

APPENDIX 1

SAMPLE RISK ASSESSMENT CHECK-LIST

This is a **sample** risk assessment checklist that can be used as a tool to analyze vulnerabilities in your data system. This checklist is not all-inclusive and does not address all areas of data and processing system vulnerabilities. University Audit or external audit firms are good resources for application administrators interested in obtaining additional or more technology specific audit/assessment checklists.

Additionally, items on this checklist may not apply to every environment (e.g., mainframe, mini, LAN/WAN, PC in office) or every situation however all items should be considered and addressed.

PHYSICAL SECURITY - GENERAL

Item	YES	NO	N/A
Location:			
not a target for vandals	___	___	___
not advertised	___	___	___
not readily accessible by general public (in a student lab?)	___	___	___
away from high traffic areas or glass enclosures	___	___	___
close to emergency response units (e.g., Fire Dept.)	___	___	___
separate from user location	___	___	___
not close to rail lines	___	___	___
not close to airports	___	___	___
not close to manufacturing or chemical plants	___	___	___
not close to research facilities with toxic waste	___	___	___
not close to landfills	___	___	___
Photo-badge systems used	___	___	___
Sign-in log at entrances	___	___	___
Policy to challenge unfamiliar visitors	___	___	___
Visitors required to wear badges	___	___	___
Entrance security devices requiring keys, pass-codes or magnetic badges	___	___	___
Security system monitored 24 hours/day, 7 days a week	___	___	___
Controlled access to computer during working hours	___	___	___
Controlled access to computer during off-shift hours	___	___	___

PHYSICAL SECURITY - GENERAL (Cont'd)

Item	YES	NO	N/A
Limit computer room access to operators and other employees with job duties requiring physical access to equipment	___	___	___
Control physical access to data libraries and files (whether paper, tape, cassette, CD, etc.)	___	___	___
Published security policy/guidelines/procedures	___	___	___
Internal staff access controlled in vital/restricted areas	___	___	___
Internal staff access supervised in vital/restricted areas	___	___	___
Authorized vendor service personnel list prepared	___	___	___
Require positive identification of vendor personnel	___	___	___
Vendor service personnel supervised while on premises	___	___	___
Age of infrastructure	___	___	___
Control access to communications facilities/phone rooms	___	___	___
Collect keys and badges and/or change codes when employees terminate	___	___	___

PHYSICAL SECURITY - MICROCOMPUTERS/PORTABLES

Item	YES	NO	N/A
Individuals authorized to use the microcomputer have been identified	___	___	___
Microcomputer protected from unauthorized access	___	___	___
microcomputer secured (e.g., has a locked cover/cabinet, is bolted/cabled to desk)	___	___	___
microcomputer is in a locked room	___	___	___
microcomputer has a locked power supply	___	___	___
microcomputer drive key is not left in machine and is properly secured	___	___	___
processing unit is locked so that the cover cannot be removed and internal boards removed	___	___	___
Microcomputers are password protected (installed chip)	___	___	___

PHYSICAL SECURITY - MICROCOMPUTERS/PORTABLES (Cont'd)

Item	YES	NO	N/A
Data storage media (e.g., tapes, disks, CD-ROM, etc.) are properly secured in a media safe rated by Underwriters Laboratories	___	___	___
An inventory (including serial and University equipment tag #) of microcomputers, laptops and other portable components is maintained	___	___	___
All microcomputers and laptops are marked in some way to indicate they are the property of the University and to help recover stolen hardware	___	___	___
Non-removable labels are attached to:			
the microcomputer	___	___	___
the laptop	___	___	___
the laptop's case	___	___	___
Non-breakable cables are used to attach laptops to desks or other heavy, stationary furniture	___	___	___
Check out procedures are used and monitored to keep track of who has specific laptops	___	___	___
Employees sign statements of responsibility for taking due care of the laptops and the data on them	___	___	___
Laptops are securely packed for travel	___	___	___
Laptops are not checked as airline baggage	___	___	___
Laptops are not passed through x-ray machines (data stored on hard drives and disks can be damaged)	___	___	___
Laptop cases meet airline safety standards	___	___	___
Laptops are checked in at hotel desk safes or cabled at when not in use (e.g., at night, during the day while left in room, etc.) to stationary furniture in the hotel room	___	___	___

