Business Continuity Planning Toolkit

(For Deployment of BCP to Campus Departments in Phase 2)

August 2010

CONTENTS:

SAN JOSÉ STATE UNIVERSITY

Business Continuity Planning (BCP) Toolkit

BACKGROUND:
Business Continuity Planning (BCP) is necessary to ensure that the campus is able to restart essential business operations after a major disruption occurs. Mission-critical (essential) functions are those functions, stated or implied, that are required to be performed by statute or Executive Order, or other functions deemed critical to carrying out the operations of the university. Business Continuity Planning requires both a university Business Continuity Plan and departmental Business Continuity Plans to ensure loss to the university is minimized, constituents continue to be served, and administrative operations are resumed safely and effectively.

A Business Continuity Plan must be maintained at a high level of preparedness and be ready to be implemented without significant prior warning. It should be implemented fully no later than 12 hours after activation and provide guidance to sustain operations for up to 30 days. Business Continuity Plans are based on the university's essential functions. It serves as an operational guide to facilitate the: relocation of university staff to an Emergency Relocation Site (ERS) if appropriate; and backup of critical systems and vital records so that essential functions may continue or be restarted. The university Business Continuity Plan describes the processes and procedures needed to support continuation of essential functions identified in the University Business Impact Analysis Matrix.

ASSUMPTIONS:
Two scenarios will be considered:
1. The disaster is significant enough that the campus facilities are not accessible. If this is the case, an Emergency Group will relocate to an ERS (to be determined, e.g., CSU East Bay's EOC/San Francisco State's EOC).

2. If the disaster does not warrant relocation to the ERS, at a minimum, the following have been restored to campus:
   a. Police, Fire and Ambulance services
   b. Electricity, water, reasonable climate control and adequate lighting
   c. Access to and egress from campus, classrooms, and administrative facilities
   d. Safe handling and proper disposal of toxic substances, biologically hazardous materials, and radioactive materials

BUSINESS IMPACT ANALYSIS

Instructions for Business Impact Analysis:
1. Review your department organization chart.
2. List all functions performed by your organization.
3. Determine if each function is "mission-critical/essential".
   a. If yes, add it to the list of mission-critical/essential functions in the University Business Impact Analysis Matrix (if it is not already on the list provided by the BCSC member).
   b. If no, delete it from the list in the University Business Impact Analysis Matrix (if it was on the list provided by the BCSC member).
4. For each essential function, assess the following:
   a. The business impact (to the University) if the function is not performed. Insert a letter in the Business Impact column that corresponds to the Business Impact Key.
   b. Determine the maximum allowable downtime for this function and insert the number of hours in the appropriate column.
   c. Determine the time to restore the function and insert the code that corresponds to the number of hours in the appropriate column .
   d. Determine the priority in restoration and insert the code that corresponds to the priority in the appropriate column.
   e. Identify the Lead Contact person (director/manager) for each essential function. The Process Owner is the AVP/Dean that oversees this function AND is a direct report to a Vice President.

Business Impact Analysis Matrix

Mission-Critical/ Essential Functions	Business Impact*	Maximum Allowable Downtime	Time to Restore CODES: 1=0-4hrs 2=4-8hrs 3=8-12hrs 4=12hrs+	Priority in Restoration CODES: 1 2 3	Contacts	
					Lead Contact	Process Owner(s)

Business Impact Key:
A – Disruption of teaching?
B – Disruption of research?
C – Loss of faculty?
D – Loss of staff?
E – Loss of students?
F – Well-being of faculty/staff affected?
G – Well-being of students affected?
H – Payment deadlines unmet by campus?
I – Loss of revenue to campus?
J – Legal/regulatory obligations unmet by campus?
K – Legal harm to the University?
L – Loss of reputation?
M – Impact on other campus unit(s)?
N – Impact on important business partner(s) or academic collaborations?
O – Data collected prior to the event is unrecoverable?
P – Data available or collected after the event is unavailable?
Q – Additional costs incurred to recover unprocessed data or transactions?

RISK (VULNERABILITIES) ASSESSMENT

Vulnerabilities Assessment

Mission-Critical/ Essential Functions	People (Trained Back-up Personnel?)	Systems		Locations Alternative locations set up?
		Backed-up at alternative location?	Can be performed manually?	

