FACILITIES SECURITY AUDIT CHECKLIST

M. E. Kabay, PhD, CISSP-ISSMP

CONTENTS

In all questions, YES answers are desirable if the question is relevant to the particular site and its security policies.

1 Fire hazards

1.1 Construction

1.1.1 Is the computer housed in a building constructed of fire-resistant and non-combustible materials?

1.1.2 Is the sub-flooring concrete or non-combustible?

1.1.3 Does the sub-flooring have drainage?

1.1.4 Is the sub-floor cabling channeled through conduits?

1.1.5 Is the raised flooring non-combustible?

1.1.6 Are walls and trim non-combustible?

1.1.7 Are walls and trim painted with water-based fire-retardant paints?

1.1.8 Are ventilator grills and light diffusers made of fire-resistant materials?

1.1.9 Are doors, partitions, and framing made of metal?

1.1.10 Have self-closing fire doors been installed to exclude fire from other areas?

1.1.11 Are self-closing fire doors rated for at least 1 hour's fire resistance?

1.1.12 Is all glass in the facility steel-mesh or otherwise reinforced?

1.1.13 Is the ceiling tile non-combustible or made of high-melting-point materials (including supports)?

1.1.14 Are cables connecting ceiling lights routed through conduits?

1.1.15 Are all electrical connections properly grounded?

1.1.16 Are sound-deadening materials (e.g., on walls, in cabinets, or around desks and other operating areas) sprayed with fire-retardant chemicals?

1.1.17 Does the construction avoid foamed cellular plastics (e.g., Styrofoam)?

1.1.18 Is the data center placed far from potential sources of fire such as

- cafeterias,
- power cables,
- rubbish storage,
- caustic chemicals,
- fumes,
- odors,
- petroleum supplies?

1.1.19 Is the data center away from steam lines?

1.1.20 Is the data center away from areas using hazardous processes (e.g., acid treatments, explosives, high-pressure vats)?

1.1.21 Within the data center, are there sufficient distance or fire-resistant materials to prevent fire in one area from spreading to other areas?

- Tape and disk libraries?
- Paper and punch-card storage?
- Backup files?
- Source listings?
- Backup copies of operations procedures?
- Forms handling equipment?
- Report-distribution facilities?
- Alternate computing facilities?
- Punch-card processing?
- Remote job entry or interactive terminals?

1.1.22 Does the construction avoid vertical cable conduits which could spread fire?

1.1.23 If a fire were to occur in one of the data center facilities, would other offices of the business be physically disabled also?

1.1.24 Do computer room walls extend from floor to roof (below the false floor and above the false ceiling)?

1.1.25 Are exits and evacuation routes clearly marked?

1.2 Combustibles

1.2.1 Are paper and other supplies stored outside the computer room?

1.2.2 Are curtains, rugs, and drapes non-combustible?

1.2.3 Are caustic or flammable cleaning agents excluded from the data center?

1.2.4 If flammable cleaning agents are permitted in the data center, are they in small quantities and in approved containers?

1.2.5 Is the quantity of combustible supplies stored in the computer room kept to the minimum?

1.2.6 Is computer-room furniture metal-only?

1.2.7 Are reference listings (e.g., lists of files backed up to tape) moved out of the computer room as soon as possible?

1.2.8 Are clothing racks excluded from the computer room?

1.2.9 Are tapes stored away from the computer room?

1.2.10 Are paper-bursting and shredding equipment away from the computer room?

1.2.11 Are computer-room or media-library safes closed when not in use?

1.2.12 Are loose pieces of plastic (e.g., tape rings, disk covers, tape covers, empty tape reels) stored outside the computer room?

1.2.13 Is decoration of the computer room (e.g., posters, company literature, holiday decoration such as Halloween and Christmas streamers) avoided?

1.3 Storage

1.3.1 Are copies of critical files stored off-site?

1.3.2 Are on-site copies of critical files in fireproof safes?

1.3.3 Is the number of tapes outside the tape library kept to a minimum?

1.3.4 Are fireproof safes located in a separate area away from the tape library?

1.3.5 Is there a fireproof safe in the computer room for storing tapes and disks while they are needed for operations in the computer room?

1.3.6 Are disk and tape storage cabinets fitted with rollers to permit rapid emergency relocation?

1.3.7 Are there obstructions (e.g., risers in front of doors, narrow doorframes) which prevent rapid removal of storage cabinets in an emergency?