ENVIRONMENTAL CONTROLS
FLOOD/WATER

Item	YES	NO	N/A
Equipment located above water grade	___	___	___
Steam or water pipes located below computer	___	___	___
Adequate water drainage: under raised floor	___	___	___
on floors above	___	___	___
in adjacent areas	___	___	___
Water detection devices located under raised floor (equipment room)	___	___	___
Adequate water leak controls	___	___	___
Inform employees of procedure to report water leak or of location of water pipe shut-off valves	___	___	___
Age of water mains	___	___	___
Equipment located away from sprinkler heads	___	___	___
Equipment located away from restrooms, cafeterias, etc.	___	___	___
Sealed windows	___	___	___
Covers for equipment in case of sprinkler release available and located near equipment	___	___	___
HOUSEKEEPING			
Flammable materials properly stored	___	___	___
Office, equipment room and area under raised floor cleaned regularly	___	___	___
Print room separate from equipment room/printers not located near hard drives/CD-ROM drives	___	___	___
Paper, supplies and trash stored outside equipment area, desktop location, computer room	___	___	___

ENVIRONMENTAL CONTROLS

HOUSEKEEPING (Cont'd)

Item	YES	NO	N/A
No asbestos on utility steam pipes	___	___	___
A no smoking policy in the office/equipment room	___	___	___
A no eating or drinking policy near desktop systems or in the equipment room/computer room	___	___	___
Subfloors properly sealed	___	___	___
Precut raised flooring panels for offsite use	___	___	___
Slots/components of laptops are protected from dust, rain, etc. (e.g., waterproof carrying case)	___	___	___

FIRE CONTROL

Fire resistant/noncombustible materials used for:			
buildings	___	___	___
partitions, walls, doors	___	___	___
furnishings	___	___	___
Solid walls constructed to extend to the true ceiling of each floor	___	___	___
Smoke and heat detectors installed, including above ceiling and below floors	___	___	___
A/C facilities automatically deactivated by smoke detectors	___	___	___
Smoke detector system tested periodically	___	___	___
Automatic carbon dioxide fire extinguishers	___	___	___
Hand-held carbon dioxide fire extinguishers	___	___	___
Hand-held water fire extinguisher	___	___	___

ENVIRONMENTAL CONTROLS

FIRE CONTROL (Cont'd)

Item	YES	NO	N/A
Adequate (i.e., size and type) fire extinguishers located with floor lifter tools in the data center's raised floor areas	___	___	___
Adequate (i.e., size and type) fire extinguishers located in equipment room/lab or office	___	___	___
Fire extinguishers easily accessible, with type and use identified	___	___	___
Fire extinguishers inspected and tested regularly	___	___	___
Established current emergency fire procedures and evacuation plan	___	___	___
Require all employees to read emergency fire procedures	___	___	___
Staff trained on each shift for fire-related procedures	___	___	___
Fire drill conducted on all shifts in the past 12 months	___	___	___
Post fire department's phone number on/near each phone	___	___	___
Close liaison established with the local fire department	___	___	___
Training for all employees in fire prevention	___	___	___
Alarm pull-boxes installed	___	___	___
Smoking restricted in the offices and equipment areas/computer room	___	___	___
Emergency power switches located at exits	___	___	___
Air conditioning system tied to emergency power switches	___	___	___
Fire alarms tested every 12 months	___	___	___
Emergency exit diagrams posted near all exits	___	___	___
Regular fire prevention inspections	___	___	___
Fire exits clearly identified and kept open	___	___	___

ENVIRONMENTAL CONTROLS

FIRE CONTROL (Cont'd)

Item	YES	NO	N/A
Multiple alarm zones	___	___	___
Audible and visible alarms	___	___	___
Fire detection system monitored 24 hours/day, 7 days a week	___	___	___
Limited number of staff with knowledge of fire detection codes, if applicable	___	___	___

