine-alternator so it can operate during a power outage.

3.17 ***Key Lock:*** The key lock devices are recommended as a second level of access control for rooms that are located within the computer facility, such as the communication/power rooms. (See Fig. 1.) These devices are not recommended as a primary access control device for the computer facility due to the ease of duplicating keys and the expense involved in continually changing locks.

3.18 ***Cipher Locks:*** These locks are not recommended for use as an access control device for the computer facility due to the following two reasons:

(1) Cipher locks require the drilling of additional holes through the fire doors, thereby violating the fire and smoke protection requirements.

(2) The possible security breaches involved with the availability of the combination to unauthorized personnel.

3.19 ***TV Surveillance:*** This type surveillance should be considered for use in areas that are not occupied by the computer facility personnel. Viewing apparatus should be located in the control area of the computer facility as well as in the security area to allow for off-tour monitoring. Consideration may also be given to attaching a video tape device to the TV surveillance equipment to permanently record any intrusions that might occur. Time-lapse video tape recorders, or equivalent time compression systems, provide increased efficiency for recovery of access viewing details.

3.20 ***Motion Detectors:*** These detectors may be considered for areas that are not occupied by the computer or full time occupied by computer personnel. Many motion detectors utilize radio frequency methods which should be compared to the constraints on radio frequency interference on computer systems. (See paragraph 4.32 and GL 78-02-019.)

3.21 ***Person Trap:*** The ideal method of access control is the use of a person trap in conjunction with a card key system. The person trap virtually eliminates the ability for one person to follow closely behind another person to gain access to the computer facility. The person trap provides an area where anyone seeking access can be observed and either allowed or denied entry.

