

Approved: 8/4/99

**UNIVERSITY OF MASSACHUSETTS
BUSINESS CONTINUITY AND PLANNING GUIDELINES**

The following documents address business continuity planning and business disruption resumption/recovery as they relate to data at the University of Massachusetts. The first part of this document is the University of Massachusetts Business Continuity and Planning Guidelines. The second part of this document consists of several sample aids/tools that were developed to assist employees in performing risk assessment and business resumption plan development. The samples are not intended to be all-inclusive and their use is not required. Please reference the [Data and Computing Guidelines/Standards Definitions](#) for definitions of terms used throughout this document.

<u>SECTION</u>	<u>PAGE #'S</u>
Business Continuity Guidelines	1 - 8
Appendix 1 - Sample Risk Assessment Checklist	9 - 37
Appendix 2 - Examples of Potential Risks That May Result in Data System Disruption	38
Appendix 3 - Sample Business Continuity Planning Steps and Issues	39 - 40
Appendix 4 - Sample Outline of a Business Resumption Plan (BRP)	41 - 42
Appendix 5 - Data System Criticality Levels	43 - 44
Appendix 6 - Sample BRP Recovery Team Responsibility Assignments	45 - 49
Appendix 7 - Sample BRP Recovery Steps/Tasks/Procedure Document	50
Appendix 8 - Sample Key Personnel Emergency Call List	51
Appendix 9 - Sample Asset Inventory	52 - 53
Appendix 10 - Sample Alternate Site/Processing Contract Issues	54 - 56
Appendix 11 - Sample BRP Testing Issues	57 - 58

University of Massachusetts
Business Continuity Planning Guidelines

Data and the electronic and manual systems through which they are processed have evolved into critical facets of the University structure. Data in these systems is relied on heavily: to perform routine University business; to supply students and external institutions with student related information; to comply with legal and contractual requirements; and as a basis for management decision making. Additionally, although increased automation of the University's administrative operations and research projects provides substantial efficiencies, it also exposes the operations/research to severe disruption if the electronic data systems are not available on a continuous basis.

Additionally data processing and business applications are no longer restricted to mainframe computer environments. The use of distributed platforms (including mid-range computers, client/server technology, and local and wide area networks) for mission-critical functions not only expands the scope of business continuity planning but makes it more important. This increased importance arises from the fact that non-operational areas are finding themselves responsible for systems which are critical or which highly impact the functioning and reputation of the University.

I. PURPOSE

These Guidelines are issued pursuant to the Board of Trustees' [Business Continuity and Planning Policy](#) (Doc. T99-060 adopted August 4, 1999) and:

- a. Define what critical and impacting data systems are and how such systems will be identified and ranked,
- b. Outline responsibilities related to business continuity planning and implementation,
- c. Provide guidelines for the development, testing, maintenance and implementation of data system specific business resumption plans (BRPs), and
- d. Provide methods for monitoring and enforcing these Guidelines.

II. SCOPE

Campus procedures relating to business continuity shall apply to all data systems (manual and electronic) designated as critical or impacting data systems of the University of Massachusetts.

III. RESPONSIBILITIES

The President, or his/her designee, shall ensure that each campus develops, implements and tests BRPs for its critical and impacting computer systems.

The President, together with the Chancellors or their designees, shall appoint a senior level individual (herein referred to as risk managers) at each campus and within Central Administrative Services, who is responsible for risk management. Further, these risk managers shall ensure that appropriate application administrators perform evaluations of the exposure of critical and impacting data systems to computer and other disruptions. Where the consequences of such disruptions would be significant, the application administrator(s) shall ensure that BRPs are developed, documented and tested.

The following areas will determine which data systems are considered critical or impacting:

<u>Data System Environment</u>	<u>Area</u>
Intracampus data systems	Chancellors or their designees
Intercampus/Multi-campus data systems	Chancellors or their designees from the effected campuses
University-wide data systems	President's Council or their designees

These areas will also rank these critical and impacting systems to indicate which systems are most crucial to the Campuses'/University's functioning. This ranking will be used to determine which data systems need to be recovered and in what order in the event of a disruption. Several factors should be considered, including but not limited to, the calendar cycle, processing hardware, system software, applications programs and essential human resources when determining whether systems are critical or impacting.

The risk manager shall:

- a. Ensure that training is available for application administrators in the areas of risk assessment, analysis and management, and BRP development.
- b. Ensure that annual risk analyses and BRP tests are performed for all critical or impacting data systems.
- c. Review the results of risk analyses and BRP tests to ensure that the proper and appropriate controls have been implemented.
- d. Work, as needed, with University audit, application administrators and data center personnel, as needed, to institute appropriate controls for critical and impacting data systems.

e. Maintain records of these risk analyses, instituted controls, and BRP test results for one year and make these records available to University Audit.

The application administrator shall:

a. Perform, at least annually, risk analyses to determine the level of exposure to data systems under their responsibility to corruption, damage or other disruption. Special attention should be given to those systems designated as critical or impacting.

b. Institute controls (e.g., proper backup plans, formalized restart procedures, installation of an uninterruptible power supply, etc.) which will minimize the probability that a disruption will occur and ensure quick business resumption when a disruption does occur.

c. Report the results of the risk analyses and instituted controls (noted in items a and b above), to the appropriate Campus/Common Administrative Services risk manager.

d. Maintain detailed records of risk analyses they perform and documentation of instituted controls for one year. These records/documentation should be made available to University Audit.

e. Develop, document, update and test business resumption plans (BRPs) for those systems designated as critical or impacting. This includes obtaining permission from software vendors to use licensed software products for testing and recovery operations.

f. Perform, at least annually, BRP tests and keep the BRP(s) current. Results of BRP testing should be reported to the Campus/Common Administrative Services risk manager. Ongoing changes in systems, software, applications, communications and operations will create many changes and updates to the plan.