1.3.8 Are disks and tapes coded to show their evacuation priority?

1.3.9 If files are kept in the computer room, are they coded to show their evacuation priority?

1.3.10 Are there means of transporting fireproof safes away from the data center in an emergency?

1.3.11 Is there a supply of critical forms stored off-site?

1.4 Practice sessions and drills

1.4.1 Are there regular fire drills?

1.4.2 Are operators trained periodically in fire-fighting techniques?

1.4.3 Are operators assigned specific, individual responsibilities in case of fire?

1.4.4 Is the fire detection system regularly tested?

1.4.5 Is the no-smoking rule for the computer room and media library strictly enforced?

1.4.6 Is an area fire warden (to coordinate evacuation) assigned for every shift?

1.4.7 Is the alarm system tested frequently?

1.4.8 Are there simulated disasters to exercise and improve the evacuation plans?

1.4.9 Is a fire inspection periodically conducted by in-house or municipal fire inspectors?

1.4.10 Are automatic detection and protection systems regularly inspected by qualified personnel?

1.5 Protection and reaction

1.5.1 Detection equipment

1.5.1.1 Do the facilities have equipment for detecting one or more of the following:

- Smoke?
- Heat?

1.5.1.2 Are any of these detection units mounted inside cabinets of critical system components?

1.5.1.3 Are smoke detectors mounted

- in ceiling (above suspended tiling)?
- under raised floor?
- in in-bound air ducts?

1.5.1.4 Does smoke-detection equipment shut down the air conditioning system?

1.5.1.5 Is the smoke-detection system tested regularly?

1.5.1.6 Are smoke and fire detection systems connected to the plant security panel and to municipal public safety departments?

1.5.1.7 Does the smoke-detection system have a count-down period (e.g., 0-180 seconds) before shutting off other systems?

1.5.1.8 Are under-floor smoke detector positions marked by hanging markers on the computer-room ceiling?

1.5.2 Alarm mechanisms

1.5.2.1 Do the detection facilities described above include alarms?

1.5.2.2 Are there several strategically-located stations for initiating a manual alarm?

1.5.2.3 Do the alarm devices report the position of a fire accurately

- locally?
- to a watchman position?
- to a centralized security position?
- to a municipal security office?

1.5.2.4 Do the alarms provide pre-alarm audible signals?

1.5.2.5 Are the alarms from different detectors clearly identifiable (e.g., are there labeled luminescent panels in a central security display)?

1.5.2.6 Do the alarm mechanisms provide for automatic shutdown of critical equipment?

1.5.2.7 Is there a smoke detector alarm horn in a central location in the computer room?

1.5.2.8 Do building alarms (linked to systems outside the computer room) sound within the computer room?

1.5.3 Protection equipment: do the facilities have

1.5.3.1 Automatic dispersal of a fire-extinguishing or retardant agent such as

1.5.3.1.1 Gas

- into main computer room volume?
- (above and beneath floors and ceilings)?

1.5.3.1.2 Have personnel been trained in

- use of the gas system?
- personal safety measures?
- gas removal standards (e.g., ventilation measures)?

1.5.3.1.3 Water (last resort) including

1.5.3.1.3.1 hoses?

1.5.3.1.3.2 sprinkling systems?

- pre-action (sounds alarm and delays water release)?
- dry pipe (lets water in only when about to release)?
- wet pipe (holds water, releases at specific temperature)?
- fixed flooding systems?

1.5.3.1.4 Dry suppressants?

1.5.3.1.5 Foam (not recommended by National Fire Protection Association)

1.5.3.2 Manual equipment such as

- portable extinguishers for electrical and other fires?
- several strategically-located, easily-accessed extinguishers in computer room?
- location markers for extinguishers clearly visible over computer equipment?
- fire-resistant gloves for picking up hot objects?
- fire-blankets in a clearly-marked cylinder?

1.5.3.3 Automatic shutdowns with appropriate delays for

- electric power?
- air-conditioning (especially if HALON installed)?
- heating & humidity systems?
- air ducts?

1.5.3.4 Automatic emergency illumination to permit effective operations?

1.5.3.5 Automatic sealing of fire-breaks or fire-doors between different sections of the facility? e.g., automatic fire-retardant doors to close off

- tape library,
- paper-storage room,
- printer room,
- bursting/decollating room?

1.5.3.6 Are any fire-suppressant outlets located inside the cabinets of critical system components? E.g., inside

- CPU cabinets?
- server racks?
- RAID arrays?
- wiring cabinets?
- firewalls?
- routers / gateways?

