

**COMPUTER CENTER PHYSICAL SECURITY AND DISASTER RECOVERY  
 PHYSICAL SECURITY EVALUATION**

	<b>CONTENTS</b>	<b>PAGE</b>
<b>1.</b>	<b>GENERAL . . . . .</b>	<b>1</b>
<b>2.</b>	<b>SURVEY . . . . .</b>	<b>2</b>
	<b>EXPOSURE TO FIRE HAZARDS . . . . .</b>	<b>2</b>
	<b>WATER HAZARD/DAMAGE EXPOSURE . . . . .</b>	<b>12</b>
	<b>AIR CONDITIONING CONSIDERATIONS . . . . .</b>	<b>13</b>
	<b>ELECTRICAL CONSIDERATIONS . . . . .</b>	<b>15</b>
	<b>PREPARING FOR CIVIL, MAN-MADE, AND NATURAL DISASTERS . . . . .</b>	<b>17</b>
	<b>ACCESS CONTROL CONSIDERATIONS . . . . .</b>	<b>19</b>
	<b>HOUSEKEEPING . . . . .</b>	<b>28</b>
	<b>OTHER FACILITY CONSIDERATIONS . . . . .</b>	<b>29</b>
	<b>PERSONNEL . . . . .</b>	<b>30</b>
	<b>TRAINING ORIENTATION . . . . .</b>	<b>31</b>
	<b>OPERATING PROCEDURES . . . . .</b>	<b>32</b>
	<b>TAPES AND/OR DISKS . . . . .</b>	<b>33</b>
	<b>FILES, DOCUMENTATION, AND DATA . . . . .</b>	<b>34</b>

**1. GENERAL**

**1.01** This aid has been developed by a multicompany GUARDSMAN project team under the direction of AT&T Information Systems Technical Support and Standards. This aid is issued by the AT&T Director—Information Systems Planning and Support for implementation by Bell System Companies.

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

**1.03** As referenced in Section 007-590-302, the purpose of this section is to provide a tool for evaluating the present physical security system in each computer facility. All questions should be answered with "Yes," except where indicated by a double asterisk (\*\*). "No" answers indicate weaknesses or potential weaknesses in existing security systems and should be investigated. On the question marked by \*\*, the correct answer is "No." A "Yes" answer would indicate a weakness or potential weakness in existing security systems.

**NOTICE**

Not for use or disclosure outside the  
 Bell System except under written agreement

**SECTION 007-590-400**

**2. SURVEY**

**EXPOSURE TO FIRE HAZARDS**

**A. Construction**

	<b>YES</b>	<b>NO</b>
1. Is the computer housed in a building constructed of fire-resistant and noncombustible materials?	_____	_____
2. Is the subflooring concrete or noncombustible with positive drainage?	_____	_____
3. Is the raised flooring constructed of aluminum or other noncombustible material?	_____	_____
4. Is the underfloor cabling channeled through conduits?	_____	_____
5. Is the floor tile nonpetroleum based?	_____	_____
6. Are the walls and trim noncombustible and painted with water-based, fire-retardant paints?	_____	_____
7. Are doors, partitions, and framing made of noncombustible materials?	_____	_____
8. Is all glass of the steel-mesh or reinforced type?	_____	_____
9. Is the ceiling tile made of noncombustible materials (including supports)?	_____	_____
10. Are cables connecting ceiling lights placed in conduits?	_____	_____
11. Has sound-deadening materials (on walls, in cabinets, or around desks and operating positions) been sprayed with fire-retardant chemicals? (Foamed cellular plastics should never be used.)	_____	_____
12. Is the position of the computer facility in an area away from potential hazards such as fire, cafeterias, power cabling, rubbish storage, caustic chemicals, fumes, odors, etc?	_____	_____
13. Have steam lines been removed from the proximity of the computer facility?	_____	_____
14. Is the computer facility near areas employing hazardous processes?***	_____	_____
15. Have hazards been removed from the immediate surrounding area?	_____	_____
16. Are the computer facility and the supporting facilities separated sufficiently by fire-resistant materials to prevent fire in one area from affecting other areas:		
(a) Tape or disk libraries?	_____	_____
(b) Paper or card storage?	_____	_____
(c) Backup files?	_____	_____
(d) Source decks?	_____	_____
(e) Source listings?	_____	_____

	YES	NO
(f) Supporting operating facilities?		
(1) Alternate computing facilities?	___	___
(2) Punch card processing facilities?	___	___
(3) Remote job entry facilities?	___	___
(4) Customer engineer facilities?	___	___
(g) Copies of operations procedures?	___	___
(h) Copies of control procedures?	___	___
(i) Forms handling equipment?	___	___
(j) Report distribution facilities?	___	___

**Note:** Certain facilities may be located far apart and yet be subject to interpropagation via cable routing through vertical cable chases.

17. Are the facilities housing the activities listed in 16 above constructed of fire-resistant and noncombustible material?	___	___
18. If a fire were to occur in a computer facility, would other offices of the business be disabled as well?*	___	___
19. Are computer room walls extended above the false ceiling to the roof?	___	___
20. Is there sufficient room between units to permit free airflow and heat dissipation?	___	___
21. Does the construction of the facilities permit distribution of detection sensors and extinguishing systems?	___	___
22. Are exits and fire evacuation routes clearly marked?	___	___