IV. **GENERAL GUIDELINES**

Application administrators shall perform risk analyses (See Appendix 1 for a sample Risk Assessment Checklist) and review controls over the data system(s) under their control as part of any implementation of a new critical or impacting data system, and annually for all existing critical or impacting data system. This will ensure that appropriate and up-to-date controls are in place. University Audit or external audit firms are good resources for application administrators interested in obtaining additional or more technology specific audit/assessment checklists.

Based on risk analyses performed by application administrators, the administrator shall institute controls (e.g., proper backup plans, formalized restart procedures, installation of

an uninterruptible power supply, etc.) which will minimize the probability that a disruption will occur and ensure quick business resumption when a disruption does occur. The costs of implementing these controls should be weighted against the loss which would result if the disruption occurred (this is referred to as risk management) and the probability of a disruption.

V. **BUSINESS RESUMPTION PLAN (BRP) STANDARDS**

Business Continuity Planning is the process of identifying critical data systems and business functions, analyzing the risks of disruption to the data systems and business functions, determining the probability of a disruption occurring and then developing business resumption plans (BRP's) to enable those systems and functions to be resumed in the event of a disruption.

The goal of an effective business resumption plan and recovery process is to facilitate and expedite the resumption of business after a disruption of critical or impacting data systems and operations has occurred. Disruptions may be minor or may include instances where normal University functions and services cannot be performed and may not be performed for an extended period of time (see Appendix 2 for an Examples Of Potential Risks That May Result in Data System Disruptions). Business continuity planning (see Appendix 3 for Sample Business Continuity Planning Steps and Issues) minimizes the impact of disruption while maximizing resources available to resume normal operations. The principle objectives are to:

- a. Minimize disruptions of service to the University community and any external entity relying on University data systems and the information stored in them.
- b. Provide a road map of predetermined actions that will reduce decision-making during recovery operations. Good planning will reduce the number and magnitude of decisions that must be made during the period when exposure to error is at a peak.
- c. Ensure the timely resumption of critical and impacting systems and enable the resumption of normal business/service at the earliest possible time in the most cost-effective manner.
- d. Limit the impact of the disruption on the University mission and reputation, and limit any financial losses.

Once critical and impacting University applications have been identified and ranked, BRPs for these applications shall be developed. Copies of the BRPs shall be accessible from any off-sight location. Key personnel should know the exact location of the BRPs and be familiar with how to access this information. BRPs should be maintained electronically in relational database software, when possible.

BRPs for critical and impacting systems shall contain the following (See Appendix 4 for Sample Outline of a Business Resumption Plan):

- a. Clarification of what constitutes a disruption (what level/extent of disruption) for which the specific BRP needs to be implemented.
- b. Maximum acceptable downtimes that can be incurred (i.e., how long the unit/University can function before the data system must be available). Business functions and/or services which must be restored within 2 - 4 hours require significantly different recovery actions than those which can be delayed a number of hours, days or weeks (See Appendix 5 for Data System Criticality Levels).
- c. Who determines whether the incident is classified as a business disruption, what level of disruption has occurred and to what degree the plan needs to be implemented. When a disruption occurs, the level and extent of the disruption must be immediately determined and appropriate steps taken to safeguard lives and prevent further destruction or escalation of the problem.
- d. Which staff are involved in the business resumption effort (part of the resumption team - See Appendix 6 for Sample BRP Recovery Teams and Responsibility Assignments) and at what disruption level are they involved.
- e. What are the resumption team member responsibilities (See Appendix 6 for Sample BRP Recovery Teams and Responsibility Assignments) and how will the non-availability of certain key team members be addressed. Step-by-step, definitive procedures (See Appendix 7 for Sample BRP Recovery Steps Document) for each team member shall be developed. Plans for cross training on duties should also be formulated. Pre-planned processes and trained personnel will significantly reduce the cost and time necessary to achieve full recovery and resume normal business operations.
- f. Contact names, phone lists and initiation procedures that are updated quarterly or as needed. An emergency call list for key personnel (See Appendix 8 for Sample Key Personnel Emergency Call List) shall be developed. Additionally, procedures shall be developed with other administrative functions that may be affected, such as, Human Resources, Public Safety, Public Relations and data center personnel, etc.
- g. The location of the BRP coordination site, if needed.

h. What information about the disruption shall be made public and how this information will be disseminated.

i. An inventory (See Appendix 9 for Sample Asset 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, cabling, communications, total square footage, personnel and office space needs, etc.
- . Hardware and peripherals (e.g., PCs, printers, etc.)
- . Data files (note format - MAC, DOS, Filemaker Pro, 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 - funding needed to implement the plan and the source of funding. This should also include a provision for incidental costs so that small needs do not hamper the resumption effort.
- . Transportation logistics (trucking, packing services, etc.) for personnel, supplies, input/output delivery between critical system users and the recovery site, and between the recovery site and the back-up facility.