1.5.3.7 Is there a means to activate an automatic system manually?

1.5.3.8 Is there a means to override an automatic system in case of false alarm?

1.5.3.9 Is there an override alarm to indicate that a system has been overridden?

1.5.3.10 Is there a non-overridable alarm to indicate that the override alarm has been disabled?

1.5.3.11 Are set-points for temperature detector/alarm systems controllable to permit temporary operations despite air-conditioning failure?

1.5.4 Reaction planning

1.5.4.1 Have building engineers recently analyzed the fire detection system to ensure that the number and location of detectors are appropriate for your current equipment and function configurations?

1.5.4.2 Is the local fire-fighting force adequate (e.g., in accordance with the American Insurance Association's Standard Fire Defense Rating Schedule)?

1.5.4.3 Is there round-the-clock watchman coverage during off-hours?

1.5.4.4 Are there established procedures for rapidly re-arming detection and fire-protection devices after discharge?

1.5.4.5 Is there easy access to the computer room and related areas by fire-fighting personnel and equipment?

1.5.4.6 Can emergency crews reach the building quickly?

1.5.4.7 If access is through electrically-controlled systems, can they be operated on battery power during a power outage?

1.5.4.8 Are emergency power shutdown controls easily accessible at points of exit?

1.5.4.9 Can emergency crews reach the computer room quickly even during off-shifts and holidays?

1.5.4.10 Is self-contained breathing equipment available for staff and fire-fighting personnel?

1.5.4.11 Are additional floor-panel removers (suction cups) located next to all extinguishers?

1.5.4.12 Are sprinkler shutoff valves in clearly marked, secure locations?

1.5.4.13 Are all staff trained in using sprinkler shutoff valves?

1.5.4.14 Does the fire department know the location of the computer room?

1.5.4.15 Does the fire department know where the alarm panels are?

1.5.4.16 Is there a battery-powered megaphone available?

- Is its location known to your staff?
- Is its operation known to your staff?

1.5.4.17 Is there a procedure or mechanism for positive identification of

- who was in the building when fire broke out?
- who is now outside the building?

1.5.4.18 Are procedures in place alert salvage crews to the importance of letting experts

- open data safes?
- salvage disk drives?
- salvage magnetic tapes and cartridges?
- salvage optical media?

2 Water

2.1 Physical location

2.1.1 Are computer facilities above the local water line?

2.1.2 If not, have sufficient sealing and foundation draining devices been included in building design?

2.2 Within the facility

2.2.1 Are overhead steam pipes absent from the facility?

2.2.2 Are overhead water pipes (except sprinklers) absent from the facility?

2.2.3 Will sub-floor drainage evacuate water quickly?

2.2.4 Are drains installed on floor above to divert away from computer room?

2.2.5 Is the roof of computer room watertight?

2.2.6 Is the upper ceiling constructed so as to shunt water away from equipment?

2.2.7 Are pipe and wire conduit openings through walls watertight?

2.2.8 Is there adequate drainage in adjacent areas so that water will not overflow into computer room?

2.2.9 Is there an industrial-grade vacuum cleaner suitable for sucking up water available?

2.2.10 Is there a dispenser for wide plastic rolls to cover equipment if sprinklers are about to go off?

2.2.11 Have all operators practiced covering equipment with plastic sheets in case of emergency?

2.2.12 Are all electrical junction boxes located under raised flooring held off the concrete to prevent immediate water damage?

2.2.13 Does the air conditioning system have adequate water ducts to lead leakage away from the building in case of rupture or other damage?

2.2.14 Are water detectors

2.2.15 installed under the raised flooring?

2.2.16 connected to the data center and building alarm panels?

2.2.17 Are water main shutoff valves in clearly marked, secure locations?

2.2.18 Do staff know how to gain access to the water shutoff valves (e.g., where the keys are, what the combinations are)?

2.2.19 Are all staff trained in using water main shutoff valves?

2.2.20 Have staff practiced water-emergency procedures?

2.3 Outside the facility

2.3.1 Is the roof sufficiently sealed and well constructed to prevent high winds from splitting it open?

2.3.2 Is there protection against accumulated air-conditioning water or leaks in rooftop water towers?

2.3.3 Is grading around the exterior of the facility constructed to conduct water away from the building?

2.3.4 Are there sufficient storm drain inlets to accommodate water accumulation during sudden or seasonal rainfall?

2.3.5 Have subterranean or under-roofing heating systems been installed to melt snow and prevent undue accumulation?

2.3.6 Are roofs rated to support maximum expected snow accumulation?

2.3.7 Are safeguards in place to prevent building unauthorized structures on the roof?

3 Air conditioning (A/C)

3.1 Equipment

3.1.1 Are the BTU ratings of A/C equipment appropriate for peak loads?

3.1.2 Is the A/C system dedicated to exclusive use by the computer facility?

3.1.3 Are A/C ducts from the rest of the building excluded from the computer room?

3.1.4 Is there a backup A/C facility?

3.1.5 Is the compressor remote from the computer room?

3.2 Intakes, ductwork, piping

3.2.1 Are duct linings and filters non-combustible?

3.2.2 Are air intakes

3.2.3 covered with protective screening?