Instructions for Vulnerabilities Assessment:
1. Assess the vulnerabilities for each essential function in terms of people, systems and locations.
   a. Do key positions have trained backup personnel? If yes, identify.
   b. Are critical systems backed up at an alternative location?
   c. Can the function be performed manually?
   d. Do you know where to go/who to contact if your location is not accessible?
2. If the answer to any question is "NO", a backup/recovery solution must be designed.

BACKUP & RECOVERY SOLUTION

1. ***Mission Critical Systems*** – complete the following table for each mission-critical system that supports an essential function.

System Name	Backup Plan	Recovery @ Current Location	Recovery @ Other Location(s)

2. ***Vital Files, Records and Databases*** – complete for vital information that relates to each essential function.

Vital File, Record, or Database	Form of Record (e.g., hardcopy, electronic)	Pre-positioned at Alternate Facility	Hand Carried to Alternate Facility	Backed up at Third Location

3. ***Forms*** – complete all forms listed below and contained on subsequent pages.
   - *Business Information and Documents Form*
   - *Function Tasks Form*
   - *Function Call Tree Form*
   - *Internal Departmental Dependencies Form*
   - *External Dependencies Form*
   - *External Contacts Form*
   - *Customer Contact Form*
   - *Response/Recovery Team Personnel Form*
   - *Business Equipment and Supplies Form*
   - *Information Technology Applications Form*
   - *Information Technology Server/Hardware Form*
   - *Information Technology Telecommunications Form*
   - *Alternate Sites Form*

FORMS

Business Information and Documents Form

Complete a form for each document, data set, hard copy file, manual, and other information you need to recover or perform your functions.

Function Name:	
Information Name:	
Information Description:	
Function Name or Support Function:	
Media Type:	

Choice: Paper File, Computer Report, Data Backup, Manual, Fiche, Form, Currency, Stamps, Other

Information Type Sensitivity:	

Choice: Public, Sensitive, or Confidential also include applicable Arizona Revised Statute

Original Source :		**Alternative Source :**	
Backed Up:		**Archived:**	

Choice: Yes or No   Choice: Yes or No

Back Up Location:			
Last Update:		**Next Update:**	

Function Tasks Form

Please indicate all the steps necessary for restoration for each critical/essential function.

Function Name:	

Task Order	Task Description	Estimated Duration	Person Responsible
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

Function Call Tree Form

Complete the form for each function.

Function Name:		
Initiator:		
Initiator Calls:	**Who Calls:**	**Who Calls:**

Internal Departmental Dependencies Form

Identify internal Department/College dependencies in which this function is dependent and briefly describe the dependency. Also, identify contact name and number for that other Division or Sub-organization.

Function Name:	

Division/Sub-organization	Dependency	Contact Name	Contact Number

External Dependencies Form

Identify outside agencies or organization in which this function is dependent and briefly describe the dependency.

Function Name:	

Agency/ Organization	Dependency	Contact Name	Contact Number

External Contacts Form

Complete a form for each vendor, business partner or other external contact that you must contact (either to notify them or to request assistance) in case of a prolonged outage of the indicated function.

Function Name:	

General

Business Name:					
Address:					
City:		State:		ZIP:	
Phone:			FAX:		

Primary Contact

First Name:		Last Name:	
Title:			
Home Address:			
City:		State:	ZIP:	
Home E-mail:		Work E-mail:	
Home Phone:		Work Phone:	
Cell Phone :		Pager :	

Service Information:

Purchase Order #:	
Product/ Service:	
Emergency Lead Time:	**Normal Lead Time:**
Disaster Recovery Agreements:	
Alternative Vendor :	
Notes :	

Customer Contact Form

Complete a form for each customer of the indicated function that you must contact in case of a prolonged outage.

Function Name:	

General

Customer Name:					
Address:					
City:		State:		ZIP:	
Phone:			FAX:		

Primary Contact

First Name:		Last Name:	
Title:			
Home Address:			
City:		State:		ZIP:	
Home E-mail:		Work E-mail:	
Home Phone:		Work Phone:	
Cell Phone :		Pager :	

Services Provided to Customer:

SLA/IGA or Agreement #:			
Product/ Service:			
Emergency Lead Time:		**Normal Lead Time:**	
Disaster Recovery Agreements:			
Notes:			

Response/Recovery Team Personnel Form

Complete a form for each person on the team.