These lists shall contain quality and quantity requirements (e.g., version 3.0 or higher of software x, 15 PC's with windows 95 software, 100 copies of form X or 8 1/2" x 11" paper, etc.).

j. Data back-up schedules and off-site storage procedures. Keep current schedules and back-ups for all critical/impacting systems at off-site storage locations. Special back-up and restore procedures should enable loading only the most critical items.

k. Contracted or agreed upon alternate facilities/operating sites, if appropriate (see Appendix 10 for Sample Alternate Site/ Processing Contract Issues). These may be hot, or cold sites, service bureaus or shared sites (i.e., reciprocal agreements) depending on the degree of disruption and need. Copies of any reciprocal agreements, or service bureau or hot/ cold site contracts should be kept at an off-site location.

l. Information regarding the type and level of hardware and software vendor support required, available and contracted. This should include any necessary purchases or leases needed in the event of a disruption (e.g., office, communications and/or computer equipment, etc.), estimated costs of specific support, payment arrangements, and vendor response times. Information should be obtained through meetings, requests for information, acquisition terms and conditions, joint vendor meetings, etc. as part of the business continuity planning efforts.

m. Hardware and software (system and application) restore procedures.

n. The off-site location of data (whether paper, tapes, cassettes, disks, etc.), duplicate copies of documentation (BRP, system/application manuals, contracts, procedure manuals, etc.), supplies, and forms.

o. A schedule for BRP testing (See Appendix 11 for Sample BRP Testing Issues). BRPs shall be tested at least annually using various testing approaches (e.g., structured walk-through; checklists; simulations; parallel testing; and full-interruption testing). Tests should be carefully planned to minimize disruption to normal operations and should address partial and full disruptions of various types. Each test scenario should be carefully developed so that all facets of the BRP are fully tested. Planning and conducting test exercises should be the joint responsibility of the data center, application administrators and the user(s). Some areas to test include, but are not limited to:

- . Data backup
- . Documentation backup
- . Facilities backup
- . Resumption team training
- . Critical applications (first singly, then in groups)
- . Response during different processing periods and shifts
- . Alternate processing procedures

p. Procedures for documenting formal plan tests and test results, following up these tests, and implementing corrective actions/recommendations arising from these tests. After each test exercise, results should be thoroughly reviewed for flaws, omissions, and overlaps in the business resumption procedures. Test results should be made available to the risk manager and University Audit.

VI. **COMPLIANCE AND ENFORCEMENT**

University and external audit shall review campus procedures and compliance with these Business Continuity Planning Guidelines.

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.

Item	YES	NO	N/A
PHYSICAL SECURITY - GENERAL			
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	___	___	___

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			
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)	___	___	___

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	___	___	___

Item	YES	NO	N/A
ENVIRONMENTAL CONTROLS			
FLOOD/WATER			
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	___	___	___

Item	YES	NO	N/A
Paper, supplies and trash stored outside equipment area, desktop location, computer room	___	___	___
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	___	___	___

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	___	___	___

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	___	___	___
CLIMATE CONTROL			
Separate HVAC system for the computer room	___	___	___
System protected from accidental and/or intentional shut-down	___	___	___
Controlled humidity	___	___	___

Item	YES	NO	N/A
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 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	___	___	___

Item	YES	NO	N/A
Policies, Guidelines and Procedures available to and understood by employees:			
Business Continuity and Planning Guidelines	___	___	___
Cross-training	___	___	___
Data and Computing Standards	___	___	___
Data/System Administrator Responsibilities and System Requirements (if applicable)	___	___	___
Drug and alcohol abuse	___	___	___
Harassment	___	___	___
Microcomputer/PC Guidelines	___	___	___
Procedures for Responding to Notifications of Copyright Violations or Requests for the Content of Electronic Communication, Any Information About Users of The University of Massachusetts Systems/Networks, Or Traffic on the University of Massachusetts Networks	___	___	___
Records Management, Retention and Disposition Guidelines	___	___	___
Responsible/Acceptable Use of Computing and Data Resources	___	___	___
Termination Procedures	___	___	___
Vacations	___	___	___
Other	___	___	___
Appropriate actions are taken when individual are found to be violating University Policies/Standards/Guidelines and Campus Procedures	___	___	___
Authorized users have signed a computing awareness and data security compliance statement	___	___	___
COMPUTER USAGE			
Employees and students at the University understand their responsibilities for implementing security in their daily interactions with people, data, systems, and facilities	___	___	___
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	___	___	___

Item	YES	NO	N/A
University employees, students and all users accessing University data or computing systems/resources accessing University data and/or computer systems/resources only access those systems for which they have been authorized	___	___	___
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 and Computing Standards) or critical data is stored or maintained	___	___	___
Passwords used to access computer systems containing Private, Restricted or Confidential data (as defined by University Data and Computing Standards) are at least 6 characters	___	___	___
Pin numbers used to access Private, Restricted or Confidential data (as defined by University Data and Computing Standards) are at least 6 characters	___	___	___
Restricted access to password file	___	___	___

Item	YES	NO	N/A	
Authorized user change their passwords periodically				—
mainframe	—	—	—	
network	—	—	—	
microcomputer	—	—	—	
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:				
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	—	—	—	

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	___	___	___

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	—	—	—
Documentation (operating system, application, communication, etc.) is secured	—	—	—

