

Physical Security Checklists

Management Considerations

Is the selection and purchase of PCs controlled?

Has a specific individual been assigned to the selection, purchase, and control of PCs

Is there PC equipment accountability?

Has a physical inventory been conducted of all PC equipment?

Do you fully realize the value of your PCs, the software, the applications, and the data being on your PC's?

Are you PC users made aware of security risks and vulnerabilities?

Do your PC users attend classes that instruct users on proper system handling and magnetic media handling?

Are the PC users informed of their security and control responsibilities?

Have written policies and procedures been prepared and implemented that govern the security and control of micro equipment and applications?

Are stringent controls placed on any PC use that could affect the accounting records of your company?

Are there adequate controls to protect against the invasion of privacy?

Are your internal/external auditors aware of your computer systems?

Do outsiders have access to your PCs?

Does top management approve of and support the use of PCs

Have emergency procedures been established to be followed in case of disaster or criminal act?

Has the amount of possible financial loss from disaster, criminal act, accident, etc., been determined?

Does the disaster recovery plan take into account multi-location PC operations?

Has a "test" disaster been conducted?

Have arrangements been made to replace the micro hardware and software in case of disaster?

Has someone been assigned responsibility for disaster planning?

Has the effect of short-term and long-term downtime of PC's been determined?

Could downtime result in loss of business, customer or employee dissatisfaction and/or loss of revenue?

If one PC is shut down, can another be utilized for necessary processing?

Vulnerability Assessment

Have you fully analyzed your exposure to these dangers:

Hardware

Electro-mechanical device failure

CPU failure

Disk unit head crash
Tape Drive failure
Environmental problems-dirt, dust, smoke
Circuit failure
Power problems-spikes, drops
Software
Operating systems problems
Programming errors
Faulty design
Insufficient testing
Poor or lost documentation
Virus
Magnetic Media
Physical damage of medium
Equipment malfunction
Software problems
Operator error
Operator mishandling
Erasure
Overwrites

Physical Security and Site Security

Is the perimeter security adequate?
Is the building's security adequate?
Access control
Proper lighting
Alarm systems
Environmental controls
Is internal security adequate?
Access control
Hardware security devices
Alarm systems
Environmental controls
Are doors and locks secure?
Keys or combinations controlled
Combinations changed frequently
Control Log kept
If card access systems are used, are cards controlled?
Is the work area secured during nonworking hours?
Have policies and procedures been developed for access controls?
Is access to electrical power controlled and secure?
Are floors and ceilings watertight?
Is there sufficient ventilation around PCs?

Is the PC placed away from water and steam pipes?
Is the PC placed near a window where:
People can view the materials being processed
Sight of the PC might tempt a thief
Are office furnishing fire resistant?

ENVIRONMENTAL CONCERNS

Housekeeping

Is the PC area and equipment kept clear of paper and paper residue?
Are wastebaskets emptied outside the computer area to reduce dust in the air?
Is carpeting and/or floor wax anti-static?
Are low fire hazard waste containers used?
Are only small amounts of cleaning solvents allowed in the area?
Is smoking prohibited?
Are liquids prohibited?
Is static electricity controlled?

Magnetic Media Handling

Are diskettes kept from being used as coasters for coffee cups or ashtrays?
Are diskettes kept from being staple, paper clipped, or bound with rubber bands?
Are diskettes properly stored and protected?
Are diskettes kept from being placed on top of or next to magnetic devices such as paper clip holders or copy holders? Are diskettes kept from being placed on top of or next to the radio or telephone?
Is the magnetic media degausser kept in a secure place and used with discretion?
Are magnetic media kept from being stored on window ledges or in someone's car?
Are approved external gummed labels used?
Are labels prepared prior to placing them on diskettes?

Electrical Power

Have electrical power monitoring and control devices been installed to protect against:
Voltage spikes/surges
Voltage dips/brownouts
Power interruptions

Noise interference

Fire and Water Protection

Are CO2 or Halon fire extinguishers strategically located, properly marked, and accessible?

Are personnel trained on the use of fire extinguishers?

Have fire/smoke sensors been placed in the areas where PCs are located?

Have the fire extinguishers been inspected recently?

Have water alert systems been installed?

Are protective covers available for the PC equipment and other electrical equipment?

Hardware Security

Has an inventory log of all PCs and their peripherals been prepared that contains the following information: Description of hardware device

Model number

Memory storage

Manufacturer's serial number

Warranty number

Place of purchase

Date purchased

ID number engraved on unit

Has a control log on all PCs been established that contains the following information:

Description of device

Manufacturer's serial number

Company identification number

Date/Time checked out

Date/Time checked in

Authorized signature

Has each component of the peripheral been marked/etched with identification number?

Are PCs secured with hardware security devices that prevent theft of the equipment or removal of circuit boards?

Have personnel controls been established for the use of each PC?

Authorizations by application

Is an operations control log kept for each PC that contains the following information:

System Identification

Date

User ID

Time signed on

Time signed off

Job(s) processed

Do you have backup available for your vital computer hardware equipment?