3.2.4 located well above street level?

3.2.5 located to minimize intake of pollution and debris (e.g., not under a large tree or next to a smokestack)?

3.2.6 Does ductwork prevent smoke and fumes from other parts of the building from reaching the computer room?

3.2.7 Does ductwork prevent smoke and fumes from reaching other parts of the building?

3.3 Shutdown

3.3.1 Will alarm or sensing devices automatically shut down the A/C system?

3.3.2 Are there alternate shutoff controls in the computer room for all power and A/C fans?

3.3.3 Can installed ceiling exhaust fan(s) provide sufficient air movement if the A/C system is inoperable for several hours?

3.3.4 Are there portable fans for emergency use to move air into the computer room from adjacent areas in case of A/C failure?

3.4 Protection

3.4.1 Is the cooling tower fire-protected?

3.4.2 Are there smoke and temperature sensors within A/C ducts?

3.4.3 Are there smoke, temperature, and water sensors within the A/C rooms?

3.4.4 Does the construction of the A/C facilities restrict access to authorized personnel, including

- placement in a high place?
- protection of water supply?
- protection of fan or cooling mechanism?
- survey of A/C area by closed-circuit television (CCTV)?
- periodic checks by security personnel?

3.4.5 Do security personnel have copies of diagrams for use by maintenance and emergency personnel showing

- wiring?
- ductwork?
- water lines?
- air-flow?

3.4.6 Are copies of building systems kept updated when the A/C system is modified?

3.4.7 Are there heat- and humidity controls for the A/C system itself?

3.4.8 Are there temperature- and humidity-monitoring and -recording devices in the computer room?

3.4.9 Do specific operations staff have explicit instructions to examine such records and report on deviations beyond the tolerance norms?

4 Electricity

4.1 Power supply (PS)

4.1.1 Is the local electrical PS reliable?

4.1.1.1 Is there sufficient voltage and amperage to support the equipment when all of it is operating?

4.1.1.2 Is there sufficient PS to support simultaneous startup of all peripherals?

- spin-up of magnetic disks?
- warm-up of large laser printers?
- startup of A/C compressors?

4.1.1.3 How susceptible is the PS to

- outages?
- brownouts (reduced operating voltages)?
- spikes (low-frequency voltage surges)?
- noise (high-frequency voltage fluctuations)?

4.1.1.4 Is the PS periodically monitored on recording devices to determine the answers to the above questions?

4.1.1.5 Are written records kept of disturbances defined in 3) above to permit evaluation of long-range trends?

4.1.1.6 If PS are unreliable, have the following mechanisms for improvement been investigated and documented for rapid response to potential management decisions?

- power filters and surge protectors (smooth out spikes and noise)?
- secondary PS sources (separate lines to utilities)?
- uninterruptable PS (UPS)?
- standby generators with tested output quality (not low-power portable gasoline engines used for domestic or low-grade industrial use)?

4.1.2 Does the data center have a dedicated PS (separate from all other users in the building)?

4.1.3 Is there a mechanism for shifting to an alternate PS if the primary source is destroyed or unavailable?

4.1.4 Are the computer room transformer and motor generator enclosed in a wire cage for protection?

4.1.5 Is there standby battery power to operate electrically-controlled doors during power failures?

4.1.6 Does the computerized access-control equipment have battery backup or rapid-acting UPS to prevent loss of configuration during power failure?

4.1.7 Does the telecommunications equipment have battery backup or rapid-acting UPS to prevent loss of configuration during power failure?

4.1.8 Do microcomputers have UPS to prevent damage to hard disks during power failures or brownouts?

4.2 Wiring

4.2.1 Is wiring in conformance to local building codes for the installation's class of service?

4.2.2 Do security and maintenance officials have a copy of the wiring diagram?

4.2.3 Are electrical junction boxes and panels in areas protected from water or other damage?

4.2.4 Are the main power control boards in a remote and restricted-access position?

4.2.5 Are there emergency power-off switches at each exit of the computer room?

4.2.6 Has all wiring under the raised floor in the computer room been checked to verify that all circuits, including 110/120 V, are wired to shunt breakers and properly grounded?