Function Name:	
Team Name:	
Team Member Position:	

Choice: Leader, Alternative Leader, and Member

Employee ID:			
First Name:		Last Name:	
Title:			
Home Address:			
City:		State:	ZIP:
Home E-mail:		Work E-mail:	
Home Phone:		Work Phone:	
Cell Phone :		Pager :	
Restoration Site Access:		Backup Site Access:	

Choices: Yes or No   Choices: Yes or No

Off-site Storage Access:		Command Center Access:	

Choices: Yes or No   Choices: Yes or No

Business Equipment and Supplies Form

List all equipment and supplies (to include but not limited to: transportation vehicles, fax, copiers, general furniture, special business forms, paper, etc.) that is needed to perform the functions.

Function Name:	

Quantity	Manufacturer	Description	Cost	*Phase

Information Technology Applications Form

Complete the form for each computer application, other than office productivity tools residing on PCs, necessary to restore the function.

Function Name:			
Computer Application Name:			
Team Name:			
*Application Listed in ISIS:			
Server/ Hardware ID:			
System ID:			
Run Frequency:			
File Structure :			
Executable Location :			
Source Code Location :			
System Documentation:		**Name:**	
User Documentation :		**Name :**	
Operations Documentation:		**Name:**	
Restoration Documentation :		**Name :**	

Information Technology Server/Hardware Form

For each function, please complete the following information about each server or other piece of centralized hardware necessary to restore the necessary computer applications.

Function Name:			
Computer Application Name:			
Server/ Hardware ID:			
Type:		**Manufacturer:**	
Model:			
Memory Size:		**Hard Disk Size:**	
Processor:		**IP Address:**	
Network Operating System:			

RTO:	

.

Information Technology Telecommunications Form

For each function, please complete the following information about the telecommunications needs for each application that supports a business service/process. This is to include, but not limited—to number of telephone lines, call center integrated applications, data lines, and or special high speed dedicated lines with external customers.

Function Name:	
Computer Application Name:	
Server/ Hardware ID:	
Telecommunication Type:	

Describe in sufficient detail the type, quantity and if known or applicable who is at the distant end that this special high-speed dedicated line connects.

RTO:	

Alternate Sites Form

Complete this form for each alternative site that is in your business continuity plan including sites used for Command Centers, Backup Sites, Off-Storage Sites, Restoration Sites, etc.

Site Type:	

Choices: Command Center, Backup Site, Off-Site Storage, Restoration Site, etc.

Description:					
Location Type:		Square Footage:		Contact Number:	

Choices: Primary or Secondary

Address:					
City:		State:		ZIP:	
Telephone:			Fax:		
Directions:					

THREAT ASSESSMENT

A threat assessment involves determining potential hazards/threats that could affect the university, assessing their likelihood of occurrence and analyzing vulnerability. From a university perspective, time and resources are spent planning for disasters that are judged to have a high likelihood of occurrence and a high level of severity. Operating units/departments use this assessment as a guide in developing their specific risk assessments. The likelihood of occurrence and consequences may differ when viewed from an operating unit/department. For example, a major fire affecting the entire university is unlikely, whereas a fire affecting a specific warehouse that lacks robust fire prevention measures may be judged as likely. BCP addresses each hazard.

SJSU is vulnerable to a range of threats given the university's varying topography, mixed use of space, large student/faculty/staff population, and the transient nature of the population. A hazard matrix from the university perspective (shown below) depicts the likelihood of occurrence and severity level of each of the hazards listed.

University Perspective – Vulnerabilities Assessment

Hazard	Likelihood of Occurrence		Severity		
	Likely	Unlikely	High	Moderate	Low
Natural Hazards					
Earthquake	√		√		
Extreme Weather/Storm	√				√
Floods		√			√
Major Wild Fire & Smoke		√			√
Technological/Man-made Hazards					
Building Fire	√		√		
Building Utility Failure	√				√
Civil Disturbance (protest demonstration)	√				√
Hazardous Materials		√		√	
Multi-Casualty Accident (airplane)		√	√		
Sink Hole		√			√
Terrorism		√	√		
Utility/Telecom Failure (downed lines)		√			√

A similar vulnerabilities assessment needs to be conducted at a departmental level.

Departmental Perspective – Vulnerabilities Assessment

Hazard	Likelihood of Occurrence		Severity		
	Likely	Unlikely	High	Moderate	Low
Natural Hazards					
Earthquake					
Extreme Weather/Storm					
Floods					
Major Wild Fire & Smoke					
Other (specify)					
Technological/Man-made Hazards					
Building Fire					
Building Utility Failure					
Civil Disturbance (protest demonstration)					
Hazardous Materials					
Multi-Casualty Accident (airplane)					
Sink Hole					
Terrorism					
Utility/Telecom Failure (downed lines)					
Other (specify)					

CONCEPT OF OPERATIONS

Business Continuity Planning (BCP) is a program that assesses the existing operations, risks, and relationships of the University for development of organizational preparedness. BCP develops an integrated approach to ensuring that critical processes continue to function during and after a disaster or incident that interrupts the operation of the organization. The BCP command structure is designed to benefit the operational environment with coordinated emergency management (EM), IT disaster recovery and continuity of operations planning functions. Roles have been assigned as they pertain to executive management and decision makers.