Item	YES	NO	N/A	
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	___	___	___	
Logs of access to Confidential, Restricted, or Private data files (as defined by University Data Security and Classification Guidelines) are:				
maintained	___	___	___	
monitored	___	___	___	

Item	YES	NO	N/A
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	___	___	___
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 and Computing Standards) are encrypted	___	___	___

Item	YES	NO	N/A
Confidential, Restricted and Private data (as defined by University Data and Computing Standards) 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)	___	___	___
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	___	___	___

Item	YES	NO	N/A
Authorized users:			
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 and Computing Standards 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	___	___	___
secured against unauthorized -			
creation	___	___	___
update	___	___	___
deletion	___	___	___
processing	___	___	___
distribution	___	___	___

Item	YES	NO	N/A
Data, regardless of medium and/or form, is 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 and Computing Standards) is appropriately backed up to allow for recovery	___	___	___
Copies of critical data are stored outside the computer room/office	___	___	___
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	___	___	___

Item	YES	NO	N/A
Confidential, Restricted and Private data (as defined by University Data and Computing Standards) are properly managed when downloaded	___	___	___
Confidential, Restricted and Private data (as defined by University Data and Computing Standards) 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 and Computing Standards) 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	___	___	___
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 and Computing Standards) transmitted over public lines is encrypted	___	___	___

Item	YES	NO	N/A
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	___	___	___
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	___	___	___

Item	YES	NO	N/A
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	___	___	___
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	___	___	___
WIRELESS NETWORKS			
Wireless network employs a combination of layered authentication methods to protect Private, Restricted or Confidential data	___	___	___
All WAPs are registered with the campus information security officer at the time of deployment in the UMass environment	___	___	___

Item	YES	NO	N/A
All Supervisory Control and Data Acquisition (i.e., SCADA) devices on the network are registered with the campus information security officer at the time of deployment in the University of Massachusetts environment	___	___	___
Only approved and registered WAPs are deployed	___	___	___
Only authorized staff install wireless networking ‘access points’	___	___	___
Final device names are assigned during the registration process	___	___	___
Wireless applications are deployed in a manner to prevent interference between the University wireless network infrastructure and other uses of the wireless radio spectrum	___	___	___
In cases where WAPs have variable radio power levels, the minimal power level that provides the intended coverage has been chosen so as to limit interference with other deices operating in that frequency range	___	___	___
All installed radio-based products comply with both the ANSI C95.1-1991 IEEE Standards for Safety Levels with Respect to Human Exposure and the FCC Office of Engineering and Technology Bulletin 65 Evaluating Compliance with the FCC Guidelines for Human Exposure	___	___	___
All installed radio-based products are evaluated by the vendor for RF Safety Compliance per the requirements of FCC Part 2.1091 and 2.1093 of the FCC Rules	___	___	___
Wireless access points are designed to reduce emissions that can interfere with medical devices	___	___	___
Access points in public areas meet the FCC requirements for devices operating in medical environment specifically EN 55011 emission standards	___	___	___
Any new construction plans are evaluated for consideration of new or updated wireless networking	___	___	___
Wireless access points are installed in physically secure areas accessible only by authorized personnel	___	___	___

Item	YES	NO	N/A
Devices are not be placed in easily accessible public locations. If the device is installed in an open area, it is located at a height of 12' or greater	___	___	___
Only WAPs that support power level adjustment are used	___	___	___
All WAPs are secured using an administrative password	___	___	___
All vendor default usernames have been removed from deployed wireless devices	___	___	___
All default passwords, SNMP community strings, and other remote-management authentication mechanisms are changed from their defaults prior to deployment onto the production network	___	___	___
Default SSIDs set by the manufacturer are changed prior to device deployment	___	___	___
Security features available with WAPs are enabled	___	___	___
Administration of wireless devices from the wireless network is prohibited	___	___	___
Wireless networks traverse a routed network interface before logically contacting a traditional wired network	___	___	___
Access control and security mechanisms are deployed	___	___	___
System logs are monitored weekly	___	___	___
Critical host logs are scanned daily	___	___	___
Wireless devices are properly secured prior to deployment	___	___	___
A security analysis using current wireless security methods has been performed	___	___	___
Periodic security verifications are performed	___	___	___
Security patches, upgrades, and antivirus software updates are pushed to clients from servers	___	___	___
All access via the wireless infrastructure requires user authentication	___	___	___

Item	YES	NO	N/A
Once authenticated to an access point, authorized users are either routed outside the UMass firewall(s), or authenticate to a University network	___	___	___
Wireless clients used for connecting to campus business systems or other systems that contain Private, Restricted or Confidential data, or are critical to the mission of the University use encryption protocols or other appropriate and equally secure methods	___	___	___
Wireless clients used for connecting to campus business systems or other systems that contain Private, Restricted or Confidential data, or are critical to the mission of the University use secure transport protocols such as SSL (Secure Sockets Layer) or IPsec	___	___	___
Wireless access points are programmed to disallow access to high risk services (e.g., PeopleSoft Human Resources and Financials, Student Administration, patient records, etc.) unless the user is using encrypted protocols	___	___	___
Wireless transmissions are not used in prohibited areas, or where interference with other electronic equipment could be a problem	___	___	___
Applications access via the wireless infrastructure includes appropriate password and data protection controls	___	___	___
Research groups and labs are aware that conditions of some federal grants include data confidentiality and protection	___	___	___
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	___	___	___