ELECTRICAL POWER

Reliable electrical power	___	___	___
Power lines checked with a power line monitor	___	___	___
Power supply monitored and recorded	___	___	___
Power regulators installed to protect against spikes/brownouts	___	___	___
Surge Protectors or line filters used on all desktop systems	___	___	___
Master power shutdown controls for computer	___	___	___
Backup power available with appropriate size UPS	___	___	___
Emergency power available for gradual power-down	___	___	___
Emergency lights installed and working	___	___	___
Microcomputer on separate power line from other office equipment	___	___	___

ENVIRONMENTAL CONTROLS

CLIMATE CONTROL

Item	YES	NO	N/A
Separate HVAC system for the computer room	___	___	___
System protected from accidental and/or intentional shut-down	___	___	___
Controlled humidity	___	___	___
Static electricity controlled by adequate humidity levels	___	___	___
periodic spraying with anti-static spray	___	___	___
use of antistatic mat under the chair/table on which the microcomputer sits	___	___	___
Backup air conditioning facilities available	___	___	___
Air conditioning shut-off readily accessible	___	___	___
Air conditioning filtration and filters cleaned annually	___	___	___
Preventive maintenance schedule observed	___	___	___
Laptop is protected from vibrations or temperature extremes during travel	___	___	___
A sufficient amount of time is allowed before a portable computer is turned on so it can adjust to room temperature and humidity, especially in very cold or hot climates	___	___	___

PERSONNEL CONSIDERATIONS

Adequate number of personnel to perform job function(s)	___	___	___
Personnel trained in security awareness and proper computer security practices (backing up data, offsite storage, password changing, keeping magnets away from disks/diskettes, etc.)	___	___	___

PERSONNEL CONSIDERATIONS (Cont'd)

Item	YES	NO	N/A
Personnel properly trained	___	___	___
training programs for the equipment are available	___	___	___
training programs for the software are available	___	___	___
proficiency testing is part of the equipment authorization procedure	___	___	___
training programs for policies, guidelines, procedure and applicable state/federal laws are available	___	___	___
Personnel trained in business functions of work area	___	___	___
Controls established for terminating/transferring employees	___	___	___
Policies, Guidelines and Procedures available to and understood by employees:	___	___	___
Drug and alcohol abuse	___	___	___
Data Security and Classification Guidelines	___	___	___
Electronic Mail Guidelines	___	___	___
Computer Security and Usage Guidelines	___	___	___
WWW Guidelines	___	___	___
Business Continuity Guidelines	___	___	___
Records Management and Disposition Guidelines	___	___	___
Network/LAN Guidelines	___	___	___
Microcomputer/PC Guidelines	___	___	___
Other Computing and Data Guidelines	___	___	___
Harassment	___	___	___
Termination Procedures	___	___	___
Cross-training	___	___	___
Vacations	___	___	___
Appropriate actions are taken when individual are found to be violating University Policies/Guidelines and Campus Procedures	___	___	___
Authorized users have signed a computing awareness and data security compliance statement	___	___	___

COMPUTER USAGE

University's computer <i>systems</i> are used for purposes related to its missions of education, research and public service including instruction, research, administrative tasks and collaborative activities with other entities, including but not limited to colleges/universities and private businesses	___	___	___
--	-----	-----	-----

COMPUTER USAGE (Cont'd)

Item	YES	NO	N/A
Computing resources are not used for commercial purposes not related to the University missions	___	___	___
Only authorized users have access to University computer systems	___	___	___
Invalid attempts to access the computer system are:			
logged	___	___	___
monitored	___	___	___
limited to a specific number	___	___	___
Authorized users have unique logon IDs or operator IDs, and passwords to access University computers and their application systems	___	___	___
User passwords are not reusable:			
microcomputer	___	___	___
network/LAN	___	___	___
mainframe	___	___	___
Users are not allowed to share Logon/operator IDs and passwords	___	___	___
Passwords are used to access all computer systems in which Private Restricted, Confidential (as defined by University Data Security and Classification Guidelines) or critical data is stored or maintained	___	___	___
Passwords used to access computer systems containing Private, Restricted or Confidential data (as defined by University Data Security and Classification Guidelines) are at least 6 characters	___	___	___
Pin numbers used to access Private, Restricted or Confidential data (as defined by University Data Security and Classification Guidelines) are at least 6 characters	___	___	___
Restricted access to password file	___	___	___
Authorized user change their passwords periodically			
mainframe	___	___	___
network	___	___	___
microcomputer	___	___	___