4.2.7 Have all junctions (plugs / sockets) in the underfloor of the computer room been placed on bricks to raise them off the floor in case of flooding?

4.3 Lighting

4.3.1 Is there an emergency lighting system which automatically activates when the main lighting fails?

4.3.2 Is the emergency lighting system tested periodically?

4.3.3 If the system has fixed-position lamps, do they illuminate all required areas of the computer room adequately for rapid work in times of emergency?

4.3.4 Are there additional light sources independent of the main PS (e.g., wide-beam battery-operated portable

flashlights and area-lamps)?

4.3.5 Are specific employees assigned to regular inspection and appropriate replacement of batteries and bulbs in such flashlights?

4.3.6 Is there an emergency PS to energize emergency lighting in case of prolonged outage of the main PS?

4.3.7 Are there adequate emergency lights for rapid entry to and exit from the computer room through passages in the main building?

4.3.8 Are the office lights wired to ensure security night lights (e.g., every 10th fluorescent panel to stay on 24 hours/day)?

4.3.9 Has a copy of the emergency light layout been supplied to the maintenance and security personnel?

5 Preparing for civil, man-made, and natural disasters

5.1 Location of the facility is

5.1.1 remote from any known earthquake fault?
5.1.2 away from a river bed or flood plain?
5.1.3 far from high-voltage transmission lines?
5.1.4 far from heavily-traveled highways?
5.1.5 far from rail lines?
5.1.6 far from overhead railways, viaducts, and aqueducts?
5.1.7 far from fuel storage sites or containers?
5.1.8 far from fuel or steam transmission lines?
5.1.9 far from isolated metal structures (e.g., pylons) that might draw lightning?
5.1.10 in a low-crime area?
5.1.11 located away from areas where civil disturbances have involved computer facilities?
5.1.12 in an area with low fire potential?
5.1.13 far from an airport or flight path for takeoff and landing?
5.1.14 far from processing plants using toxic or caustic chemicals?
5.1.15 away from dense or tall trees?
5.1.16 away from plant processing areas where materials are dried, ripened, or composted?
5.1.17 far enough from adjacent structures that disasters in those buildings would not damage your facility?
5.1.18 located where problems with small animals (e.g., rodents, insects) are not a problem?
5.1.19 located where there are alternative access roads in case of major disaster?
5.1.20 free from serious vibrations?

5.2 Construction

5.2.1 Is the building sound enough structurally to resist

- wind storms and hurricanes?
- flood damage?
- earthquakes?
- blizzards?

5.2.2 Are building and equipment properly grounded to prevent lightning damage?
5.2.3 Is the foundation solid enough to prevent subsidence?
5.2.4 Is the building defensible in case of civil unrest?
5.2.5 Are alternative emergency accesses available for emergency crews and equipment?

5.3 Natural disaster prediction

5.3.1 Is there some means to advise personnel of possible natural disasters such as

- torrential rains?
- blizzards?
- tornadoes, hurricanes, or other wind storms?
- severe electrical disturbances?
- sand storms?
- rising rivers?

5.3.2 Is there a series of contingency steps that are invoked when a natural disaster advisory is received?

5.4 Man-made disaster prediction

5.4.1 Will appropriate personnel be notified in case of a nearby disaster, such as fire in adjacent buildings or woods?
5.4.2 If the facility is in the flight path of an airport, are measures in place to notify personnel in case of potential aircraft disasters?

5.5 Civil disaster prediction

5.5.1 Is someone in the facility specifically responsible for being aware of potential unrest in the locale?
5.5.2 Is there a procedure for civil authorities to notify the facility in the event of civil unrest?
5.5.3 Does the organization's contract with security services agencies provide for profiling potential unrest?
5.5.4 Is there a procedure for handling threats to the facility?
5.5.5 Is there a policy for handling and controlling rumors?
5.5.6 Is there a battery-operated AM/FM radio available in the data center?
5.5.7 Is there a citizen's-band radio (preferably with emergency PS such as batteries) available in the facility?
5.5.8 Is there a cellular phone available in the facility?

6 Alternate location

6.1 Is there an alternate location for resumption of operations following a disaster?

6.2 Is space allotted in the alternate location for

6.2.1 Computer and telecommunications hardware?

6.2.2 Forms-handling and distribution equipment?

6.2.3 Data preparation?

6.2.4 Documentation files?

6.2.5 Program files?

6.2.6 Tape and disk files?

6.2.7 Programming functions?

6.2.8 Administrative functions?

6.2.9 Supply storage?

6.2.10 A/C and electrical equipment?

6.3 Is there an alternate-site implementation plan?

6.3.1 Has it been approved by facilities personnel?

6.3.2 Has it been approved by security personnel?

6.3.3 Has it been coordinated with key user representatives?

6.4 Are there arrangements for support services such as

6.4.1 transportation?