Item	YES	NO	N/A
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 dial tone thereby allowing calls anywhere in the public network, including international calls	___	___	___
Automated call directors/distributors do not allow the caller to obtain a dial tone 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	___	___	___
Offsite records to restore data communications equipment are maintained:			
Modems	___	___	___
Multiplexers	___	___	___
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	___	___	___

Item	YES	NO	N/A
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	___	___	___
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	___	___	___

Item	YES	NO	N/A
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	___	___	___
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	___	___	___

Item	YES	NO	N/A
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	___	___	___
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	___	___	___

Item	YES	NO	N/A
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		___	___
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	___	___	___

APPENDIX 2

EXAMPLES OF POTENTIAL RISKS THAT MAY RESULT IN DATA SYSTEM DISRUPTIONS

HVAC Failure
Blizzard
Bomb
Civil Disturbance/Student Protests/Building Takeovers
Communications (voice/data) Interruption
Data Unavailable - file erased, incorrect data available
Earthquake
Electrical Failure - storm, construction accident
Employee Error
Epidemic- flu
Equipment Malfunction - drive crash, check signer broken
Facility Structural Failure - burst pipe, wall collapse
Fire
Flood
Financial Support Systems Unavailable (e.g., banks, and other institutions)
Hardware Upgrade, Obsolescence or Incompatibility
Hurricane
Postal/UPS/Fed Ex Strike
Union Issues/Strikes
Sabotage - disgruntled employee damages files/equipment
Software Error - virus on install disk
State of Emergency
Software Upgrade, Obsolescence or Incompatibility
Staff Shortage or Unavailability
State or Federal Funds Unavailable
Terrorism
Theft - equipment stolen public labs, disks stolen
Tornado
Untrained or Improperly Trained Staff (in job function, hardware, software, etc.)
Utility Outage

APPENDIX 3

SAMPLE BUSINESS CONTINUITY PLANNING STEPS AND ISSUES

This is a **sample** list and is not intended to be all-inclusive.

1. Establish a Business Resumption Planning Committee
 - Project Leader
 - Project Plan/Control
 - Committee Selection
 - Assign Responsibilities
 - Regular Committee Meetings
 - Periodic Management Briefings

2. Perform a Business Resumption Capability Assessment - if a disruption were to occur today, how quickly and fully could you resume business/services?
 - Security Check List
 - Recovery Analysis
 - Task Assignments

3. Perform a Risk Analysis
 - Risk Assessment
 - Risk Management
 - Evaluate Threats
 - Establish Controls
 - Review Security Measures

4. Analyze and Define Requirements for Recovery
 - Hardware
 - Software - system and application software
 - Communications
 - Back-up Data
 - Physical Facility
 - Vendor Support
 - Inter-Campus or Commonwealth Agency (MITC) Support
 - Personnel
 - Security
 - Office Equipment
 - Forms/Paper Supplies
 - Logistics
 - Storage
 - Funding/Purchase Orders

5. Design and Document the BRP for Recovery Operations

Organization

Damage Assessment Team

User Liaison Team (if needed)

Communications Team

Operations Team

Security/Back-up Team

System Software Team

Procurement Team

Facilities Team

Identify Processes Required

Develop Procedures (by team)

Risk Manager or University Audit Review and Approval

6. Conduct BRP Implementation Training

Select Training Topics - emergency procedures, use of fire extinguishers, backup retrieval, etc.

Select Instructors

Develop Training Material

Risk Management

Procedures

Select Personnel for Training

Train Personnel

7. Test the BRP

Frequency - at least annually

Develop a Test Plan/Script

Test Scenario

Evaluation and Reporting

Follow-up

8. Maintain and Update the BRP

Follow-up BRP Test

Report Test Results to Risk Manager

Institute Controls/Changes - environmental, procedural, personnel, training, etc.

APPENDIX 4

SAMPLE OUTLINE OF A BUSINESS RESUMPTION PLAN (BRP)

Publication Date

Distribution List

Sensitive Information Disclosure Notice

Executive Overview

This section contains the executive management perspective, policies, plan concept and overview of the business resumption plan.

Introduction: Purpose, Goals, Objectives, Benefits

Scope (what data systems does the BRP address)

What Constitutes a Disruption

Responsibilities

Assumptions (Risk Analysis, Criticality Level, Acceptable Downtimes)

BRP Activation Authority- who determines that the BRP should be implemented when an interruption occurs

Recovery Operations (Process, Procedures, Teams)

Training (Teams, Users)

Testing of BRP (Schedule, Scenario, Monitoring, Follow-up)

Plan Revisions and Updates (Environmental Changes, Test Results, Review Schedule)

Contact Section

BRP Activation Authority contact and telephone number:

Key technical contact(s) and telephone number(s):

Key user contact(s) and telephone number (s):

Criticality Section

Criticality Level/Period:

Maximum Allowable Processing Delay:

Processing Time Required:

Legal Requirements:

Detailed Business Resumption Steps

This section details the procedures to be followed during resumption activities:

Responsibilities - who does what, when, where, how
(BRP Team Leader, BRP Team Coordinator, BRP Coordination Site Coordinator, Recovery Team Leaders, Recovery Teams, BRP Activation Authority, Situation Identification, Damage Assessment, Notification Procedures, BRP Activation Process, User Departments/Section, MIS staff, etc.)