COMPUTER USAGE (Cont'd)

Item	YES	NO	N/A
Computerized password creation checking is implemented for administrative and research computer systems on networks carrying administrative and research data	___	___	___
Smart card or token-based security is implemented on all workstations and microcomputers/PCs that access Private, Restricted or Confidential data	___	___	___
Passwords or pin numbers(e.g., mainframe, network/LAN, microcomputer, laptop, etc.) are not stored in: <ul style="list-style-type: none"> batch files in automatic login scripts in terminal function keys in computers without access control hardcoded in any computer program 	___	___	___
User passwords (e.g., mainframe, Network/LAN, microcomputer, laptop, etc.) are not sent unencrypted over electronic mail or unsecured networks.	___	___	___
The display and printing of passwords or pin numbers is masked, suppressed, or otherwise obscured such that unauthorized parties will not be able to observe or subsequently recover them	___	___	___
Passwords are required on all computer systems on which Private, Restricted, Confidential or critical data is transmitted, stored or Maintained.	___	___	___
Administrative and research computer systems displays a notice at log-in (i.e., login banner) stating that the system is to be used by authorized users only and that by continuing to use the computer system, the individual represents themselves as an authorized user	___	___	___
Computer system "idle time" or "time-out" capabilities are implemented for: administrative and research computer systems on networks carrying administrative and research data	___	___	___

COMPUTER USAGE (Cont'd)

Item	YES	NO	N/A
Logged on microcomputers are not left unattended	___	___	___
All job or course specific access granted to an authorized user is removed when that user transfers from one department to another or when a course is completed. All computer access granted to an authorized user will be removed when that user terminates employment, graduates, or withdraws from the University, or when their courtesy account is inactive/unneeded	___	___	___
Security tokens and/or passwords are not kept in laptop cases	___	___	___
Laptops are not programmed with passwords, phone numbers, or ids	___	___	___
Instructions for dialing into Administrative or Research computer systems are not kept in laptop cases	___	___	___
Academic game development, computer security research, and the investigation of self-replicating code is allowed on the computer system	___	___	___

HARDWARE CONSIDERATIONS

Operations compared to scheduled activities	___	___	___
All periods of reported downtime verified	___	___	___
Incoming work checked against an authorized user list	___	___	___
Output spot-checked for possible misuse	___	___	___
Output distribution lists updated periodically	___	___	___
Tapes and disks cleaned at regular intervals	___	___	___
Equipment/network configurations documented/standardized	___	___	___
Equipment upgraded as needed, to ensure business functions can be performed	___	___	___
Equipment upgrades planned to minimize: employee disruption	___	___	___
job function disruption	___	___	___

HARDWARE CONSIDERATIONS (Cont'd)

Item	YES	NO	N/A
Equipment upgrades address issues of incompatibility	___	___	___
Equipment reviewed for utility periodically and obsoleted as needed	___	___	___
Only systems/security administrators or their designees modify the configuration of the University or Campus computing infrastructure by adding or removing network links, computers, or peripherals	___	___	___
Tape and disk records maintained - what is on what disk and where is backup	___	___	___
Preventive maintenance schedule observed	___	___	___
Restricted Access to Disk Drives/ Driveless Systems	___	___	___
Restricted use of personal equipment for University business	___	___	___

SOFTWARE CONSIDERATIONS

Software upgraded as needed, to ensure business functions can be performed	___	___	___
Software upgrades planned to minimize: employee disruption job function disruption	___	___	___
Software upgrades address issues of incompatibility to previous versions, etc.	___	___	___
Software reviewed for utility periodically and obsoleted as needed	___	___	___
Only Administrative and research computer systems contain audit trails to monitor access and modification to critical operating system components	___	___	___
Master and backup copies of software is secured	___	___	___

SOFTWARE CONSIDERATIONS (Cont'd)