**SECTION 007-590-400**

**B. Combustibles**

	<b>YES</b>	<b>NO</b>
1. Are paper and other supplies stored outside the computer area?	_____	_____
2. Are curtains, carpets, furniture, and drapes fire-retardant treated or noncombustible?	_____	_____
3. Are caustic or flammable cleaning agents permitted in the computer facility?*	_____	_____
4. If flammable cleaning agents are permitted in the computer facility, are they kept in small quantities and in approved containers.	_____	_____
5. Is the quantity of combustible supplies stored in the computer facility kept to the minimum?	_____	_____
6. Is the space beneath the access flooring used for storage of class A combustible materials such as data processing (DP) cards?***	_____	_____
7. Is subfloor volume cleaned regularly?	_____	_____
8. Is all furniture of metal construction?	_____	_____
9. Are copies of listings and card decks kept in the computer facility?	_____	_____
10. Are clothing racks stored in the computer facility?	_____	_____
11. Are there excess tapes, disks, or cards in the computer facility?***	_____	_____
12. Is paper-bursting and shredding equipment kept away from the computer facility?	_____	_____
13. Is report distribution and forms handling equipment kept away from the computer facility to keep dust to a minimum?	_____	_____
14. Are computer facility safes closed when not being accessed?	_____	_____
15. Are loose pieces of plastic (such as tape rings, disk covers, tape covers, empty tape reels) kept out of the computer facility?	_____	_____
16. Does "decoration" of the computer facility with posters, company literature, graffiti, or holiday decoration meet the requirements of Section 760-610-200?	_____	_____

**C. Storage**

	YES	NO
1. Are critical files "backstopped" with current copies in fireproof safes or remote facilities?	_____	_____
2. Could the last several days processing be recaptured with copies of files and transactions remotely located?	_____	_____
3. Is the number of tapes outside the tape library kept to a minimum at all times?	_____	_____
4. Are data safes located in a separate fire hazard area other than the tape library?	_____	_____
5. Are disk pack storage cabinets fitted with casters to aid in emergency evacuation?	_____	_____
6. Are tape storage racks fitted with casters to aid in emergency evacuation?	_____	_____
7. Are there obstructions (risers, width of doorway, etc) that prohibit the evacuation of storage racks? **	_____	_____
8. Is there a wall in the tape library to secure tape racks and other equipment?	_____	_____
9. Have all source decks been copied to tape and stored in the data safe?	_____	_____
10. Are all of the user department's card files removed from the computer facility?	_____	_____
11. Is there a data safe located in a remote area away from the computer facility for backup protection?	_____	_____
12. Are cabinets housing card decks stored away from the computer area?	_____	_____
13. Have alternate storage facilities been selected?	_____	_____
14. In case of emergency, is transportation scheduled to move files?	_____	_____

D. Detection Equipment

YES NO

- 1. Do the facilities have one or more of the following:
  - (a) Smoke detection equipment?\*
  - (b) Humidity control equipment?
  - (c) Thermocouple detectors?
- 2. Are any of these detection units mounted *inside* the cabinets of critical system components?
- 3. Are smoke detectors installed:
  - (a) In ceiling?
  - (b) Under raised floor?
  - (c) In air return ducts?
  - (d) In the compartment?
- 4. Are smoke detectors properly engineered to function in a computer facility?
- 5. Are detection systems tested on a scheduled basis?
- 6. Are smoke and fire detection systems connected to the plant security panel and municipal police departments?
- 7. Are underfloor smoke detector heads identified by hanging markers in the computer facility ceiling?

\*Specifically recommended by NFPA.

**E. Alarm Mechanism**

	YES	NO
1. Do the facilities listed in A through D above provide alarm mechanisms, such as automatic alarming upon detection of fire (light), smoke, or inordinate heat rise?	_____	_____
2. Are there several manually operated alarm systems located strategically throughout the facility?	_____	_____
3. Does the alarm device report the location of the fire to a centralized or municipal fire or security position?	_____	_____
4. Does the alarming mechanism contain automatic shutdown of critical equipment? (Particularly required with sprinkler systems.)	_____	_____
5. Is there a smoke detector alarm horn in a central location in the computer room?	_____	_____
6. Does the alarm sound:		
(a) Locally?	_____	_____
(b) At watchman stations?	_____	_____
(c) At central station?	_____	_____
(d) At fire department or police headquarters?	_____	_____

F. Protection Equipment

	YES	NO
1. Do the facilities have one or more of the following:		
(a) Automatic dispersal of a fire extinguishing or retardant agent, such as:		
(1) Gas-Halon 1301 (above and beneath floors and ceilings)? Have personnel been trained both in the use of the gas and personal safety measures?	_____	_____
(2) Foam?*	_____	_____
(3) Water (last resort)?		
• Wet pipe (releases water at a set temperature)?	_____	_____
• Preaction (may sound an alarm and delay release of water)?	_____	_____
(4) Fixed flooding systems?	_____	_____
(b) Manual equipment, such as:		
(1) Portable extinguishers for electrical and other fires?	_____	_____
(2) Are portable fire extinguishers located strategically around the area with location markers clearly visible over computer equipment?	_____	_____
(3) Water or other extinguishing agent for nonelectrical fires?	_____	_____
(4) Are extinguishers located throughout the facilities where they can be easily obtained within a few steps?	_____	_____
2. Automatic and/or delayed interruption of power sources where electric fires have been discovered?	_____	_____
3. Automatic shutdown of air conditioning systems (particularly where Halon 1301 is used)?	_____	_____
4. Automatic shutdown of heating or humidity systems?	_____	_____
5. Automatic close off of air ducts?	_____	_____
6. Automatic illumination of emergency lighting on interruption of the prime power source?	_____	_____
7. Automatic sealing of firebreaks or fire doors between sections of the facility?	_____	_____
8. Are there any fire suppressant outlets mounted <i>inside</i> the cabinets of critical system components?	_____	_____
9. Is there a means of manually activating an automatic system?	_____	_____
10. Are automatic devices "rate compensated" to allow for sudden increases in temperature?	_____	_____

- |   | YES   | NO    |
|---|-------|-------|
| 11. Does emergency power shutdown include the air conditioning system?  | _____ | _____ |
| 12. If a total flooding fire protection system is installed, does it have a manual override abort capability? | _____ | _____ |

\*Not recommended by NFPA.