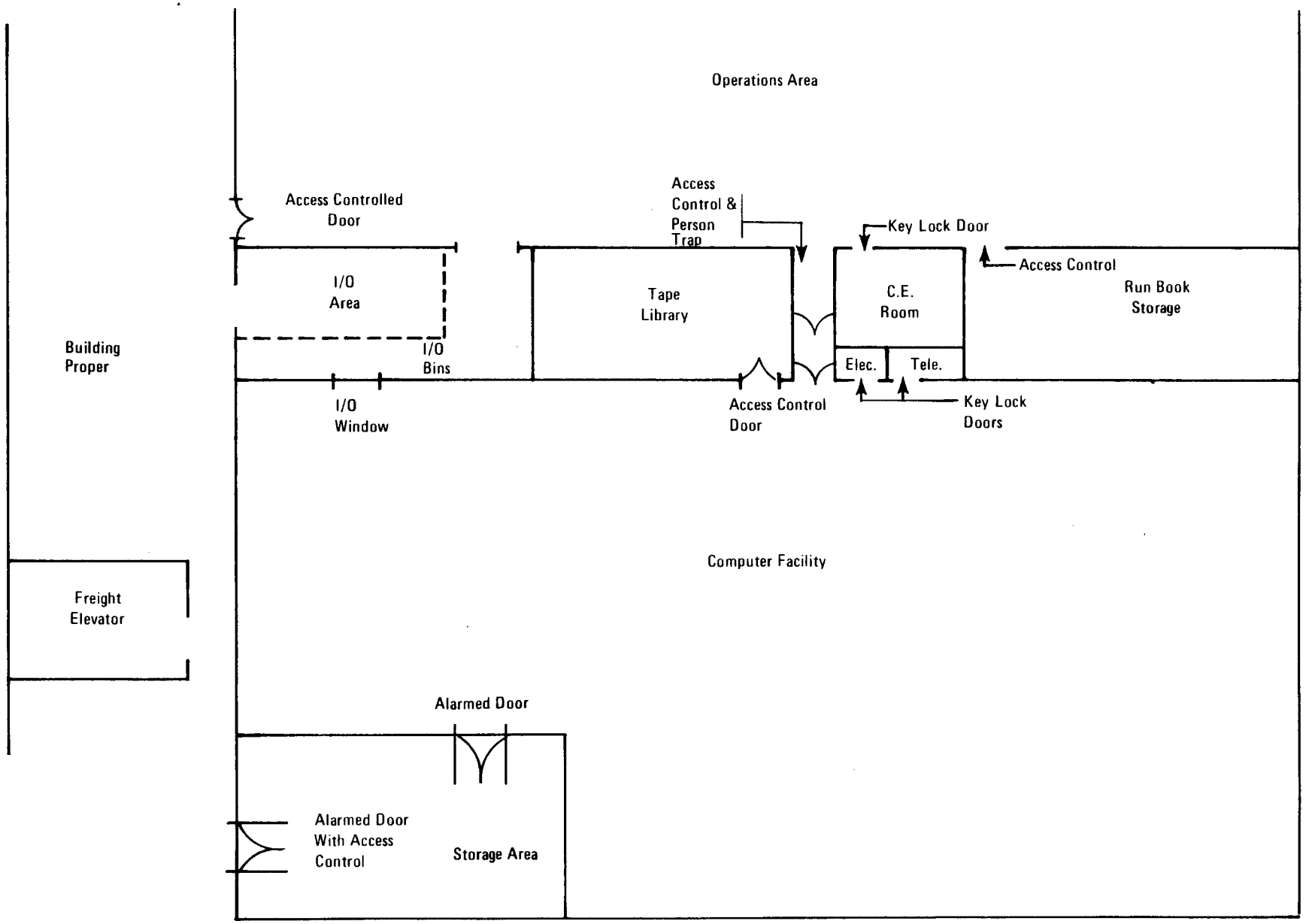

Fig. 1—Computer Facility Operations Layout

The person trap must conform to the egress/access requirements documented in Section 760-630-300.

E. Emergency Devices

3.22 ***AC Protection Equipment:*** Protected ac power equipment for computers along with guidelines for data processing centers and clusters of Operations Support Systems, which were published in GL 77-08-178 and GL 77-04-087 are discussed in Section 790-100-660. In addition, Section 790-100-660 includes a list of OSS (and associated air conditioning) for which standby engine-alternators are recommended to meet the desired objective during emergencies. (See GL 78-05-173.) The various types of ac protection available are listed below.

(a) ***Impulse Suppressors:*** High voltage impulses that could degrade computer performance may be mitigated through the use of relatively inexpensive devices, commonly called "transient suppressors" or " lightning arrestors." These devices should be installed at strategic points to absorb the impulse energy so that the generated voltages and currents do not exceed damage levels to the equipment.

(b) ***Dual Power Feeds:*** Dual power feeds can be provided by the serving utility from two separate substations. It should be provided by utilizing two separate transmission lines on separate poles (if aerial cable is used). In the event that one substation or transmission line fails, the other should be available.

(c) ***Standby Engine Alternators:*** Diesel (or turbine) alternators provide long-term, backup power in the event of total loss of commercial service. These alternators are used in a standby mode and may require up to several minutes to start up and come on-line. Hence, they provide no protection against disturbances other than long-term brownouts and blackouts. Fire protection should be provided in accordance with Section 760-610-400.

(d) ***Line Voltage Regulator (LVR):*** There are many devices currently available in this category of ac protection. These devices are sometimes called "line conditioners," "ac regulators," "line regulators," "constant voltage transformer," "line voltage regulators," and "isolation transformers." Since the performance of these devices varies, depending on the manufacturer, the local engineering group in charge of power should make the final decision as to the device to be used. The primary use of this equipment is to regulate sags, surges, and brownouts on the commercial ac service.

(e) ***Uninterruptible Power Supplies (UPS):*** This system consists of a battery reserve, an inverter (dc-ac), and a rectifier which are used to supply sufficient power to the critcal load and recharge the batteries. Usually, the battery reserve is sized to provide power for 15 minutes. If longer protection is desired, the UPS is used in conjunction with an engine-alternator (rather than more batteries to the UPS) to power the computer system plus the air conditioners and/or water chillers needed to maintain a long-term environment. The arrangement of engine-alternator plus UPS represents the ultimate in ac protection; however, it is the most expensive and should not be implemented without adequate evaluation.

3.23 ***Emergency Lighting:*** The emergency lighting units which include exit markers of sufficient intensity to illuminate the computer facility for access to the exits in the event of an emergency shall be installed in accordance with Section 802-015-158. This may be accomplished by means of automatic special battery-operated lighting units if emergency power is not available.