6.4.2 equipment service?

6.4.3 food?

6.4.4 shelter?

6.4.5 clean clothing?

6.4.6 contact with family members?

6.4.7 ancillary services such as

- kitchen
- washrooms
- showers
- sleeping areas
- relaxation (TV, radio)?

7 Access control

7.1 Identification (ID)

7.1.1 Is advertising the location of the computer room discouraged?

7.1.2 Is access to the computer room restricted to selected personnel?

7.1.3 Is there a photo-badge system for positive identification of authorized employees?

7.1.4 Are there mechanisms to ensure that an ID badge belongs to the bearer?

7.1.5 Is there a file of current photographs of all authorized personnel available for security officers?

7.1.6 Is even a familiar person forbidden access to the computer room without positive ID?

7.1.7 Is a person accompanying a familiar or authorized person prevented from entering the facility without authorization?

7.1.8 Are temporary badges matched against some other form of ID?

7.1.9 Are ID badges color-coded, facility-zoned, or otherwise marked to demonstrate security clearance or access?

7.1.10 Are transient personnel (e.g., equipment service people) checked out of as well as into the data center?

7.1.11 Are there restrictions on who may receive data files (e.g., tapes, disks) or reports?

7.1.12 Is there a security-clearance procedure to authorize personnel to obtain files or other material from the data center?

7.1.13 Is there a need-to-know restriction enforced on dissemination of information?

7.1.14 Are there restrictions enforced on what visitors and staff may bring into or out of the data center?

7.1.15 Are food and beverages strictly prohibited in the computer room?

7.1.16 Are blind trials conducted to test all aspects of access control (e.g., hiring a bonded security agent to attempt unauthorized entry)?

7.1.17 Are executives aware of security restrictions (e.g., the President)?

7.1.18 Has a top executive tested security by pretending to bully his/her way into the facility without authorized ID?

7.2 Access routes

7.2.1 Are there guards on every street entrance that allow access to the data center?

7.2.2 Are there control points (e.g., guards or locks or other access-control devices) blocking direct access from any elevator doors?

7.2.3 Do hallways have no false floors that might allow hidden access to the computer room?

7.2.4 Are stairways locked to permit exit but prevent unauthorized entry to the data center floor(s)?

7.2.5 Are access routes to and from adjacent offices controlled?

7.2.6 Are all exterior windows at or near street level covered with metal grills?

7.2.7 In areas with high crime rates, is there bullet-proof glass?

7.2.8 Are windows taped for intrusion detection?

7.2.9 If there is a dumb-waiter or freight elevator, is its access to the data center protected?

7.2.10 Is access from a loading dock controlled?

7.2.11 Are electrically-operated doors protected against intrusion by interrupting the local electrical supply (e.g., by cutting wires)?

7.2.12 Is the computer room screened to render it invisible from outside the building?

7.2.13 Are doors to the computer room and data center locked during evening, night, weekend, and holiday shifts?

7.3 Visitor control

7.3.1 Is there an organized and enforced visitor control procedure?

7.3.2 Are all visitors required to wear a distinctive identification badge with the expiration date prominently marked on it?

7.3.3 Are all visitors without a badge reported to the security staff at once?

7.3.4 Are all visitors accompanied at all times (except washrooms with a single door)?

7.3.5 Are all unaccompanied visitors challenged by all staff?

7.3.6 Is there a computer room sign-in/out log for all visitors?

7.3.7 Are temporary passes numbered to prevent re-use of an expired pass?

7.3.8 Is there a procedure for returning and accounting for temporary passes?

7.3.9 Are temporary passes difficult to duplicate or forge?

7.3.10 Are pass and access rules consistently enforced

- by security guards?
- by receptionists?
- by operators?
- by all other employees including programmers, managers, secretaries, and clerks?

7.3.11 Is there a validation procedure to ensure that unwarranted visitors cannot obtain a temporary pass?

7.3.12 Are vendor personnel and consultants checked for valid proof of their affiliation before being granted a pass?

7.3.13 Are vendor personnel and consultants accompanied at all times despite their familiarity to the data center staff?

7.3.14 Are corporate executives prevented from including the data center in their facilities tours?

7.3.15 Are visitors excluded unconditionally from sensitive areas of facility (e.g., telecommunications network control monitors)?