**SECTION 007-590-400**

**G. Reaction Planning**

	<b>YES</b>	<b>NO</b>
1. Have building engineers analyzed the fire detection system to ensure that the number and location of detectors are appropriate for the <i>current</i> configuration?	___	___
2. Is there around-the-clock watchman coverage during nonworking hours?	___	___
3. Do procedures exist to "rearm" any fire prevention equipment?	___	___
4. Does the construction of the facilities permit easy access by fire-fighting personnel and equipment?	___	___
5. If access is through an electrically controlled system, can it be operated by standby battery power?	___	___
6. Are emergency power shutdown controls easily accessible at points of exit?	___	___
7. Can emergency crews gain access to the computer room without excess delay even during off shifts and holidays?	___	___
8. Are additional floor panel removers installed adjacent to fire extinguishers?	___	___
9. Have locations been identified and have personnel been informed of and provided instruction on the operation of the sprinkler shutoff valve for annexes, computer operations, and data entry?	___	___
10. Does the fire department know the location of both the computer room and flashing red lights or other alarm devices? Is there a reception area that contains indicators of alarm conditions in the computer facility?	___	___
11. Is there a battery-powered megaphone available, and are personnel knowledgeable of its location and operation?	___	___
12. Are fire drills held regularly?	___	___
13. Are operators trained periodically in fire-fighting techniques and assigned individual responsibilities in case of fire?	___	___
14. Is the no-smoking prohibition in the computer room and tape library strictly enforced?	___	___
15. Is there a documented Disaster and Security Plan?	___	___
16. Is there an area "Fire Warden" appointed?	___	___
17. Is the alarm tested regularly?	___	___
18. Are there "simulated" disasters to exercise an evacuation plan?	___	___
19. Is a fire inspection conducted periodically by organizational or municipal fire officers?	___	___
20. Are fire and evacuation plans easily available and reviewed periodically with the staff?	___	___

- |   | YES   | NO    |
|---|-------|-------|
| 21. Is the use of incendiaries controlled within the facilities?  | _____ | _____ |
| 22. Is there a regular inspection by qualified personnel of all automatic detection and protection systems? | _____ | _____ |

**SECTION 007-590-400**

**WATER HAZARD/DAMAGE EXPOSURE**

**Physical Location**

**YES**      **NO**

- 1. Are computers excluded from areas below grade? \_\_\_\_\_
- 2. If not, have sufficient sealing and foundation draining devices been included? \_\_\_\_\_

**A. Within the Facility**

- 1. Are overhead steam or water pipes (except sprinklers) eliminated? \_\_\_\_\_
- 2. Is there sufficient drainage under the raised floor to remove accumulated liquid quickly? \_\_\_\_\_
- 3. Are drains installed on floor above the facility to divert accumulated water from all hardware? \_\_\_\_\_
- 4. Is the upper ceiling constructed so as to conduct water from higher levels away from the computer facility? \_\_\_\_\_
- 5. Is the floor above the facility watertight? \_\_\_\_\_
- 6. Are the pipe and wire openings watertight? \_\_\_\_\_
- 7. Is there adequate drainage to prevent water overflow from adjacent areas? \_\_\_\_\_
- 8. Is an industrial-type vacuum cleaner (one that will pick up water) readily available to computer facility? \_\_\_\_\_
- 9. Is there a dispenser for tarpaulins (tarps) to be used for covering the hardware in the event the sprinkler heads discharge? \_\_\_\_\_
- 10. Are all electrical junction boxes under the raised flooring held off the slab to prevent water damage? \_\_\_\_\_
- 11. Are there sufficient ducts to conduct water used in air conditioning systems away from the building? \_\_\_\_\_

**B. Outside the Facility**

- 1. Is the roof sufficiently sealed to prevent opening and subsequent leakage caused by wind damage? \_\_\_\_\_
- 2. Is there protection against accumulated air conditioning water or leaks in rooftop water towers? \_\_\_\_\_
- 3. Are exterior windows and doors watertight? \_\_\_\_\_
- 4. Is grading around the exterior of the facility constructed to conduct water away from the building? \_\_\_\_\_
- 5. Are there sufficient storm drain inlets to accommodate water accumulation during sudden or seasonal rainfall? \_\_\_\_\_
- 6. Have subterranean or underroof heating systems been installed to melt snow? \_\_\_\_\_

**AIR CONDITIONING CONSIDERATIONS**

**A. Air Conditioning Facility**

YES NO

- 1. Are the BTU ratings of air conditioning equipment appropriate for the facility?
- 2. Is the air conditioning system used exclusively for the computer area?
- 3. Is there a backup air conditioning capability?
- 4. Is the compressor remote from the computer facility?

**B. Intakes, Ducting, and Piping**

- 1. Are duct linings and filters noncombustible?
- 2. Are air intakes:
  - (a) Covered with protective screening?
  - (b) Located well above street level?
  - (c) Located so as to prevent intake of pollutants or other debris?
- 3. Could ducting carry fumes and smoke to other offices? \*\*

**C. Shutdown**

- 1. Are there alternate locations in the computer facility area where all power and air conditioning fans for the area can be shut off?
- 2. Can installed ceiling exhaust fan(s) provide sufficient air movement should the air conditioning system become inoperable for several hours?

**D. Protection**

- 1. Is the cooling tower fire protected?
- 2. Are sensors installed within the air conditioning system?
- 3. Does the construction of the air conditioning facilities permit only authorized access, including:
  - (a) Placement in high place to restrict access?
  - (b) Protection of the water supply source?
  - (c) Protection of fan or cooling mechanisms?
  - (d) Survey of air conditioning area by closed circuit television?
  - (e) Periodic check by security personnel?

**SECTION 007-590-400**

**YES**      **NO**

4. Do security personnel have copies of wiring, ducting, water, and air flow diagrams for use by maintenance or fire-fighting personnel?