Emergency Management
SJSU's Emergency Operations Plan (EOP) establishes policies, procedures and an organizational structure for response to major emergencies occurring on campus. The Plan incorporates operating procedures from the Incident Command System (ICS), the Standardized Emergency Management System (SEMS) and the National Incident Management System (NIMS) for handling major emergencies which could disrupt normal campus operations The EOP is a campus-level plan that guides the emergency response of appropriate SJSU personnel and resources during an emergency.

> Priority I: Preservation of Human Life
> Priority II: Preservation of Order
> Priority III: Mitigation of Immediate Threats to Life
> Priority IV: Preservation of Property
> Priority V: Restoration of Essential University Services and Operations

As the EM operations progress from Priority I through Priority V responses, the administrative control of the campus will transition from the NIMS/SEMS/ISC structure back to the SJSU organizational structure.   When required, the Emergency Operations Center (EOC) may be activated to support the ongoing response. The EOC serves as the centralized facility in which the predetermined Emergency Operations Staff will gather, check in and assume their emergency response roles.

The EOC is organized in accordance with NIMS/SEMS guidelines. The five Sections within the EOC are:
1. *Management Section:* The Emergency Director is responsible for overall implementation of the resources needed to respond to mitigate and terminate an emergency situation.
2. *Operations Section:* Represents the campus emergency services units – the actual on-scene emergency responders. They are responsible for the implementation of field operations and management of personnel assigned to response roles.
3. *Planning & Intelligence Section:* Responsible for receiving, evaluating and analyzing an emergency related information and providing updated status reports to the EOC Management and Operations Sections.

4. *Logistics Section:* Responsible for procuring supplies, personnel and materials support necessary to conduct the emergency response.
5. *Financial & Administration Section:* Responsible for cost accountability and risk assessment.

For a more detailed description of the EOC, see the SJSU Emergency Operations Plan.

Emergency operations have established methodologies for emergency response. These include roles and activities that define initial emergency response (activation phase), resolution of the emergency situation (termination phase) and return to normal operations (recovery phase). The EOC Emergency Director will have authority of control for the BCP activation and operation phases for all operations of the organization. Upon the Emergency Director's declaration of BCP activation, the BCP Coordinator coordinates BCP operations with the EOC Section Chiefs and the Emergency Management Recovery Team (Recovery Manager and Recovery Coordinators).

BCP Conditions of Activation

The Emergency Director declares BCP activation to initiate resumption and recovery services and communication. BCP activation puts into action plans to sustain critical processes and services. Mission recovery includes the recovery of facilities, infrastructure and services required for the return to normal operations.

Orderly alert and notification depends upon the amount of warning received, whether employees are on duty at university locations and the extent of risk for university employees or locations. Any disaster that adversely affects the university's ability to perform essential functions requires activation of the BCP.
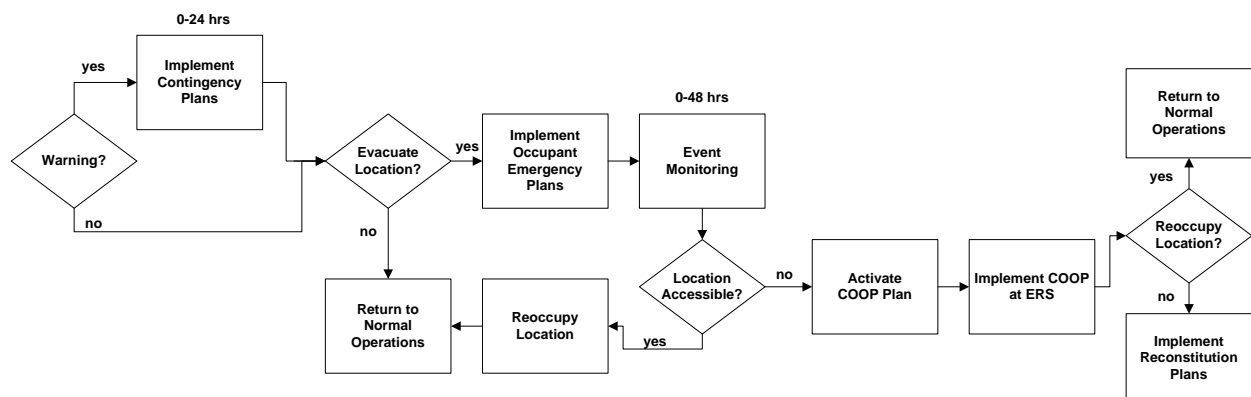
University employees will be contacted with alert and notification information using variety of communication resources/contact lists (e.g., Alert-SJSU, Emergency Personnel Roster; Response/Recovery Team Personnel form, etc.).