7.4 Surveillance and other security measures

7.4.1 Are keys, combination locks, and other security devices installed and used to control access?

7.4.2 Are combination locks protected with hoods or other devices to prevent discovery of the code by an observer?

7.4.3 Can a single individual be prevented from gaining access to the data center without the knowledge of a security guard or other employee?

7.4.4 Is there a round-the-clock watch patrol going through the facility?

7.4.5 Has closed-circuit television (CCTV) been installed to

- cover critical computer equipment?
- cover access routes?
- cover critical storage areas?
- cover A/C and PS?
- cover critical telecommunications equipment?
- permit monitoring at all times by safety or security personnel?
- monitor external access and building periphery?
- cover hallways and exits from washrooms?

7.4.6 Are communications lines protected against external access (e.g., through manholes adjacent to the building)?

7.4.7 Have ID markings been removed from power rooms, communications closets, etc. to reduce ease of locating critical resources?

7.4.8 Is access to communications equipment (e.g., junction boxes, switches) restricted?

7.4.9 Are there restrictions on the introduction into the data center of

- camera or other photo-recording equipment?
- sound magnetic or other recording devices?
- unauthorized radio communications equipment (e.g., portable transceivers)?

7.4.10 Are there metal detectors in use for checking visitors to the data center?

7.4.11 Is there a means to inspect parcels and other articles (e.g., briefcases) carried into and out of the data center?

7.4.12 Are there mechanisms to verify that crates and boxes containing products or equipment received at the data center actually contain their specified contents?

7.4.13 Are there electric eyes or motion detectors installed in infrequently-used rooms and passageways?

7.4.14 Are there motion detectors or other intrusion-detecting devices in the false floors and ceilings of the computer room?

7.4.15 Are all internal doors in the data center fitted with self-closing mechanisms?

7.4.16 Are internal doors and passageways free of all obstructions (e.g., wedges, boxes)?

7.4.17 Are internal aisles wide, straight, and unobstructed (permitting a clear view of all aisles as well as facilitating movement in an emergency)?

7.4.18 Do all access doors open fully and freely?

7.4.19 Are cabinets and equipment so disposed in the computer room that a person can work effectively on each device once its doors have been opened?

7.4.20 Are all doors equipped with sensors to detect and indicate that they are open?

7.4.21 Are there security guards at every data center access?

7.4.22 Are critical files under lock and key to limit access?

7.4.23 Is there a periodic security check of all personnel?

- Spot inspections while under operation?
- Complete background investigation upon hiring?
- Thorough investigation of all personnel being granted access to the data center?

7.4.24 In addition to CCTV, are there sound-monitoring systems to locate and listen to sounds when the facilities are supposed to be unused?

7.4.25 Can all external doors be locked on command from a single security station?

7.4.26 Can all internal doors be locked on command?

7.4.27 If there is a CCTV system, are there personnel assigned to watch the monitors at all times?

7.4.28 If someone monitors the CCTV, is that his/her sole function?

7.4.29 Are there double-door arrangements to trap an intruder within a fixed space?

7.4.30 Are security precautions enforced at the same level at every entrance, including the loading dock?

7.4.31 Are plans and blueprints for the data center and other important areas controlled or restricted?

7.4.32 Are these plans and blueprints unavailable outside the organization?

7.4.33 Are external walls and windows proof against easy access by a saboteur?

7.4.34 If the organization is subject to civil disturbance, is the disaster plan filed with local authorities (e.g., civil defense, police, fire, or military)?

7.4.35 Are master controls for detection and suppression systems located outside the data center?

7.4.36 Are all emergency exits wired to sound alarms when opened?

7.4.37 Are all emergency exit alarms wired to the central security panels?

7.4.38 Do emergency exit alarms indicate unambiguously which door has been opened?

7.4.39 Are all master-key locks removed from the exterior of emergency exits?

7.4.40 Are windows into the computer room replaced by secure partitions such as metal panels?

7.4.41 If windows into the computer room have been allowed to persist, are they secure glass (e.g., embedded-wire or laminated) to preclude shattering?

7.4.42 Is a badge-reader access-control system installed for the computer room and adjacent data center facilities?

7.4.43 If cipher (combination) locks are used, are the combinations changed immediately when personnel resign or are fired?

7.4.44 Are casual visitors prevented from learning and using door access codes?

7.5 Procedures

7.5.1 Is there a system of signatures to control access to critical areas, documents, and data?

7.5.2 Is there a control sheet to cross-reference console log number to CPU hours by shift?

7.5.3 If computerized access-control systems are in place, are violation reports analyzed (e.g., reports on piggy-backing by personnel entering through a door already opened by another employee)?