Operating Procedures - specific procedures for each Recovery Team members to follow including the Post -Implementation Review Team)

Detailed Lists, Inventories, and Business Requirements:

This section identifies all resources critical to the business resumption effort. It should be organized in such a way as to address the "who, what, when, where, and how" in the process of identification, location, commitment, funding and deployment of those resources.

Resources include: Configuration Drawings, Hardware, Software, Communications, Back-up Data (include medium of data), Physical Facilities, Vendor Support, InterCampus/Commonwealth Agency Support, Personnel, Applications, Security, Office Equipment, Forms/Paper, Logistics, Storage, Funding, Purchase Orders, etc.

APPENDIX 5

DATA SYSTEM CRITICALITY LEVELS

These are SAMPLE data system criticality levels. The University has not specifically defined criticality levels. Several factors should be considered when determining data system criticality levels, including but not limited to, the calendar cycle, processing hardware, system software, applications programs and essential human resources. The same data system may have different criticality levels assigned to it depending on the time of year, day of week, hardware used, etc.

System Identification, Brief Description and Title:

Classification: Critical: Level 1 ___ Level 2 ___ Level 3 ___

 Impacting: Level 1 ___ Level 2 ___

 Other (note specific needs if data system criticality level does not fall into one of the above levels)_____

Critical Level 1 = restore immediately. This is highly critical to the survival of the University. Immediate recovery is required to prevent substantial loss to or degradation of University operations.

Critical Level 2 = restore within 12 hours. This is relatively critical to the survival of the University. Further delay could raise this to Criticality Level 1.

Critical Level 3 = restore within 24 hours. This is important to the survival of the University. To delay further could raise the Criticality Level due to increase in volume or passage of time.

Impacting Level 1 = restore within 7 days. This is important to the effectiveness or efficiency of the management of the University.

Impacting Level 2 = restore within 14 days. This is important to the effectiveness or efficiency of the management of the University but is not important to the survival of the University.

APPENDIX 6

SAMPLE BRP RECOVERY TEAM AND RESPONSIBILITY ASSIGNMENTS

This is a **sample** list and does not include all possible recovery teams.

Teams may be merged or eliminated depending on the size, type, and platform on which the data system(s) is running.

Additionally, teams may not always be needed for each business resumption effort. Teams needed will depend on the type and degree of disruption.

BRP Team Leader

Responsible for directing, coordinating, and reporting to management until full recovery has been accomplished (generally the applications administrator).

BRP Coordination Site Coordinator

Responsible for ensuring that a facility adequately equipped with phone lines (automatic switching of phones from the primary facility should be pre-arranged so vital communications can continue during the recovery operation) status boards, conference equipment, etc. to function as an information and operations center for an extended period of time during business resumption has been established.

BRP Team Coordinator

Assist the BRP Team Leader by coordinating and reporting on task assignments and progress of the teams, investigating problems, reporting on findings, and other assistance as appropriate for operation of the BRP Coordination Site.

Damage Assessment Team

A technical group responsible for assessing damage to the facility and its components:

- Identify extent of damage to the facility.
- Determine condition of equipment.
- Identify software problems.
- Define data problems.
- Identify data communications problems.
- Describe salvageability of supplies.

- Assess operational capability.
- Define restoration requirements.
- Schedule salvage and restoration.
- Monitor salvage and restoration operation.
- Provide a detailed accounting of damages for insurance claims, if applicable.
- Advise BRP Coordination Site Coordinator of status and progress.

User Liaison Team

Major user area managers, production control, and applications lead analysts responsible for coordination and liaison with the information resources staff for applications recovery and restoration of data files and data bases:

- Advise users of critical systems of the disruption and recovery production schedule.
- Monitor the actual production schedule continually.
- Provide programming and support services for alternate processing of critical systems.
- Help system users prepare for resumption of normal operations as recovery progresses.
- Advise BRP Coordination Site Coordinator of status and progress.

Under the general leadership of the User Liaison Team, technical applications specialists and data base administration sub-teams perform necessary application restoration activities. Setting priorities for applications recovery is a primary influence on procedures for this team and its subgroups.

Communications Team

- Communications specialists responsible for restoring voice, data, and video communications links between users and the computer, regardless of location.
- Assist in damage assessment.
- Coordinate restoration of service with vendors.
- Test data communications operation.
- Establish data communications for critical applications.
- Identify equipment and software requirements.
- Provide necessary telephone service.
- Monitor restoration of normal communication operation.
- Advise BRP Coordination Site Coordinator of status and progress.

Communications vendor (carrier) input in designing and implementing the recovery plan is very important. Influential factors in developing recovery procedures for this team include: the type and size of network, the time requirement for restoration, percentage of the network to be recovered, and budget considerations.

Operations Team

Operators responsible for running emergency production for critical systems, coordinating with the Back-up Team to insure that applications system data and operating instructions are correct and with the Liaison Team to advise of the production status and any unusual problems requiring assistance:

- Initiate emergency production schedule for critical applications systems.
- Operate host computer center.
- Coordinate input/output from recovery facility.
- Receive backup versions of appropriate software.
- Establish production control function.
- Establish data entry/collection functions.
- Establish micrographics functions.
- Secure back-up forms as needed.
- Establish distribution function.
- Establish forms handling function.
- Assist the Facilities Team.
- Advise BRP Coordination Site Coordinator of status and progress.