3.24 ***Air Conditioning Redundancy:*** Critical operations will require standbys for all operating components of the air conditioning system, or the equivalent thereof. A critical operation is one in which the computer units must operate continuously or severe hardships will be experienced and/or an air conditioning failure could cause residual damage to the computer components which cannot be tolerated. A second alternative would be to provide cross-connections between the air conditioning unit in the computer facility and the unit used to cool the building properly so that if the air conditioning unit for the computer facility fails, the other unit can be used as a backup.

3.25 ***Chilled Water Redundancy:*** The refrigeration cycle must be selected with sufficient standby or spare facilities to maintain operations when any one of the primary unit components become inoperable. Standby equipment should be controlled so that upon the failure of

the primary unit, automatic transfer is achieved with proper alarming. The following recommendations for chilled water redundancy are taken from GL 70-07-236 which should be referenced for additional details.

(a) Two refrigeration units of 100 percent capacity, two pumps and tower cells similarly sized, and two chilled water pumps.

(b) Three refrigeration units, each at 50 percent capacity, three pumps and tower cells similarly sized, and three chilled water pumps.

(c) Where a winterized refrigeration system serving other building systems is available, an acceptable alternate to (a) and (b) above is the installation of one refrigeration unit and auxiliaries sized for the computer system installation with condenser water and chilled water cross-connections to the existing winterized system (assuming that the existing system has sufficient capacity). With such an arrangement, the refrigeration plant sized for the computer installation would be the lead unit with the existing winterized system used as an alternate.

3.26 ***Air Conditioning Dampers:*** It is recommended that the air conditioning unit for the computer facility be designed to contain dampers that would close automatically in the event of a smoke or fire emergency. The purpose of the dampers is to prohibit the spread of fire or smoke through the air conditioning ducts. Refer to Section 760-640-110 for additional information.

3.27 ***Floor Lifters:*** It is required that a minimum of two floor lifters be located in the computer facility. The floor lifters should be conspicuously mounted and designated for fire emergency use. (Refer to Section 760-250-100.)

3.28 ***Master Disconnect Switch:*** A master disconnect switch should be provided as part of the main service wiring, controlled from a location readily accessible to the main control panel and the exit doors. This master power control, when activated, disconnects the power to all electronic equipment in the computer facility and to the air conditioning system servicing that area.

F. Perimeter Protection

3.29 ***Perimeter Lighting:*** The perimeter of the building and the parking area should contain sufficient lighting to provide for the safety of the employees during off-tour hours and also to discourage attempted intrusion by outside sources.

3.30 ***Perimeter TV Surveillance:*** TV surveillance should be considered to augment the guard service in monitoring the perimeter of the building. The monitors for the TV surveillance should be located in a security area occupied at all times.

3.31 ***Perimeter Fencing:*** If the area surrounding the building is too large to effectively secure with lighting and TV surveillance, consideration should be given to enclosing the perimeter with fencing. The access/egress opening of the fencing should meet the local fire regulations.

G. Communication

3.32 ***Multiple Feeder Routes:*** In computer facilities that rely heavily on teleprocessing equipment for the transmission or receiving of data or on-line processing, it is recommended that the communications network be designed to include multiple feeder lines with sheath and route diversity for data lines. The internal distribution of communication lines or cables should not be routed through or near volatile material storage areas (ie, paint lockers, etc).

4. PROTECTION BY PROCEDURES

4.01 This part contains the procedures necessary to control access to the building and computer facility, provide personnel security, and institute protective measures to enhance the overall physical security program.

4.02 The procedures contained in this part are the foundation from which the other areas of physical security achieve their effectiveness. It is recommended that they be implemented and closely monitored.

A. Access Controls—Building

4.03 ***Employee Identification:*** Upon entering the building, employees must present their company identification to the security guard or

company-appointed representative. Employees not possessing their company identification will not be admitted to the building until they have completed the employee register as discussed in paragraph 4.04. It may also be advisable to require that all employees associated with the computer facility have their company identification visible at all times.

4.04 ***Employee Register:*** Employees not having their company identification in their possession, as well as employees entering the building during nonscheduled hours, should record their entry and exit in the employee register under the supervision of a security guard or management personnel. Employees not having their company identification in their possession should be required to sign in by a management level person and assigned a temporary pass (to be returned upon exit).