\_\_\_\_\_

5. Is there heat or humidity control equipment?

\_\_\_\_\_

6. Are there temperature and humidity monitoring and recording devices?

\_\_\_\_\_

**ELECTRICAL CONSIDERATIONS**

**A. Power Supply**

- |   | YES   | NO    |
|---|-------|-------|
| 1. Is the local electrical power reliable?  | _____ | _____ |
| (a) Is there sufficient amperage to support the facility when all equipment is operating?   | _____ | _____ |
| (b) Is the power supply susceptible to:   |       |       |
| (1) "Blackouts"?**  | _____ | _____ |
| (2) Reduced operating voltages?**   | _____ | _____ |
| (3) Surges or power "spikes"?**   | _____ | _____ |
| (c) If electrical power is unreliable, have alternate power sources been investigated?  |       |       |
| (1) Secondary sources?  | _____ | _____ |
| (2) Standby generators?   | _____ | _____ |
| (d) Is the voltage input monitored with a recording voltmeter that displays changes?  | _____ | _____ |
| 2. Does the data center have a devoted power system? (The source of power should not connect to other parts of the organization.) | _____ | _____ |
| 3. Is there an alternate power source that permits resumption of operation if the prime power source is destroyed?                | _____ | _____ |
| 4. Is needed air conditioning connected to this alternate source?   | _____ | _____ |

**B. Wiring**

- |  |       |       |
|--|-------|-------|
| 1. Is wiring in conformance with local building codes for the installation's class of service?   | _____ | _____ |
| 2. Do security and maintenance officials have a copy of the wiring diagram?  | _____ | _____ |
| 3. Are electrical boxes placed in areas not exposed to water or other potential damage?  | _____ | _____ |
| 4. Are the main power control boards in a remote or restricted access position?  | _____ | _____ |
| 5. Are there emergency power-off switches at each exit of the computer room to meet OSHA requirements?   | _____ | _____ |
| 6. Has all wiring under the raised floor in the computer facility been checked, assuring that all circuits (including 110 volt) are wired to shunt breakers and are properly grounded? | _____ | _____ |
| 7. Are all power panels supplying the computer facility locked?  | _____ | _____ |
| 8. Are all circuit breakers/fuses clearly labeled?   | _____ | _____ |

C. Lighting

	YES	NO
1. If there is an emergency lighting system, has it been recently tested?	_____	_____
2. If the system has fixed position lamps, have they been tested to determine if they illuminate the proper area?	_____	_____
3. Are there sources of light, strategically located, that do not depend upon the main power source?	_____	_____
4. Is there an emergency power source to energize emergency lighting?	_____	_____
5. Are the office lights wired to provide a security night-light?	_____	_____
6. Have emergency lights for the computer facility, annex, and data entry area been installed?	_____	_____

**PREPARING FOR CIVIL, MAN-MADE, AND NATURAL DISASTERS**

**A. Location**

	YES	NO
1. Is the facility remote from any earthquake fault?	_____	_____
2. Is the facility located in a riverbed or floodplain?***	_____	_____
3. Is the facility close to high voltage transmission lines?***	_____	_____
4. Is the facility close to heavily traveled highways?***	_____	_____
5. Is the facility close to rail lines?***	_____	_____
6. Is the facility close to fuel storage containers?***	_____	_____
7. Is the facility close to fuel or steam transmission lines?***	_____	_____
8. Is the facility close to an isolated metal structure that might draw lightning?***	_____	_____
9. Is the facility located in a high crime area?***	_____	_____
10. Have there been reports of local civil unrest vis-a-vis computer facilities?***	_____	_____
11. Is the facility in an area of high fire potential?***	_____	_____
12. Is the facility close to an airport?***	_____	_____
13. Is the facility close to the storage or processing of toxic or caustic chemicals?***	_____	_____
14. Is the facility located in an area of dense trees or other tall foliage?***	_____	_____
15. Is the facility located in an area where flora is allowed to dry, ripen, or compost?***	_____	_____
16. Would disasters occurring in adjacent structures have a deleterious effect on your facility?***	_____	_____
17. Is the facility located where problems with small animals and/or rodents might occur?***	_____	_____

**B. Construction**

1. Is the building structurally sound:		
(a) To resist windstorms and hurricanes?	_____	_____
(b) To resist flood damages?	_____	_____
(c) To resist earthquakes?	_____	_____
2. Are building and equipment properly grounded for lightning protection?	_____	_____
3. Is the building on a solid foundation?	_____	_____

**SECTION 007-590-400**

**YES**      **NO**

4. Is the building constructed so as to be "defensible" in the case of civil unrest?      \_\_\_\_\_      \_\_\_\_\_

**C. Natural Disaster Prediction**

1. Are there some means to advise personnel of possible natural disaster?      \_\_\_\_\_      \_\_\_\_\_

2. Is there a series of contingency steps that are invoked when a natural disaster advisory is received?      \_\_\_\_\_      \_\_\_\_\_

**D. Man-Made Disaster Prediction**

1. Will appropriate personnel be notified in the case of a nearby disaster, such as fire in adjacent buildings?      \_\_\_\_\_      \_\_\_\_\_

2. If the facility is in the flight path of an airport, will appropriate personnel be notified of potential aircraft difficulty?      \_\_\_\_\_      \_\_\_\_\_

**ACCESS CONTROL CONSIDERATIONS**

**A. Identification**

- |   | YES   | NO    |
|---|-------|-------|
| 1. Is advertising the location of this computer facility discouraged?   | _____ | _____ |
| 2. Is access to the computer area restricted to selected personnel?   | _____ | _____ |
| 3. Is there a photo-badge system for positive identification of employees?                                    | _____ | _____ |
| 4. Do mechanisms exist to ensure that the person is carrying his/her own badge?                               | _____ | _____ |
| 5. Does the computer facility have a current photograph of every person with legitimate access to the area?   | _____ | _____ |
| 6. Is a person admitted merely because he/she is known?***  | _____ | _____ |
| 7. Is a person admitted merely because he/she is accompanied by a known person?***                            | _____ | _____ |
| 8. In the case of temporary badges, is the badge matched against some other form of identification?           | _____ | _____ |
| 9. Are identification badges color-coded, facility-zoned, or marked to indicate security clearance or access? | _____ | _____ |
| 10. Are transient personnel checked <b>out</b> of as well as into the computer facility?                      | _____ | _____ |
| 11. Can anyone ask for and receive data files or reports?   | _____ | _____ |
| 12. If not, is there a procedure to ensure:   |       |       |
| (a) Security clearance of the individual relative to the files or reports sought?                             | _____ | _____ |
| (b) The "need to know" access permitted relative to the files or reports sought?                              | _____ | _____ |
| 13. Are <b>all</b> visitors challenged?   | _____ | _____ |
| 14. Are people free to carry <b>anything</b> in and out of the facility?***                                   | _____ | _____ |
| 15. Are food and beverages prohibited in the computer room?***  | _____ | _____ |