Data input/control teams could be separate groups or subgroups of this team.

Security/Back-up Team

Responsible for retrieving back-up copies of operating systems, applications systems, applications data and ensuring security of the data, and back-up and original facilities:

- Retrieve back-up software, applications software, applications data and documentation required for emergency processing of critical applications systems.
- Advise the Operations Team of the status of back-up data and software.
- Advise BRP Coordination Site Coordinator of status and progress.

System Software Team

Systems software programmers responsible for providing the system software support necessary for production of critical applications systems during recovery:

- Assist the Damage Assessment Team in determining the extent of damage to system software.

- Advise the Procurement Team of specific system software purchase requirements.

- Oversee initialization of operating system, JCL, and other control systems.

- Restore applications and communications system software at the back-up or primary site as appropriate.

- Assist the Operations Team in restoring operation at the back-up or primary site.

- Advise BRP Coordination Site Coordinator of status and progress.

Procurement Team

Persons knowledgeable of the information resources and supplies inventory and the budgetary, funding, and acquisition processes responsible for expediting acquisition of necessary resources:

- Assist Damage Assessment Team in determining equipment, software, facility, and other components beyond repair and in determining additional equipment or supplies required at the back-up site for expediting the recovery process.

- Coordinate identification of purchases.

- Contact vendors to procure necessary equipment, software and supplies.

- Monitor acquisition and delivery of purchases.

- Advise BRP Coordination Site Coordinator of status and progress.

Facilities Team

Responsible for arranging for the alternate and backup facilities and all components:

- Assist the Damage Assessment Team in identifying specific damage to the facility.

- Reference floor plan documentation for required dimensions and environmental.

- Identify repair or replacement requirements.

- Arrange for necessary repairs or replacement.

- Oversee and monitor repair, reconstruction, or replacement.

- Prepare back-up site for occupation and operation.

- Advise BRP Coordination Site Coordinator of status and progress.

Standards and Procedures Team

Responsible for reassembling all documentation for guidelines, standards, procedures, applications, programs, systems, forms, etc. as required at the alternate site.

PC Support Team

This Team could also be part of the Operating, Security/Backup-up and/or System Software Teams.

Responsible for re-establishing microcomputer operations at back-up or remote sites and for assisting with reinstating PC applications.

Administrative Services Team

Responsible for clerical and administrative services support for BRP Team Leader and all other Teams. May also assist groups outside the information resources area, as needed.

University Audit Team

Responsible for observation and oversight participation in the recovery effort:

- Review the existence of sufficient control to assure reliability and consistency of financial records.
- Observe implementation of necessary supervision and controls during recovery.
- Review logs of recovery activities.
- Advise BRP Coordination Site Coordinator of status and progress.

Public Information Team

Responsible for disseminating information concerning the emergency or event requiring the recovery effort.

- Have a single spokesperson accessible to employees and external forces.
- Provide accurate, essential, and timely information to combat spread of rumors and adverse publicity.

Logistics Team

Arrange for transportation of staff, equipment, supplies and other necessary items between sites.

APPENDIX 7

SAMPLE BRP RECOVERY STEPS/TASKS/PROCEDURE DOCUMENT

Title:

A short descriptive title for the step/task/procedure

Purpose:

Clearly state the purpose for this step/task/procedure.

Scope:

Describe what the step/task/procedure covers and a summary of its content.

Authority:

Define any specific requirement for this step/task/procedure.

Responsibility:

Identify who, by position title, is charged with a responsibility and describe that responsibility succinctly but in sufficient detail to be readily understood by the reader. Where the procedure covers the responsibilities for a team or other group, specify members by position title and/or name and telephone number.

Procedure and Steps:

Describe the steps/task/procedure and/or process to be accomplished and where they should be performed (if applicable). Use flow charts, diagrams or tables to clarify the procedure in sufficient detail to enable ready comprehension by the reader(s).

APPENDIX 8

SAMPLE KEY PERSONNEL EMERGENCY CALL LIST

It is recommended that this list be developed based upon the Business Resumption organization with the BRP Team Leader responsible for calling key management personnel and the BRP Team Coordinator responsible for calling Team Leaders. Team Leaders will then call each Team Member until all personnel have been notified.

The list should contain work, home and beeper telephone numbers with space to record the time of contact. The process must include telephone numbers for fire, police, ambulance services and procedures for notifying these agencies.

In addition, the User Liaison Team members will notify the Users. This process should be reviewed to determine that all appropriate personnel have indeed been notified.

Team Member Name	Team	home phone	work phone	work hrs.	contact date/time
------------------	------	---------------	---------------	-----------	----------------------

(U) = Unlisted/unpublished phone number. Care should be taken when distributing such telephone numbers.

APPENDIX 9

SAMPLE ASSET INVENTORY

DATA SYSTEMS	DESCRIPTION	QUANTITY	COST	LOCATION	SOURCE*
	Computer Hardware				
	Logical/Physical Configuration Diagram				
	Systems Software				
	Application Software				
	Facilities				
	Communications Equipment				
	Data Files				
	Documentation				
	Supplies				
	Office Equipment				

DATA SYSTEMS	DESCRIPTION	QUANTITY	COST	LOCATION	SOURCE*
--------------	-------------	----------	------	----------	---------

Forms/Paper

Vendor Support

Personnel

* Refer to physical location or contract number if equipment, software, etc. source during a business disruption has been previously contracted for.