4.05 ***Visitor Register:*** The entry and exit of visitors (people who do not normally work in the building or computer facility or vendors who are assigned to the facility) should be recorded in the visitor register. The proper recording and monitoring of all visitors are mandatory if successful access controls are to be implemented.

4.06 ***Visitor Badges:*** All visitors should be required to wear badges that are clearly visible at all times. The assigned badge number should be entered in the visitor register opposite the entry for each visitor. This will aid in the control of the badges and assure that all visitors are accounted for upon departure. It is advisable to consider the use of color-coded badges that would indicate the areas of the building the visitor would be allowed to access.

4.07 ***Visitor Escorts:*** Nonemployee visitors should not be allowed access to any portion of the building or computer facility unless they are escorted by an authorized Bell System employee. Employees are expected to question unescorted visitors as to their purpose for being in the building or the computer facility. All such occurrences should be reported to either supervision or security immediately.

4.08 ***Package Control:*** All packages entering and leaving the building will be subject to inspection by the security guard. Employees or visitors attempting to remove either company or personal property from the building will be required to obtain a package or material removal pass that has been approved by an appropriate level of management, consistent with the local security practices. Refer to GL 77-03-043 for more details.

4.09 ***Security Guards:*** These guards should be stationed at any entrance to the building where the normal flow of traffic, both employees and visitors, will pass. They should also be stationed in areas, such as loading docks, where access to the building could be obtained. Additional information concerning the responsibility of the security guards should be obtained from the local security group.

B. Access Control—Computer Facility

4.10 ***Authorization:*** Employees or resident customer engineers that are directly responsible for the daily operation of the computer facility should be the only persons granted access authorization to the computer facility. All other access authorization should be granted on a need-to-enter basis. Company employees that are not regularly assigned to the computer facility will not be granted automatic admission. They will be required to justify their reason for entering and will be subject to the normal controls placed on visitors.

4.11 ***Distribution of Access Devices:*** The distribution and monitoring of access devices such as card keys, keys for locks, combinations for locks, etc, will be the responsibility of the organization accountable for the individual computer facilities. These devices should be issued only to those persons directly responsible for the daily operation of the computer facility. Temporary access devices will be issued at the discretion of the responsible organization.

4.12 ***Visitor Register:*** All visitors (those employees who do not work in the computer facility or persons visiting the computer facility) will be required to record their entry and exit as well as any other information deemed necessary for security purposes in the computer facility visitor register. It will be the responsibility of the organization in charge of the computer facility to ensure that all visitors are recorded in the register and that all entries have been verified.

4.13 ***Visitor Badges:*** It is recommended that a computer facility visitor badge be issued

to any noncomputer facility employee or visitor who has completed the visitor register and has been granted permission to enter the computer facility. The badge should be a distinctive color and be clearly visible at all times.

4.14 ***Visitor Escorts:*** Visitors or noncomputer facility employees should not be allowed to enter the computer facility unless accompanied by an escort. The escort will accompany the individual to the desired destination, ensure continued escorting throughout the visit, and accompany visitor from the computer facility upon completion of the task.

4.15 ***Tours:*** It is recommended that tours of the computer facility not be conducted. However, if they must be conducted, the number of people in the tour should be kept to a manageable size (five to seven people). They will be subject to the normal rules placed on visitors.

4.16 ***Vendors:*** The two types of vendors having access to the computer facility are:

(a) ***Temporary Vendors:*** These vendors are not permanently assigned to the computer facility and therefore not a part of the day-to-day operation. They will be subject to the normal controls placed on visitors with the exception that they may be temporarily assigned an access device to help expedite their assignment.

(b) ***Resident Vendors:*** These vendors are permanently assigned to the computer facility and are a necessary part of its daily operations. They should be issued a temporary access device in exchange for their company identification at the beginning of their tour. Upon return of the temporary access device, their company identification will be returned. This access should be restricted to only those areas where the equipment they are servicing is located. The resident vendors should not be allowed to sign in any visitors or vendors.

C. Personnel Security

4.17 ***Personnel Screening:*** A security background investigation should be made (as permitted by law) on all new hires, transferees, and contracted services (security guards and house services) for jobs which involve unsupervised access to computer hardware or software which could result in severe damage to the computers or compromise of proprietary information. It is the responsibility of the Employment staff and the Security Organization to conduct the investigations on candidates for jobs that have been designed as requiring screening.