In the event of a vacancy in the position of President, succession lines have been established. Presidential Directive # 2009-03 serves as the official delegation of both authority and responsibility to the following administrators to make decisions on behalf of the President in a disaster or an emergency in which the President is absent or disabled.   The "Chain of Command" is as follows:

1. President
2. Provost and Vice President for Academic Affairs
3. Vice President for Administration and Finance/CFO
4. Vice President for Student Affairs
5. Vice President for University Advancement
6. President's Chief of Staff

The following should be added to the "Chain of Command" for major disaster or emergency situations:

7. Vice Provost for Academic Planning and Budgets
8. Chief of Police
9. Vice President for Information Technology and Chief Information Officer

BCP Conditions of Operation
BCP operations initiate upon BCP activation as contingency plans and recovery operations begin. Contingency operations run in conjunction with emergency management recovery operations through to completion of the BCP operations phase. Mission recovery includes the recovery of facilities, infrastructure and services required for the return to normal operations.

BCP Conditions of Termination
BCP operations can be terminated when facilities, infrastructure and services are sustainable and reliable. The Emergency Director declares that normal operations may resume upon consensus from the BCP Coordinator, Section Chiefs, Recovery Manager and Recovery Coordinators.

BCP Critical Issues
BCP operations are dependent on planning, communication, coordination and security. Critical issues include: personnel safety, environmental safety, physical security, cyber security, identification of critical personnel, identification of critical assets, identification of critical processes, identification of vital records, established command structure, managed command communications, managed public information and safety communications, managed emergency management and BCP internal communications, prioritization of activities, training, testing and continual improvement, and timely implementation.

University employees with select knowledge, skills and abilities are required to perform the tasks associated with the university's essential functions. The following personnel are identified as critical members of the Emergency Response Group (ERG).

Emergency Personnel			
Office/Division	Position	Duties	Number

The alternative facilities (ERS) will be capable of supporting operations in a threat-free environment in the event that essential functions and supporting staff are relocated to the site. The ERS will have sufficient space and equipment to sustain operations for a period of up to 30 days.

Alternate facilities that will serve as Emergency Relocation Site (ERS) are under consideration. The strategy is to partner with other CSU campuses (i.e., East Bay, and/or San Francisco) to develop a reciprocal arrangement via a Memorandum of Understanding that would allow one campus to use the other campus' Emergency Operations Center in case of a disaster.

A changing threat environment emphasizes the need for BCP capabilities that enable the university to continue its essential functions across a broad spectrum of emergencies. Testing, training, and exercising of BCP capabilities are necessary to demonstrate and improve the ability of departments to execute their essential functions. The university's testing, training, and exercises incorporate the three functional areas of testing systems and equipment, training personnel, and exercising plans and procedures.

BUSINESS CONTINUITY PLAN MAINTENANCE

To maintain viable continuity of operations capabilities, the University is continually engaged in a process to designate essential functions and resources, define short- and long-term BCP goals and objectives, forecast budgetary requirements, anticipate and address issues and potential obstacles, and establish planning milestones. Following is a list of activities necessary to monitor the dynamic elements of the university Business Continuity Plans and the frequency of their occurrence.

Business Continuity Plan Maintenance

Activity	Tasks	Frequency
Plan update and certification	• Review entire plan for accuracy. • Incorporate lessons learned and changes in policy and philosophy. • Manage distribution.	Annually
Maintain orders of success and delegations of authority	• Identify current incumbents • Update rosters and contact information	Semiannually
Maintain emergency relocation site readiness	• Check all systems. • Verify accessibility. • Cycle supplies and equipment, as necessary.	Monthly
Monitor and maintain vital records management program	• Monitor volume of materials. • Update/remove files	Ongoing