APPENDIX 10

SAMPLE ALTERNATE SITE/ PROCESSING CONTRACT ISSUES

Effective contracts between vendors and users are probably the best means to prevent disputes. Given the complexities and dynamics of computer and information technology law, the potential for disagreements and litigation between users and vendors will increase. Both vendors and users are challenged to implement controls and procedures that minimize the potential for information solutions to fail.

Include contingency and recovery provisions in equipment contracts.

Alternate Site Services

It is necessary to have a consistent set of issues to truly compare different vendors.

Applications Impact Analysis

Know what you need before you buy. If 100% capacity is not an absolute requirement, fees may be lowered substantially.

Location or Site Information

- Multiple hot or cold site locations

- Multiple locations networked together

- Contract terms: length of contract time; minimum/maximum fee; test hours allowed under contract; cost of additional test time not included in contract; lead time for notification of scheduled tests; maximum number of subscribers per location

Policy regarding site availability for testing while in use for recovery of a declared disaster by another subscriber

The number of other clients; from what geographical area

Any former inability to accommodate a subscriber in a declared emergency; how resolved

Base list price for equipment size and different contract terms

Availability of mobile recovery services and normal length of set-up time

Configuration Information

By manufacturer, model/series number, and size/quantity:

Mainframe processors (MIPS - million instructions per second)

Desktop requirements (hardware and software)

Systems software

Storage devices - DASD units (gigabyte), drives, disks, cassettes, CD-ROM

Front-end processors, controllers, etc.

Printers

FAX machines

Any critical unusual equipment

Telecommunications systems (T1, T3, satellite, microwave, or dial-up; routers firewalls, etc.); network software (NetWare, BANYAN VINES, MICROSOFT NT, etc.) network availability (24 hours a day, 7 days a week)

Voice communications options: (ACD/UCD, number of headsets available, number of incoming and outgoing lines)

Disaster Declaration Information

Declaration fee

Criteria for use, e.g., first-come, first-served

Any requirement for resource sharing by subscribers

Time limits for occupation per declaration

Number of experienced vendor technicians on hand to assist that work only on business resumption

Other Information

Availability of electronic vaulting services
System software loading prior to subscriber arrival
Available square footage for: data center, tape library, office space, tape/disk storage, forms/paper, supplies, cold site, etc.

Levels of physical security access

Internal fire, water, and security protection
Documented and tested BRP for each location; availability of plan and test results to potential subscribers for review
User guide available to the facility with: local vendors and locations/phone numbers; emergency numbers for police, fire, hospitals; restaurants; housing (hotels, motels, apartments)
Established agreements with outside vendors/services such as: airlines; offsite tape/disk vault; taxis; tape/cassette vendors; trucks and vans; paper supplies; physical security vendors; travel agency; couriers; car rentals; microfiche; microfilm; banks; hardware vendors, etc.
Petty cash for subscribers and any limits
Available inventory of scratch tapes/cartridges, disks, and quantity
Familiarity with recovery plans for local utilities (electric, water, gas, and voice communications)
Designated customer services representative available during business hours
Provision of administrative supplies (pens, paper, staplers, scotch tape, etc.)
Current client reference list
Additional services

NOTE: Use of temporary/contract personnel at a distant site may expose the organization to inefficiencies and errors.

APPENDIX 11

SAMPLE BRP TESTING ISSUES

Evaluation of Test Results

It is essential to quantitatively measure the BRP test results, including: elapsed time to perform various activities, accuracy of each activity, and amount of work completed. Preformatted forms can be useful to document and evaluate test results. You may devise a form that could include the following information:

- Recovery Task Estimated Time - the estimated time to perform the step/task/procedure
- Plan Cross Reference - cross-reference to the specific section of the BRP that is to be tested
- Action Number - sequential number assigned to each step/task/procedure
- Action - description of the step/task/procedure to be performed during the BRP test
- Sequential or Parallel Notation - certain steps/tasks/procedures need to be performed sequentially and others can be performed concurrently or in parallel
- Responsibility - Person(s) assigned specific responsibility for performing the BRP testing step/task/procedure
- Actual Time - Actual time required to perform the specific recovery step/task/procedure
- Successful/Unsuccessful Notation - description of result
- Comments - further description of the evaluation of the test results
- Recommendations for BRP updates and control implementations

Sample Scenarios

1. All external data communications have been lost during student add/drop for an indeterminate length of time.
2. Programs which process weekly payroll and generate payroll checks have abended (ended without processing because of an error detected by the computer system) and will not perform properly the day before checks need to be distributed to employees. Additionally, the electronic transfer of automatic deposit information to banks has failed.
3. The mainframe on which student grades are processed and printed crashes and can not be repaired for several days.
4. The PC hard drive on which a critical medical application and patient data is stored crashes and the data is unretrievable.

5. A fire occurs in the storage facility resulting in the loss of all blank vendor check stock and the destruction of the check signing equipment.

Depending on the details of the appropriate BRP, notification of management would be followed by assembly of the appropriate teams, an assessment of the damage and initiation of the business resumption process.

The scenario could proceed into recovering one or more critical data systems from the backed-up data at an alternate facility or could be terminated at the option of management.