Have you kept an accurate and complete inventory of your current PC specifications and configurations including:

Number and type of PCs

Number and type of tape drives
Number and type of disk drives
Number and type of printers
Number and type of diskette readers
Number and types of other peripherals or components
Have you determined what is the acceptable downtime for each piece of equipment at your location?
Short-term
Long-term
If hardware failures occur. Do you have an alternate method for processing?
Do you have a backup system available
On site?
Off site?
Alternate sites?
Loaner equipment?
Is your backup site location close enough to allow smooth recovery operations?
Is your current PC so outdated or unique that backup equipment is hard to find?
Are personnel trained in the procedures for:
Orderly shutdown of hardware
Orderly power-up of hardware
Manual processing in case of system failure
Is your software protected legally?
Copyright
Patent
Trade secret
Employee contract
Has a company identification and protection statement been embedded in each source program?
Are protection hardware/software devices being used to protect the company's proprietary software?
Have the following controls been placed on sensitive programs including new programs and program changes:
Control list of sensitive programs
Program name/description
Programmer responsible for the program
Appropriate storage of sensitive programs and related documentation
Documentation check in/out logs
Restrictions against program patching
Management review of changes or requests for changes
Audits of program changes
Review and approval of test results
History log of programs and changes

Documentation Security

Is it possible for the wrong version of a program to be run?
Is identical backup operating software available?
Have you tried running your operating system on your backup computer?
Have you defined and listed which application programs are vital to your operation?
Do you copy these programs at regular intervals?
Do you maintain a copy of the source code?
Do you maintain a copy of the object code?
Do you maintain a set of test data (including the desired test results) for each application system for testing at the backup location?
Are your applications programs written so not to depend on any one particular piece of hardware?
Have you provided adequate security for on-site and off-site software and documentation storage?
Are your storage cabinets and safes resistant to:
Burglary
Fire
Water
Smoke
If you use vendor-supplied software, is there a clause in the contract which extends the terms of the license agreement to permit use of the software and backup, security, and control?
Is there a person assigned specific responsibility for software backup, security, and control?
Are surprise inventories taken of the software maintained at the backup location?
Have you established "waiting periods" which indicate a need for action. For example, a list of run times (approximate) should be maintained to determine if a program has run properly?

Data Security and Records Management

Have you classified the value of your data records into classes of: vital, important, useful, and nonessential?
Input records
Source documents
Control documents
Magnetic media records
Programs
Output data
Do you understand and comply with legal record retention regulations?
Internal Revenue Service
Insurance
Legal Considerations
Customer/product history information
Have you evaluated the possible types of threats and vulnerabilities that your records/files

may be exposed to:

Data entry errors

Data transmission errors

Mechanical malfunctions

Program errors

Updating of wrong file

Operator errors

Lost files

Defective magnetic media

Theft of records

Criminal activity

Loss by natural disaster

Do you maintain duplicate copies of your vital records?

Do you maintain a list of critical vital files?

Do you maintain reconstruction capability for your paper and magnetic files (preferably in the generation approach)?

Do you maintain daily file dumps and transaction files for reconstruction purposes?

When you copy magnetic files for off-site storage, do you first check the copies for readability and accuracy?

Are your on-site and off-site magnetic media storage cabinets:

Fire resistant

Water resistant

Smoke resistant

Removable (make sure they fit through doors)

Secure

Do you microfilm records as an additional means of providing backup?

Is there a procedure for evacuating critical files in case of emergency?

Is access to information on PC databases strictly controlled?

Are there ways of ensuring that the version of a data file is being used?

Can outdated files be processed accidentally?

Does software provide for internal label checking?

COMMUNICATIONS ACCESS CONTROL

Access Control

Are one or more of the following access control provided?

Passwords

Card key access

Key lock

Access logs

Communications Backup

Have you determined the effect of short or long term communications failure on:

Batch processing communications system

On-line real time processing

Local communications network

Remote communications network

Have you made and tested backup plans in case of total, long-term failure of your communication system?

Does your backup communication system take into account:

Mail

Radio communications

Manual procedures

Alternate networks

Does your backup site contain similar communications capabilities to your primary site?

Hardware

Software

Communication utility service

Proper cables and connectors

Is your communication system fully documented?

Depending upon the sensitivity of your information, have you taken into consideration:

Communication hardware security

Means of identifying the terminal user

Has the communications hardware at your backup site been tested?

Incoming File Security

Are personnel made aware of the possible dangers attached to incoming incoming diskettes and files?

Have you established a clean-room procedure for checking all incoming files and diskettes?

Are policies and procedures for use of bulletin board and online services written and implemented?

Virus Recovery

Are all data files routinely backed up

Do you have a separate hard drive or PC available in case of a suspected VIRUS attack so that the PC may be examined by experts without interruption of work flow?

Are you using a data protection utility that will detect unwanted activity before data destruction can take place?