Item	YES	NO	N/A
Documentation (operating system, application, communication, etc.) is secured	___	___	___
Operating system and application software are backed up as needed	___	___	___
Software backups (e.g., operating and application software) are regularly stored off-site	___	___	___
Access to operating software is restricted	___	___	___
Access to production software is restricted	___	___	___
The use of personal software for University business is restricted	___	___	___
Employees are aware of and understand software licenses	___	___	___
Copyrighted software is not copied unless explicitly allowed in the software license agreement	___	___	___
Anti-virus software is installed and continuously enabled on all:			
microcomputers	___	___	___
laptops	___	___	___
networks	___	___	___
Anti-virus software installed on laptops and microcomputers is configured so that it is automatically run during the boot process	___	___	___
Shareware and public domain software are:			
installed	___	___	___
properly used	___	___	___
Multilevel access to files is controlled by:			
groups	___	___	___
job function	___	___	___
levels of security	___	___	___
breakdowns within files	___	___	___
restrictions (read-only, write-only, etc.)	___	___	___
Security software and access codes are validated	___	___	___

SOFTWARE CONSIDERATIONS (Cont'd)

Item	YES	NO	N/A
Logs of access to Confidential, Restricted, or Private data files (as defined by University Data Security and Classification Guidelines) are: maintained	___	___	___
monitored	___	___	___
Unauthorized access attempts to Confidential, Restricted, or Private data files (as defined by University Data Security and Classification Guidelines) are: logged	___	___	___
monitored	___	___	___
Operating system security bypass protection is built-in	___	___	___
Operating system change control and testing procedures are implemented	___	___	___
ACCESS/DATA/FILE CONTROLS			
Restart/recovery procedures exist for application programs	___	___	___
Program change documentation and control procedures are implemented	___	___	___
Software is backed-up before system change: operating system	___	___	___
application	___	___	___
Source code escrow agreements are used	___	___	___
Information is safeguarded by security systems designed for the protection of, detection of, and recovery from the misuse of information resources	___	___	___
A specific individual(s) has/have administrative responsibility for data access authorization (i.e. data custodians)	___	___	___
When records are created, two classifications are assigned to the record: a data security classification based on the University levels of data classification	___	___	___
a retention designation based on legal, administrative, research and historical requirements	___	___	___

ACCESS/DATA/FILE CONTROLS (Cont'd)

Item	YES	NO	N/A
Confidential, Restricted and Private data (as defined by University Data Security and Classification Guidelines) has been identified	___	___	___
Confidential, Restricted and Private data (as defined by University Data Security and Classification Guidelines) are encrypted	___	___	___
Confidential, Restricted and Private data (as defined by University Data Security and Classification Guidelines) contain audit trails to monitor access and modification	___	___	___
Fireproof and waterproof containers/storage are used for original and backup:			
programs	___	___	___
documentation	___	___	___
data files	___	___	___
A current inventory of application files is maintained	___	___	___
Program files stored at off-site facility are tested periodically	___	___	___
Duplicate rather than the original program file is used for changes	___	___	___
Duplicate copies documentation stored off-site are verified periodically	___	___	___
Data files are physically controlled by:			
computer center personnel	___	___	___
the application administrator	___	___	___
Only authorized users have access to University data	___	___	___
Access to data other than unclassified data is denied unless the user has obtained explicit approval by the data custodian	___	___	___
Access to data classified as Private, Restricted or Confidential is based on legal requirements or on a need to know; job function; or course requirement basis	___	___	___
Access to data is given to authorized users only	___	___	___
Access to data is not shared, transferred or delegated (e.g., authorized users do not log on, access data and then let others use that data)	___	___	___

ACCESS/DATA/FILE CONTROLS (Cont'd)