**B. Access Routes**

- |   |       |       |
|---|-------|-------|
| 1. Are there guards on all street entrances that lead to the computer area?                         | _____ | _____ |
| 2. Do hallways have false floors that could permit unauthorized access to the computer facility?*** | _____ | _____ |
| 3. Are accesses from stairways restricted or in any way controlled?                                 | _____ | _____ |
| 4. Are access routes to and from nearby offices controlled?   | _____ | _____ |
| 5. Are all exterior windows at or near street level covered with expanded metal grills?             | _____ | _____ |

**SECTION 007-590-400**

	YES	NO
6. In areas with a high crime rate, is there bulletproof glass?	_____	_____
7. Is there a "dumbwaiter" or freight elevator that could be used as an unauthorized access route?***	_____	_____
8. Is access controlled from a loading dock?	_____	_____
9. If the facilities have electrically operated doors, can they be opened manually if the power source is interrupted to gain unauthorized access?***	_____	_____
10. Is the computer facility screened so that it is not visible from the street?	_____	_____
11. If not, could access be gained through street level windows?***	_____	_____
12. Are the doors to the computer facility and annex locked during second shift, third shift, and weekends?	_____	_____
<b>C. Visitor Control</b>		
1. Is there a visitor control procedure?	_____	_____
2. Is there a computer room sign in/out log for visitors?	_____	_____
3. Are "temporary passes" numbered to permit control of the pass as well as the person using it?	_____	_____
4. Is there a procedure for returning and accounting for temporary passes?	_____	_____
5. Can temporary passes be duplicated easily?***	_____	_____
6. Are pass and access rules consistently enforced?	_____	_____
7. Can anyone who wants to see the data center do so upon request?***	_____	_____
8. Are vendor personnel allowed to "roam freely" because of their apparent vendor affiliation?***	_____	_____
9. Is the casual visitor eliminated by stopping organization executives from including the data center in a facilities tour?	_____	_____
10. Does someone accompany <b>all</b> visitors?	_____	_____
11. Are visitors excluded from sensitive areas of the facility?	_____	_____
12. Are visitors controlled under the suggestions for access contained in these guidelines?	_____	_____
13. Where sensitive data or files are concerned, is there <b>positive</b> security clearance for the visitor?	_____	_____

**D. Security**

	YES	NO
1. Is it possible for someone to access communications lines externally?***	_____	_____
2. Have identification markings been removed from power rooms, communications closets, etc?	_____	_____
3. Once open, do cabinet doors permit room for a person to work on the device?	_____	_____
4. Are there magnetic sensors in access doorways?	_____	_____
5. Are there security guards at data center accesses?	_____	_____
6. Are critical files "under lock and key," limiting the access?	_____	_____
7. Is there a periodic security check of all personnel?		
(a) Spot inspection under operation?	_____	_____
(b) Complete background investigation on hiring?	_____	_____
(c) Thorough investigation of all personnel with access to the data center?	_____	_____
8. Can all external doors be locked on command?	_____	_____
9. If there is a closed circuit television, is it monitored at all times?	_____	_____
10. Are there double-door arrangements that will "lock in" an intruder between them?	_____	_____
11. Are the security precautions the same at every entrance, including the loading dock?	_____	_____
12. Are plans and blueprints for the data center and other important areas controlled or restricted?	_____	_____
13. Is access to communication equipment, such as junction boxes, switching mechanisms, terminal outlets, etc, freely available?***	_____	_____
14. Are there restrictions on the introduction of camera or other photographic recording equipment in the data center?	_____	_____
15. Are there restrictions on the introduction of sound magnetic recording equipment, radios, or other electronic devices in the computer facility area?	_____	_____
16. Is metal detection equipment available? Is it used?	_____	_____
17. Is there a means to inspect parcels and other articles moved in and out of the data center?	_____	_____
18. Are there "alert" mechanisms for the summoning of security personnel?	_____	_____
19. Are there electric eye or proximity warning indicators positioned in infrequently used rooms or hallways?	_____	_____
20. Have self-closing mechanisms been installed on all internal doors?	_____	_____

**SECTION 007-590-400**

	YES	NO
21. Are internal doors and passageways free of all obstructions, including wedges?	_____	_____
22. Are internal aisles wide, straight, and free of obstructions?	_____	_____
23. Is all equipment positioned so that access doors open fully and freely?	_____	_____
24. Are there external walls and windows that permit easy access to a saboteur?*	_____	_____
25. Are monitoring devices connected to access doors, emergency exits, and windows for the computer room and annex, connected to the company security system?	_____	_____
26. Are master key locks removed from the exterior of emergency exits?	_____	_____
27. Are file areas segregated so that only specific individuals have access to them?	_____	_____
28. Are PLEXIGLAS* windows installed between the data entry area and the computer room and between the computer room annex and computer room to reduce the personnel traffic?	_____	_____
29. Are master controls for detection and suppression systems located outside the data center?	_____	_____
30. Are communication devices and equipment relative to the computer facility in a remote or restricted access area?	_____	_____
31. Is the computer room located in an inner core of the building and off the street floor and/or out of the basement?	_____	_____
32. If not, are the glass windows impact resistant and protected by steel bars, grills, or mesh screens?	_____	_____
33. Does the computer center have an automated access control system which provides a documented log (including employee identification, date, time, and location) of all authorized employees' entries and exits on a 24-hour basis?	_____	_____
34. Is this access control system designed to restrict entry to this particular building and/or to a particular room within this building on certain days and at designated times?	_____	_____
35. Does this access control system include a security buffer zone or mantrap which is located at the entrance of the computer center or computer room? (Small vestibule area with an interlock exterior door and interior door through which a person must pass to display proper identification and be relieved of any magnetic or radio frequency device before entering the computer center or computer room.)	_____	_____
36. Does the access control system automatically log, and/or signal by, alarm attempts of unauthorized entry (ie, use of invalid identification or entry card, unauthorized employee or nonemployee following an authorized employee through a restricted door, compromised intrusion alarm, etc)?	_____	_____
37. Are separate entrances used by personnel and delivery of supplies, packages, mail, etc?	_____	_____

\*Trademark of Rohm & Hass Co.