7.5.4 Is security documentation updated promptly when procedures or equipment are changed or newly implemented?

7.5.5 Are there periodic (e.g., quarterly) departmental review meetings on security and control procedures?

7.5.6 Have you and mail room staff or company messengers reviewed procedures for handling incoming and outgoing confidential mail and reports?

7.5.7 Is there a specific person or group assigned to review periodic reports on everyone who has access badges for data center areas?

8 Housekeeping

8.1 Is the data center free of accumulations of trash?

8.2 Is the data center free of

8.2.1 surplus or broken furniture?

8.2.2 tapes, canisters, straps or disk covers on top of drives

8.2.3 printouts or card decks?

8.2.4 newspapers and magazines at the console?

8.2.5 paper clips, rubber bands on the floor?

8.2.6 surplus tape rings (1 per tape drive maximum)?

8.2.7 surplus, disconnected or broken computer equipment?

8.2.8 extra, unused floor panels?

8.2.9 floor panels left out of place (when no one working on installation)?

8.3 Are equipment covers and work surfaces cleaned regularly?

8.4 Are floors washed regularly?

8.5 Are under-floor areas vacuumed regularly?

8.6 Are waste baskets

- provided with hinged covers?
- fire-resistant (e.g., metal rather than plastic)?
- emptied only outside the computer room to reduce dust discharge?

8.7 Is carpeting anti-static?

8.8 Are maintenance areas (e.g., where cleaning materials are kept) clean and tidy (to prevent spontaneous combustion, for example)?

8.9 Are all flammable materials (paper, inks, ribbons, boxes) kept to a minimum in the computer room?

8.10 Are food and drink absolutely forbidden in the computer room?

8.10.1 Have all employees been notified in writing of specific sanctions for bringing food into the computer room?

8.10.2 Are damp towlettes available just outside the computer room door to permit staff to clean their hands before entering the computer room if they have just eaten something?

8.11 Is smoking absolutely forbidden in the computer room?

8.12 Have all employees been notified in writing of specific sanctions for bringing smoking materials into the computer room?

8.13 In areas within the data center where smoking is permitted, are ashtrays

- Easily accessible?
- Self-extinguishing?

8.14 Are CCTV lenses regularly cleaned?

8.15 Are operator and maintenance manuals stored neatly in an assigned place adjacent to (but outside) the computer room?

8.16 Is there a prominent notice announcing AUTHORIZED PERSONNEL ONLY--OPERATORS MAY NOT ADMIT VISITORS WITHOUT AUTHORIZATION.

8.17 Are operators

8.17.1 neatly dressed (not necessarily formally, but clean)?

8.17.2 positive and helpful when responding to user calls or problems?

8.17.3 trained to refuse access to the computer room to unauthorized visitors no matter how high their apparent or claimed rank within the organization?

8.17.4 trained to phone for help if an unauthorized visitor (say, the CEO) demands admittance despite the posted restrictions?

8.17.5 trained to question unaccompanied visitors in the data center politely but firmly?

8.17.6 trained to report unusual events to their supervisors at once?

8.17.7 tested without warning and unpredictably by simulated anomalies on the computer systems?

8.18 Bulletin (cork) boards

8.18.1 Is all material on bulletin boards periodically inspected to remove obsolete information?

8.18.2 Are confidential data (e.g., the phone numbers for modems) kept off the bulletin boards?

8.19 Identification of critical equipment

8.19.1 Are all emergency shut-off valves and switches clearly labeled with signs visible across the computer room machinery?

8.19.2 Are normal settings posted beside controls such as thermostats and humidistats?

8.19.3 Are telephone numbers, contacts, and company names for maintenance on critical equipment posted on or next to the equipment?

9 Miscellaneous

9.1 Is there a plan for security and operations personnel for responding to civil disturbances?

9.2 Is there a liaison program with local law enforcement agencies?

9.3 Do personnel know how to handle and report telephone bomb threats?

9.4 Are report-distribution systems (e.g., racks or bins) remote from the computer room?

9.5 Are there intercom systems between the computer room and other areas within the data center and the building?

9.6 Are hinges of computer room doors on the inside only (inaccessible from outside)?

9.7 Are hinge pins for computer room doors welded on to prevent easy removal?

9.8 Are there astragals (protectors on the door edge) to preclude tampering with the latches?

9.9 Are doorframes solidly installed in the walls?

9.10 Are safety devices (e.g., fire extinguishers, hoses, flashlights) regularly inspected and, if possible, tested?

9.11 Are there first aid stations clearly marked and readily accessed in the computer room and throughout the data center?