Item	YES	NO	N/A
Authorized users:			
use their access to University data for approved purposes only	___	___	___
logoff University computer systems if they will not be accessing data for an extended time	___	___	___
do not use University applications and their data in illegal activities	___	___	___
do not view or access data, in any medium and/or form, for which they are not approved	___	___	___
understand the data they are accessing and the level of protection required	___	___	___
set file protections correctly when they create or copy a file	___	___	___
periodically "refresh" downloaded data to ensure they are working with accurate, up-to-date data	___	___	___
Programs and files are confidential unless they have explicitly been made available to other authorized users	___	___	___
Classified data is not copied without prior approval	___	___	___
Vendors, contractors, consultants and external auditors needing access to University data have read, and acknowledge in writing that their firm has read, understood and will comply with the University Data Security and Classification Guidelines and Campus procedures	___	___	___
Data, regardless of medium and/or form, is:			
identified as to its classification (i.e. Unclassified, Operational Use Only, Private, Restricted or Confidential)	___	___	___
accessed in a manner commensurate with the data's classification and with University Records Management, Disposition and Retention Policies/Guidelines/Schedules and Campus procedures	___	___	___
used of in a manner commensurate with the data's classification and with University Records Management, Disposition and Retention Policies/Guidelines/Schedules and Campus procedures	___	___	___
disposed of in a manner commensurate with the data's classification and with University Records Management, Disposition and Retention Policies/Guidelines/Schedules and Campus procedures	___	___	___

ACCESS/DATA/FILE CONTROLS (Cont'd)

Item	YES	NO	N/A
secured against unauthorized - creation	___	___	___
update	___	___	___
deletion	___	___	___
processing	___	___	___
distribution	___	___	___
not accessible to non-approved users when not in use	___	___	___
Aggregates of data are classified as to the most secure classification level (e.g. when data of mixed classification exist in the same database, file, report, etc., the classification of that database, file, or report should be that of the highest level of classification)	___	___	___
Databases containing Operational Use Only, Private, Restricted or Confidential data are secured	___	___	___
Extracts of Operational, Private, Restricted or Confidential data are secured at the same level as the file/database from which the data was extracted	___	___	___
Reports containing Operational Use Only, Private, Restricted or confidential data are disposed of properly:	___	___	___
paper is shredded	___	___	___
microfiche/film is shredded	___	___	___
disks/ hard drives are erased so as to be unretrievable	___	___	___
Access to data storage (e.g., onsite and offsite, vault, cabinet, etc.) is specifically controlled	___	___	___
Applications requiring electronic authorization use the level of secure authorization most appropriate for their data's classification	___	___	___
Electronic vaulting is used	___	___	___
Confidential, Restricted and Private data (as defined by University Data Security and Classification Guidelines) is appropriately backed up to allow for recovery	___	___	___
Copies of critical data are stored outside the computer room/office	___	___	___

ACCESS/DATA/FILE CONTROLS (Cont'd)

Item	YES	NO	N/A
University data, regardless of medium and/or form, is disseminated by officially designated offices only	___	___	___
Deleted and erased data is really destroyed or overwritten so it can not be recovered by utility programs	___	___	___
Confidential, Restricted and Private data (as defined by University Data Security and Classification Guidelines) are properly managed when downloaded	___	___	___
Confidential, Restricted and Private data (as defined by University Data Security and Classification Guidelines) is used for analysis only and not permanently stored on diskettes or hard drive units	___	___	___
Confidential, Restricted and Private data (as defined by University Data Security and Classification Guidelines) stored at the microcomputer level is encrypted or protected with password access	___	___	___

COMMUNICATIONS/NETWORK CONSIDERATIONS

All communications lines backed up	___	___	___
Dual paths to processor for all communications lines exist	___	___	___
Alternate path to backup for all communications lines exist	___	___	___
Telephone company junction boxes are secure	___	___	___
Access to dial-up telephone numbers is restricted (i.e., need-to know basis only)	___	___	___
Dial-up lines are monitored for repeated failed access attempts	___	___	___
Mainframe operator is notified of repeated violations	___	___	___
Line is disconnected after repeated violations	___	___	___

COMMUNICATIONS/NETWORK CONSIDERATIONS (Cont'd)

Item	YES	NO	N/A
All accesses and access attempts are logged:	___	___	___
user identified	___	___	___
date and time of access are identified	___	___	___
functions performed are identified	___	___	___
microcomputer is identified	___	___	___
Dialup access is restricted to authorized users only	___	___	___
dial-back installed	___	___	___
Confidential, Restricted or Private data (as defined by University Data Security and Classification Guidelines) transmitted over public lines is encrypted	___	___	___
Standard mainframe access control measures are employed once the dial-up connection has been made	___	___	___
Network control function password is protected	___	___	___
Access to the network control center is restricted	___	___	___
Can anyone configure and change management system access from anywhere in the network	___	___	___
Are Firewall(s) installed and implemented	___	___	___
using screening router(s)	___	___	___
using bastion host	___	___	___
using screened host gateway	___	___	___
using screened subnet	___	___	___
using proxy gateway	___	___	___
which support encryption	___	___	___
in a single tier configuration	___	___	___
in a multi-tier configuration	___	___	___
Are intrusion detection sensors implemented	___	___	___
Is a Virtual Private Network (VPN) installed and implemented	___	___	___
Is only email traffic allowed through the firewall	___	___	___
Is access to the mainframe restricted to intranets only by IP address	___	___	___