	YES	NO
38. Is a separate, specially constructed room utilized for receiving, inspecting, and opening of supplies, packages, mail, etc? Are incoming packages X-rayed?	_____	_____
39. Is there a material pass system for inspecting incoming and outgoing items, packages, etc?	_____	_____
40. Is the library or storage room for magnetic tapes and disks located adjacent to the computer equipment space?	_____	_____
41. If so, is the room adequately secured and is the entrance door equipped with the appropriate lock or other protective device, ie, card reader?	_____	_____
42. Are periodic inventories of the tapes and disks made by an assigned employee; are the results of the inventories documented and retained?	_____	_____
43. Are tapes regenerated periodically? (It is recommended that tapes be rewound annually and that 5 percent of the tapes be test read.)	_____	_____
44. Is a computer maintenance room located near the equipment area to provide on-site maintenance on the equipment?	_____	_____
45. Are locked cabinets and/or vaults used to store sensitive data files, backup files, associated operating procedures, and documentation?	_____	_____
46. Are company contractors, vendors, and/or consultants required to sign nondisclosure agreements which have been approved by the appropriate departments, including Legal?	_____	_____
47. Are the local police and fire department basically familiar with the construction and equipment within the center to take the appropriate action in cases of emergency?	_____	_____
48. Are all outside utility service entrances (ie, gas, electric, water, telephone circuits, etc), including control valves, meters, and terminals, constructed and located in a manner to prevent tampering or destruction?	_____	_____
49. Is the control principle of division of responsibilities and rotation of assigned personnel in various duties effectively used by computer center management personnel?	_____	_____
50. Has a background check been conducted on all personnel assigned to the computer center?	_____	_____
51. Are all personnel assigned to the computer center required to wear some prominent identification such as badges or special cards?	_____	_____
52. Have procedures, precautions, and/or techniques been established and implemented to prevent unauthorized access and to provide access control to the computer system and/or remote terminals? Are key locks utilized on data terminal keyboards? Are keys controlled?	_____	_____
53. Is someone at the computer center presently assigned the responsibilities of administering the security measures and procedures?	_____	_____

**SECTION 007-590-400**

- |   | YES   | NO    |
|---|-------|-------|
| 54. Has an emergency shutdown, evacuation, and restoration plan been formulated for each work shift?  | _____ | _____ |
| 55. Is there ever any occasion when only one person is in the computer room?***   | _____ | _____ |
| 56. Is all proprietary information material properly destroyed and/or erased prior to collection by public waste or trash collectors?   | _____ | _____ |
| 57. Are employees who handle extremely sensitive information and/or material on a daily basis required to sign a nondisclosure agreement which has been approved by the appropriate departments, including Legal? | _____ | _____ |
| 58. Are tapes transmitted via a secure packaging? If so, are company mail or vehicles used?   | _____ | _____ |

**Chain Link Fence:** If the perimeter of the computer facility is protected by a chain link fence, the following items should be considered.

- |  |       |       |
|--|-------|-------|
| 59. Is the fence constructed of adequate gauge wire, generally No. 11 gauge or heavier?  | _____ | _____ |
| 60. Is the mesh opening in the fence no larger than a 2-inch square?   | _____ | _____ |
| 61. Is the bottom of the fence embedded in a suitable material to a minimum depth of 3 inches or secured to barbed wire at or below ground level?                        | _____ | _____ |
| 62. Are the fence posts 6 feet on center and embedded in cement?   | _____ | _____ |
| 63. Are sufficient steel tie wires used to secure the fence to the posts?  | _____ | _____ |
| 64. Is the distance from the ground to the top of the fence at least 7 feet (height sometimes dependent on zoning and/or city, county, etc, ordinance)?                  | _____ | _____ |
| 65. If the fence joins other structures (fences or buildings), generally not recommended, is adequate protection available to prevent unauthorized entry or exit?        | _____ | _____ |
| 66. Do the fence and gates have three strands of barbed wire offset from the vertical to both the interior and exterior of the property and upward at a 45-degree angle? | _____ | _____ |
| 67. Are the 4-point barbs, generally No. 12 gauge wire or heavier, spaced 4 inches apart?  | _____ | _____ |
| 68. Do the fence or gates need repair at any location?   | _____ | _____ |
| 69. Is the fence equipped with an alarm?   | _____ | _____ |
| 70. Is the alarm operative?  | _____ | _____ |

**Other Type Barriers:** If the perimeter of the computer facility *is not* protected by a chain link fence, consideration should be given to the following items.

- |   |       |       |
|---|-------|-------|
| 71. Is the facility defined by any type barrier (ie, masonry wall, shrubbery, etc)? | _____ | _____ |
| 72. If so, is the barrier adequate?   | _____ | _____ |

- |  | YES   | NO    |
|--|-------|-------|
| 73. If no barrier is present, is one warranted?  | _____ | _____ |
| 74. If so, will the recommended barrier be acceptable by the zoning and/or city, county, etc, ordinance? | _____ | _____ |

**Barrier Hazards:** Regardless of the type of perimeter barrier present, consideration should be given to the following.