4.18 ***Termination Procedures:*** When considering the dismissal of an employee, the supervisor should closely monitor the employee's access to critical records or procedures until separation occurs. When an employee has been notified of dismissal, access to the computer facility should no longer be permitted, Vendors should notify the organization responsible for the computer facility when an employee who is associated with the computer facility has either resigned, being considered for termination, or has been terminated. In cases of impending employee termination, it may be determined that the employee should be immediately excluded from the computer facility in the interest of security. If transfer to another assignment is not practical, consideration should be given to paying the employee for the notice period and releasing the individual. A disgruntled employee who has notified management of intent to resign should be treated in the same manner.

4.19 ***Rotation of Employees in Sensitive Positions:*** Strong consideration should be given to rotation of employees in sensitive or high pressure type positions into areas where the sensitivity and pressure are lessened. When employees are rotated, any passwords, keys, access cards, etc, associated with the employee should be changed or deleted. The advantages of such rotations are threefold:

(1) It reduces the risk of employee fraud.

(2) It allows the employee who has been under constant pressure to unwind.

(3) It can be used to train employees so they can become more flexible in their assignments and also create a backup for those positions.

4.20 ***Job Design:*** Jobs assignments within the computer facility should be designed so they are self-checking. The last step of one assignment should be the first step of the next assignment. This would ensure that the end result of the first assignment is correct and would help to reduce the cost of rerunning jobs. It would also reduce the probability of one employee being

able to defraud the company since two people would be involved with the task.

4.21 ***Conferences:*** It is strongly recommended that periodic employee/management conferences be scheduled. The purpose of these conferences would be to determine if the morale level among the computer facility employees is satisfactory and also to allow the employees to interject their comments concerning the computer facility.

4.22 ***Vacation Schedules:*** Vacation schedules should be monitored to ensure that all employees take vacation. Many types of fraud require that the individual responsible be present at all times. Vacation monitoring will help to protect against this type of fraud.

D. General Considerations

4.23 ***Media Security:*** Media being rotated off-site should be packaged in containers designed to resist heat, mositure, dust, shock, and any other potentially hazardous condition. The media should not be exposed to any potential danger such as X rays or magnetic fields that could destroy or damage the data residing on the media. Procedures must be instituted to ensure the protection of media in transit and at the off-site storage facility such as:

(a) Managerial trails that monitor the shipment of media from the computer facility to the off-site storage location.

(b) Inventory checks at the off-site storage location to ensure that the media can be accounted for and is properly protected.

(c) Media tests that would ensure the readability of the magnetic media (tapes and disks).

E. Protective Measures

4.24 "No Smoking" signs shall be posted conspicuously throughout the computer facility, in the tape library, storage areas, and any other areas within the computer facility or nearby areas that open into the facility.

4.25 Food or drink should not be allowed in the computer facility or any associated areas.

4.26 The quantity of paper, unused magnetic tapes, recording media, or any other combustible items that may be needed in the computer facility should be kept to an absolute minimum. All recording media and supplies should be stored in external areas until needed.

4.27 Cleaning of the air conditioning ducts and under the raised flooring should be periodically scheduled. This will prevent a buildup of dust or any other potentially hazardous substances in these areas.

4.28 Inspection and testing of the detection and suppression devices should be conducted on a periodic basis to ensure that they are functioning properly.

4.29 Carpet is not recommended for use in the computer facility. However, existing carpets or carpets to be installed shall meet the requirements specified in Section 760-610-200.

4.30 All furniture, fixtures, and interior finishes must be of noncombustible materials as outlined in Section 760-610-200.

4.31 Inspection and testing of the emergency backup systems (air conditioning, chilled water, UPS, and engine-alternator) must be conducted on a regularly scheduled basis. Normal computer facility operations should not be interrupted during these tests.

4.32 Magnetic, electromagnetic, and flash devices (magnets, walkie-talkies, flashbulbs, 2-way radios, etc) should not be permitted in the computer facility (GL 78-02-019). Exposure to the interference emitted by these sources may adversely affect the processing equipment and magnetic storage media.

4.33 Fire protection floor plans should be developed in accordance with Section 760-660-100.

4.34 Computer facilities are required to establish a Firesafety Organization as described in Section 770-300-200.