COMMUNICATIONS/NETWORK CONSIDERATIONS (Cont'd)

Item	YES	NO	N/A
Are domain name service names public	___	___	___
Are the following ports open for remote connection			
port 23 (Telnet)	___	___	___
port 80 (http)	___	___	___
port 25 (sendmail)	___	___	___
port 143 (IMAP mail server)	___	___	___
Are PING requests allowed	___	___	___
Are FINGER requests allowed by University connections only	___	___	___
Are anonymous connections allowed	___	___	___
Are proxy logins allowed	___	___	___
Is FTP controlled by a proxy server	___	___	___
Network failure detection equipment is in use	___	___	___
Communications failure troubleshoot/correction procedures	___	___	___
Network troubleshooting procedures updated regularly	___	___	___
Vendor list for trouble calls available	___	___	___
Vendor list regularly updated	___	___	___
Multiple carrier connections	___	___	___
Switchable network topology based on intelligence embedded into carrier backbone networks	___	___	___
Records of cabling plan offsite	___	___	___
Critical network circuits tagged	___	___	___
Offsite records to restore voice foundation systems	___	___	___
Unattended units logged off or turned off when not in use	___	___	___

COMMUNICATIONS/NETWORK CONSIDERATIONS (Cont'd)

Item	YES	NO	N/A
Screensaver passwords are used to protect desktop	___	___	___
Both public and private files are maintained on the network private files are secure from “browsing” by unauthorized users	___ ___	___ ___	___ ___
PBX			
Passwords used to access the maintenance ports are secured and controlled	___	___	___
VOICE MAIL			
Call forwarding is allowed only to: Campus exchanges University exchanges “local” exchanges	___ ___ ___	___ ___ ___	___ ___ ___
Voice Mail Mailbox passwords are: secured changed periodically of sufficient length to protect against hacking are not guessable	___ ___ ___ ___	___ ___ ___ ___	___ ___ ___ ___
Voice Mail does not allow the caller to obtain a dialtone thereby allowing calls anywhere in the public network, including international calls	___	___	___
Automated call directors/distributors do not allow the caller to obtain a dialtone thereby allowing calls anywhere in the public network, including international calls	___	___	___
TFMS calling codes (e.g., for long distance and international calls) are secured	___	___	___
Long distance and international calls made with TFMS calling codes are: Logged Monitored	___ ___	___ ___	___ ___
Confidential, Restricted or Private data is not discussed over unencrypted/ scrambled cellular phone transmission	___	___	___

COMMUNICATIONS/NETWORK CONSIDERATIONS (Cont'd)

Item	YES	NO	N/A
Offsite records to restore data communications equipment are maintained:			
Modems	___	___	___
Multiplexors	___	___	___
Matrix switches	___	___	___
Data PBXs	___	___	___
Bridges	___	___	___
Routers	___	___	___
Protocol Converters	___	___	___
Front End Processors	___	___	___
Concentrators	___	___	___
Digital Access and Cross Connect System	___	___	___
Subscriber Loop Carrier Cable Systems	___	___	___

CONTINGENCY PLANNING

Risk analyses (including a review of implemented controls) are performed annually on existing data systems	___	___	___
Risk analyses (including a review of controls) are performed as part of the implementation of a new critical or impacting data system	___	___	___
Multiple generations of operating system, application and data backups are be maintained in both on-site and off-site storage facilities	___	___	___
Copies of reciprocal agreements, or service bureau or hot/ cold site are kept at an off-site location	___	___	___
A formal written business resumption plan (BRP) is available which contains the following information:	___	___	___
a clarification of what constitutes a disruption (what level/extent of disruption) for which the specific BRP needs to be implemented	___	___	___
the maximum acceptable downtimes which can be incurred (i.e., how long the unit/University can function before the data system must be available)	___	___	___
who determines whether the incident is classified as a business disruption	___	___	___