- |   |       |       |
|---|-------|-------|
| 75. If there are openings in the barrier (ie, culverts, tunnels, manholes for sewers and utilities, etc), are they properly secured?  | _____ | _____ |
| 76. Is the area surrounding the barrier clear of any growth of objects (ie, trees, overhanging limbs, poles, motor vehicles, stored materials, etc) that could provide cover or assistance to persons seeking unauthorized entry?                         | _____ | _____ |
| 77. Is the distance between the enclosed building and the perimeter barrier sufficient to prevent unauthorized entry or exit or possible detection of such?   | _____ | _____ |
| 78. Is protection provided (ie, guard rails, etc) inside the perimeter barrier to protect same from damage by company vehicles and to prevent vehicles from parking adjacent to the barrier in order to deter unauthorized entry or exit to the facility? | _____ | _____ |
| 79. Is the employee parking area separated from the company parking area by a fence or wall?  | _____ | _____ |
| 80. If employee parking is permitted inside the perimeter barrier with company vehicles, are security precautions taken when employees visit their personal vehicles?   | _____ | _____ |
| 81. If company parking is provided for employees, are employee identification cards and/or vehicle decals utilized to prevent unauthorized parking, access, etc?  | _____ | _____ |

**Entrance and Exit Gates:** Consideration should be given to the following items in connection with the perimeter barrier entrance and exit gate to the computer facility.

- |   |       |       |
|---|-------|-------|
| 82. If double gates are used, are they constructed in a manner to prevent them from being forced open?          | _____ | _____ |
| 83. Are there any openings around the gates larger than 6 inches?   | _____ | _____ |
| 84. Are gate hinge pins installed in such a manner to prevent the gate from being removed by lifting, etc?      | _____ | _____ |
| 85. If a chain is used for locking the gate, is it welded to the gate or adjoining post to prevent its removal? | _____ | _____ |
| 86. Is the padlock (combination lock not recommended) welded to the chain to prevent its removal?               | _____ | _____ |
| 87. Are padlocks changed periodically depending upon employee turnover, lost keys, major thefts, etc?           | _____ | _____ |
| 88. Is someone assigned the responsibility of key control and inventory?  | _____ | _____ |

**SECTION 007-590-400**

	YES	NO
89. If automatic or electrical gate is installed, are the controls located and operated from inside the gates to prevent unauthorized entry?	_____	_____
90. Are the serial numbers removed from the locks to prevent someone from obtaining duplicate keys?	_____	_____
91. Are all gates locked when the facility is unattended?	_____	_____
92. Is someone at the facility assigned the responsibility of securing the entrances or exits after all persons have departed?	_____	_____
93. Are gates, which are not in use, inspected frequently to make sure they remain locked and in good condition?	_____	_____
94. If the gate is equipped with an alarm, is it operative?	_____	_____
95. If closed circuit television is utilized to observe the gate, is it operative?	_____	_____
96. Is responsibility for the monitoring assigned?	_____	_____
97. If contract guard service is utilized, is the guard(s) present and alert?	_____	_____
98. Are informational, warning, or no trespassing signs bilingual (two appropriate languages), when necessary, and legally posted?	_____	_____

**Outside Lighting:** Consideration should be given to the following items in connection with the perimeter lighting.

99. Is the perimeter lighting sufficient to provide detection of authorized entry? Are these lights reduced due to an energy conservation program?*	_____	_____
100. Is the lighting sufficient at the entrance gate for identification of individuals and verification of credentials?	_____	_____
101. Is the lighting at each building entrance sufficient for security purposes?	_____	_____
102. If closed circuit television is utilized, is lighting sufficient for its use?	_____	_____
103. Were all lights operative at the time of inspection?	_____	_____
104. Do light beams overlap to provide coverage in case a bulb burns out?	_____	_____
105. Is there a dependable auxiliary source of power for the lighting system?	_____	_____
106. Are all lighting fixtures and wiring installed beyond easy reach?	_____	_____
107. Are protective lighting guards provided at necessary locations within the perimeter to prevent intentional breaking of bulbs?	_____	_____
108. If contract guards are provided, is there sufficient light for them to detect movement at all points within the perimeter barrier?	_____	_____

- |  | YES   | NO    |
|--|-------|-------|
| 109. Is the lighting system controlled by photoelectric cells or locked time clocks which are more reliable than manual operation? | _____ | _____ |
| 110. Is someone assigned the responsibility of inspecting and maintaining the lights on a scheduled basis?                         | _____ | _____ |
| 111. Are outside lights utilized for deterring unauthorized entry?   | _____ | _____ |

HOUSEKEEPING

	YES	NO
1. Is there an accumulation of trash in the computer area?***	_____	_____
2. Are equipment covers and work surfaces cleaned regularly?	_____	_____
3. Are floors washed regularly?	_____	_____
4. Are wastebaskets emptied outside the computer area to reduce dust discharge?	_____	_____
5. Is carpeting of the antistatic type?	_____	_____
6. Are low fire hazard waste containers used?	_____	_____
7. Are maintenance areas kept clean and orderly?	_____	_____
8. Is there a mandated and enforced housekeeping procedure that ensures that flammable materials (such as paper, inks, corrugated boxes, and ribbons) are kept to a minimum?	_____	_____
9. Are closed circuit TV lenses cleaned regularly?	_____	_____

**OTHER FACILITY CONSIDERATIONS**

	YES	NO
1. Are security and operations personnel briefed on how to react to civil disturbances?	_____	_____
2. Is there a good liaison program with local law enforcement agencies?	_____	_____
3. Do personnel know how to handle telephone bomb threats?	_____	_____
4. Are dry-cell lanterns available for computer room emergency use?	_____	_____
5. Are door hinges on all doors to the computer room and computer room annex welded?	_____	_____
6. Is there a paper shredder to destroy confidential reports?	_____	_____
7. Are there metal trash receptacles with hinged covers?	_____	_____
8. Have locks been installed on the windows connecting the data entry area and computer operations?	_____	_____
9. Is the data center in proximity to the organization's medical facilities?	_____	_____

**SECTION 007-590-400**

**PERSONNEL**

	<b>YES</b>	<b>NO</b>
1. Are supervisors alert to the possible disgruntled employee?		
(a) Conflict between employees?	_____	_____
(b) Dissatisfaction over pay, company policies, or other company-related incidents, such as working conditions, work period, or performance evaluation?	_____	_____
(c) Possible personal problems with family, finances, etc?	_____	_____
2. Do personnel policies allow for containment or immediate dismissal of employees who may constitute a threat to the installation?		
(a) Notification procedures?	_____	_____
(b) Minority considerations?	_____	_____
(c) Political considerations?	_____	_____
3. Do supervisors know their people well enough to detect a change in their living habits?		
(a) Financial status?	_____	_____
(b) Living conditions?	_____	_____
(c) Clothing, automobile, etc?	_____	_____

**TRAINING ORIENTATION**

	YES	NO
1. Is there a continuing personnel education program in computer security?	_____	_____
2. Are the personnel trained for an orderly shutdown of the equipment for various types of emergencies, such as fire, earthquake, and bomb threat?	_____	_____
3. Are there orientation sessions dealing with emergency procedures?	_____	_____
4. Has a fire extinguisher demonstration been held for all operators?	_____	_____
5. Have computer operators attended a class of computer room security?	_____	_____
6. Are people cross-trained to cover all functions?		
(a) Can more than one operator on each shift operate each piece of hardware?	_____	_____
(b) Can more than one operator on each shift run each system?	_____	_____
(c) Can more than one person on each shift perform each emergency task?	_____	_____
(d) Does each person have a primary and secondary emergency assignment?	_____	_____
7. Are key personnel, at the minimum, trained in first aid procedures to treat burns and smoke inhalation (such as hydrogen chloride gas from insulation)?	_____	_____
8. Is first aid equipment available within the facilities and do key personnel know its location and contents?	_____	_____
9. Have all personnel been trained in the use of fire-fighting equipment.	_____	_____

OPERATING PROCEDURES

	YES	NO
1. Are meter hours correlated with utilization hours?	_____	_____
2. Has an acceptable range of correlation of meter versus utilization hours been established?	_____	_____
3. Do employees have access to tools with which they might do harm or "experiment" with the hardware?*	_____	_____
4. Are scheduled maintenance activities monitored to assure proper reliability and hardware performance?	_____	_____
5. Is there a mechanism to verify that maintenance <b>claimed</b> is maintenance <b>performed</b> ?	_____	_____
6. Have record systems indicating vendor, model numbers and features, and level of engineering change been established?	_____	_____
7. Are all periods of downtime verified?	_____	_____
8. Does each period of downtime have a corresponding maintenance request?	_____	_____
9. Are "end meter" with "begin meter" readings checked each morning for unexplained gaps?	_____	_____
10. Are steps taken to resolve unexplained time periods?	_____	_____
11. Is all incoming work checked against an authorized user list?	_____	_____
12. Is output spot-checked for possible misuse of the system?	_____	_____

## TAPES AND/OR DISKS

	YES	NO
1. Is there a procedure for tape and/or disk accountability?	_____	_____
2. Does the tape and disk accountability procedure cover:		
(a) Frequency of use?	_____	_____
(b) Frequency of cleaning?	_____	_____
(c) Authorized user?	_____	_____
(d) Security classification?	_____	_____
(e) External evacuation classification?	_____	_____
(f) Release procedures?	_____	_____
3. Are magnetic tapes and disks filed in an orderly manner?	_____	_____
4. Is there a tape and/or disk cleaning plan?		
(a) Are tapes cleaned on a regular basis?	_____	_____
(b) Are disk packs checked and cleaned?	_____	_____
5. Are tapes kept in their containers except when in use?	_____	_____
6. Are tapes stored vertically?	_____	_____
7. Are tape utilization records maintained?	_____	_____
8. Are tape containers cleaned periodically?	_____	_____
9. Are tape heads cleaned every shift?	_____	_____
10. Are tapes sample-tested periodically for dropouts to determine the general condition of the tape library?	_____	_____
11. Is frayed leader stripped regularly?	_____	_____
12. Has the possibility of a tape rehabilitation or recertification program been investigated?	_____	_____
13. Is the tape library located in an area not subject to explosion or other dangers?	_____	_____
14. Are storage vaults specifically designed for magnetic media used for critical tape files?	_____	_____
15. Has magnetic detection equipment been considered to preclude the presence of a magnet near tapes and disks?	_____	_____
16. Is similar protection provided for tape files while in transit to a backup site, etc?	_____	_____

FILE, DOCUMENTATION, AND DATA

	YES	NO
1. Are duplicate files stored in a building separate from that containing the originals?	_____	_____
2. Is there a current inventory of such files?	_____	_____
3. Have the merits of leasing underground storage space from a reputable vital records concern been considered?	_____	_____
4. Are programs stored in a low fire-hazard container?	_____	_____
5. Has a "dry run" been held in the past 3 months to test the ease and accuracy of the file backup system?	_____	_____
6. Are program changes controlled and recorded?	_____	_____
7. Are changes made only to a copy of a program file, but not to the original?***	_____	_____
8. Is a record maintained of items withdrawn from the production file area?	_____	_____
9. Does the computer operations department review systems documentation for compliance with operational standards?	_____	_____
10. Is there a backup of source data for programs under development?	_____	_____
11. Are all computer room and data entry tape files retained for at least 5 days?	_____	_____
12. Are all payroll JCL controlled and accessed only by a minimum of operators?	_____	_____
13. Have data, programs, and documentation been classified in terms of criticality to the organization?	_____	_____
14. Is there a marking system for evacuating the most critical items first?	_____	_____
15. Are data files of the highest classification together in racks to permit easy removal?	_____	_____
16. Is system backup (disk-to-tape-to-disk) done weekly? Is JCL backup (card-to-tape) done bimonthly?	_____	_____
17. Is there restricted access to all JCL for confidential jobs?	_____	_____

\*\*\*INDICATES "No" answer. "Yes" answers in these areas are potential security weaknesses and require future investigation.