CONTINGENCY PLANNING (Cont'd)

Item	YES	NO	N/A
who determines what level of disruption has occurred	___	___	___
who determines to what degree the BRP needs to be implemented	___	___	___
which staff are involved in the business resumption effort (part of the resumption team and at what disruption level are they involved	___	___	___
resumption team member responsibilities	___	___	___
how the non-availability of certain key team members is addressed	___	___	___
step-by-step, definitive procedures for each team member	___	___	___
plans for cross-training on team member duties	___	___	___
contact names and phone lists exist updated quarterly	___ ___	___ ___	___ ___
call initiation procedures updated quarterly	___ ___	___ ___	___ ___
the location of the BRP coordination site	___	___	___
what information about the disruption is made public	___	___	___
how information about the disruption is disseminated	___	___	___
an inventory of all critical resources necessary to resume processing including, but not limited to:	___	___	___
software (systems and applications)	___	___	___
communication requirements (front-end processors, lines, modems, etc.)	___	___	___
physical site requirements for an alternate facility, including air conditioning	___	___	___
power	___	___	___
raised floor	___	___	___

CONTINGENCY PLANNING (Cont'd)

Item	YES	NO	N/A
cabling	___	___	___
communications	___	___	___
total square footage (personnel and office space needs, etc.)	___	___	___
hardware and peripherals (e.g., PCs, printers, etc.)	___	___	___
data files (including format - MAC, DOS, etc.)	___	___	___
forms/documents	___	___	___
vendor support	___	___	___
staff security - this should include any modifications to physical, data, and networks needed to allow the resumption team members to implement the BRP	___	___	___
office equipment (e.g., telephones, copiers, typewriters, fax machines, etc.)	___	___	___
storage for supplies, forms, etc.	___	___	___
funding and acquisitions	___	___	___
transportation logistics for -			
personnel	___	___	___
supplies	___	___	___
input/output delivery	___	___	___
data back-up schedules	___	___	___
off-site storage procedures	___	___	___
contracted or agreed upon alternate facilities/operating sites	___	___	___
hot site	___	___	___
cold sites	___	___	___
service bureaus	___	___	___
shared sites (i.e., reciprocal agreements)	___	___	___
the type and level of hardware and software vendor support required	___	___	___
available	___	___	___
contracted	___	___	___
hardware and software (system and application) restore procedure	___	___	___

CONTINGENCY PLANNING (Cont'd)

Item	YES	NO	N/A
the off-site location of data (whether paper, tapes, cassettes, disks, etc.)	___	___	___
duplicate copies of documentation	___	___	___
BRP	___	___	___
system/application manuals	___	___	___
contracts	___	___	___
procedure manuals	___	___	___
supplies and forms	___	___	___
a schedule for BRP testing	___	___	___
procedures for -			
documenting formal plan tests and test results	___	___	___
following up these tests	___	___	___
implementing corrective actions/recommendations	___	___	___
BRP is tested:			
at least annually	___	___	___
using various testing approaches	___	___	___
BRP training is regularly conducted	___	___	___
An uninterruptible power supply (UPS) is installed	___	___	___
Parallel or backup systems are implemented for:			
network./LAN	___	___	___
PBX	___	___	___
Back-up computer system is available:			
hot site	___	___	___
cold site	___	___	___
alternate processing site (i.e. reciprocal agreement)	___	___	___
Back-up computer not located with main computer	___	___	___
Sufficient back-up capacity for required workload	___	___	___
Access to another computer available	___	___	___

CONTINGENCY PLANNING (Cont'd)

Item	YES	NO	N/A
Plans available for use of back-up: facility	___	___	___
computer	___	___	___
A back-up facility designed	___	___	___
Equipment and/or network configurations are stored offsite	___	___	___
Copies of data, software, and documentation are stored offsite	___	___	___
Backup hardware is available	___	___	___
Backup software is available	___	___	___
BRP is tested on yearly basis	___	___	___